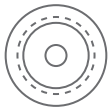


ONE

Introduction

In India, proving your identity is only a fingerprint scan away. In less than seven years, more than 1.1 billion residents have enrolled in what must be the most innovative identification system in the developing world. Each resident can now authenticate themselves at banks, government offices, shops, and a host of other point-of-service facilities across the country by providing only their unique Aadhaar ID number and either a fingerprint or iris scan. Using the number and a scan, they can satisfy Know-Your-Customer (KYC) requirements to open bank accounts, with no need to laboriously assemble and copy documents. Beneficiaries of the country's public distribution system are increasingly authenticated through fingerprint scans when they receive their subsidized food allocations through Fair Price Shops. In Andhra Pradesh's Krishna District, where reforms are most advanced, the supply chain for the public distribution system has been totally revamped. Deliveries are checked on electronic scales and must be signed off jointly by the transport operator delivering the goods and the Fair Price Shop proprietor, each certifying by registering their ID number and fingerprint.

The same identification system can be used in an unlimited range of transactions and interactions: to receive pensions and administer scholarship programs, to monitor the attendance records of public officials, or to administer energy or fertilizer subsidy programs. India's Aadhaar-enabled reforms of liquefied petroleum gas marketing have shifted household price subsidies to direct transfers into bank accounts; they are already among the world's largest

reforms in the energy sector. Measures are now under way to extend the use of the system to an ever-widening range of applications, such as registering property, filing taxes, and identifying children for school meal programs. Digital payment is now possible from any Aadhaar-linked bank account to any other account simply with the payee's Aadhaar number.

More advanced digital services are also in progress. Indian residents will soon be able to sign documents electronically and to store key credentials, such as digitally certified copies of birth or school examination certificates, in a secure digital locker opened by a biometric scan. Documents can be shared as desired with potential employers or other entities linked to the country's digital ecosystem. The process even distinguishes between copies of certificates uploaded by the applicant and those directly issued and certified by the relevant authority.

Such a sophisticated system has become possible only recently. Before it demonstrated its capabilities, there was considerable doubt over whether biometric technology would be precise enough to successfully distinguish among individuals in so large a population. Comparing every one of India's people against each of the others to ensure that identities are unique involves a huge number of pairwise comparisons and requires extremely high accuracy. This accuracy appears to have been achieved—proof-of-concept tests conducted in 2012 suggest an error rate in deduplication of less than 7 in one trillion (Gelb and Clark 2013b).

India's system offers capabilities far ahead of those available to residents of other countries, even those in the Organization for Economic Cooperation and Development (OECD). It also appears to be the lowest-cost digital identification system on a per-head basis, by a considerable margin. But it is only one of many transformative identification programs being implemented today, in some cases with significant technology and institutional innovations. National ID programs intended to provide "foundational" identification for multiple purposes are being rolled out across the developing world at an unprecedented pace. "Functional" identification programs, designed to support a particular purpose or service such as access to healthcare, a pensions program, or voting, have also mushroomed in the past decade and a half. Virtually all of these programs incorporate digital technology, including biometrics.

The right to a recognized identity has long been an element in the human rights agenda. The 1948 International Declaration of Human Rights, for instance, contains the right to recognition before the law and the right to a nationality. Yet it was only in 2015, with the adoption of the Sustainable Devel-

opment Goals (SDGs), that the global community recognized identification as a development priority. SDG target 16.9 sets out to "provide legal identity to all, including through birth registration, by 2030" (UN 2015). It is not entirely clear how to interpret this target, or whether a simple enumeration of those with and without legal identity is a sufficient metric. The only quantitative indicator attached to SDG target 16.9 refers to birth registration: the percentage of children under age 5 whose births have been registered with a civil authority, disaggregated by age. However, ensuring that all members of society—no matter how poor or isolated they may be—have their existence officially recognized is only a start.

Robust identification systems designed and implemented with the SDG aspirations in mind can be a catalyst for achieving many other development goals and targets, from gender equality to environmentally sustainable energy systems. For these ambitions to become a reality, formal identification systems must open doors rather than lock in hardship, and be used to expand freedoms and capabilities rather than enable exclusion or coercion.

Although the "legal identity" target is new, donors and partners have supported many identification programs in developing countries over the past two decades. However, with only a few notable exceptions, engagement has been fragmented and driven by individual applications. Identification has been considered as a mechanism for a particular purpose, such as improving the accuracy of a voter roll for a particular election or implementing a social transfer or health insurance program more effectively. This has encouraged the emergence of multiple ID programs, often disconnected and with little or no synergies between them—an inefficient and wasteful approach, considering that programs to register people and provide identification services are inherently multiple-use investments. The stakes are raised as they include higher levels of technology that boost their capabilities but also increase their costs and threaten the sustainability of fragmented systems.

What are the implications of the rapidly changing identification capabilities and new aspirations for development policies and programs? How should countries and their development partners respond to the identification revolution? Any effort to address these questions has to recognize that knowledge gaps are large; these are still early days in the identification revolution. Far more evidence, and far more rigorous evidence, is needed to understand the longer-term impact of the new systems and their underlying technologies. Only a limited number have been analyzed in any detail, and even in those cases the systems and their uses are still evolving. Nevertheless, this is a good time to

take stock of ID programs and policies, especially as the development discourse around them needs to respond to the SDG target for establishing "legal identity" for all.

This book aims to provide an overview of the rapidly changing area of identification, including evidence on positive effects, good practices, and innovative solutions, and at the same time pinpoint the need to address crucial risks. It should be of interest to policymakers and development partners that invest in and implement ID programs, or are planning to do so; development practitioners, including the staff of international financial institutions (IFIs), multilateral organizations, and donors that want to learn more about systems and technologies that can accelerate the achievement of the SDGs; and researchers, academics, and others who would like to gain a better understanding of how new ID technologies can be and are being used.

Robust and inclusive identification systems can be an important pillar of sustainable development, particularly when leveraged by new technologies that greatly increase their accessibility, precision, and usefulness. The emerging evidence suggests that, at their best, they can be a tool to recognize and realize individual rights and expand economic opportunities, including for the poorest segments of society. They also can help build state capacity to deliver public services and social protection programs more effectively, to manage public spending, and to make public institutions more accountable. With the adoption of the legal identity SDG target 16.9, policymakers and practitioners alike are seeing the appeal of a more strategic approach to the role of identification in countries' development strategies. Such an approach requires a stronger focus on multipurpose country systems, including both civil registration and identification, rather than simply seeing each possible use-case as a separate venture.

Yet success is not guaranteed. Achieving positive development outcomes depends on many factors, including the design of the systems and how effectively they are implemented on the ground. At their worst, they can exacerbate existing problems and introduce new ones. The formalization of identification processes and requirements can exclude poor and vulnerable groups and support institutionalized discrimination; ID systems can also facilitate state and commercial surveillance. Even in less unfavorable contexts, they can waste valuable resources on costly programs of little value, especially as more expensive technologies are employed. Not surprisingly, views differ on the contribution that such systems can make to development and the possible ways to balance potential gains and risks.

This book will not delve deeply into all details of the current systems, as

these details are evolving, in some cases rapidly. Nor will it produce a manual for digital identification systems or advocate for any particular system as a model for all countries; doing so would be neither realistic nor appropriate. However, even from the emerging evidence to date, it is possible to outline sensible guidelines and approaches that will enable the identification revolution to help achieve many of the wide-ranging development outcomes articulated by the SDGs. The authors' more modest objective is to contribute to this process.

Why Does Identification Matter for Development?

All communities—families, bands, tribes, nations—require mechanisms to establish and manage the identities of their members. "Identity" can have many interpretations. In this discussion, identity comprises the range of attributes that go into defining a person as a distinct and unique individual.[1] Some attributes may relate to appearance, others to behavior, still others to ethnicity, friendships and family connections, or the details of a person's birth—date, location, and parentage. Within any community, individual identity is linked to rights, entitlements, and responsibilities, including the critical question of whether or not an individual is recognized as a member of that community. The ability to distinguish between people is essential to administer community affairs, including security, as well as to establish and enforce private contracts.

Establishing an identity—one that exists and is unique—can pose a challenge even in the richest countries. Alecia Faith Pennington, the "girl who does not exist," was born in Texas to conservative religious parents. Her birth was purposefully not recorded, this being seen by her parents as a way of making her "sovereign" and independent from the wider, more secular, society. She lived on a farm, was homeschooled, and her medical treatment was provided in ways that left no medical records. Her plight became apparent in September 2014 when she left home at the age of 19, only to find that she was unable to provide sufficient documentary proof of her actual existence to obtain a birth certificate. Without some proof of existence, she could not function in society or the U.S. economy. She could not apply for a Social Security number to work

1 The definition of "identity" in the Merriam-Webster dictionary includes: "sameness in all that constitutes the objective reality of a thing" or "oneness" and "the distinguishing character or personality of an individual" or individuality. This definition does not mean, of course, that an individual might not be distinguished by different attributes in different contexts, but it points to the combination of features that renders the individual unique.

or a license to drive; nor could she hold a bank account. She was not covered by existing provisions for aliens or refugees; they came from "somewhere," but she came from "nowhere." Her situation was only resolved by the passage of a special bill, HB 2794, which was signed into law in Texas in June 2015.[2]

Validating oneself against a known identity can also be a challenge. One celebrated case is the still-debated story of Martin Guerre, a French peasant who disappeared from his village and his wife, Bertrande, in 1548, only to apparently reappear in 1556. The arrival looked similar to the man who had vanished and could support his claim to be Martin with detailed knowledge of his previous life. He was accepted as Martin by Bertrande and lived with her for three years, and he also claimed the inheritance of Guerre's deceased father. He was, however, not accepted as Martin by other members of Guerre's family, who continued to search for the "true Martin." The case was finally resolved after the appearance of another man with a wooden leg who claimed to be Martin Guerre, although he was apparently less able to recall previous details of his life with Bertrande than the first arrival. After a series of legal proceedings, the second arrival was accepted as the true Martin by Bertrande and other members of the family. The imposter confessed and was hanged.[3]

There are millions—by some estimates, over 1.1 billion—Alecias and Martins living today: people who do not have an officially recognized identity or are not able to provide necessary proof of who they are. They live mostly in poor countries and are usually among the poorest and most marginalized members of their societies.[4] The global identification and identity verification gap limit the freedoms and capabilities of the individuals directly affected, and can have system-wide effects that hamper the development of effective and capable institutions and constrain sustainable development and economic growth.

Globally, it has been estimated that some 2 billion children and adults have not been issued with birth certificates. In some countries, schools may turn away children who do not have an official birth record. If these children are

2 See, for example, Ohlheiser (2015), or the 2016 Radiolab podcast "The Girl Who Doesn't Exist," www.radiolab.org/story/invisible-girl/.

3 Martin Guerre's story is described in detail in Natalie Zemon Davis' 1983 book *The Return of Martin Guerre*. It has also been adapted to a film ("Le Retour de Martin Guerre") and was the subject of several musicals.

4 The contemporary problem of proving identity is not confined to poor countries, however. Bradley (2017) paints a jarring picture of the difficulties faced by homeless and other poor people in Washington, D.C., who have lost identity documents even though they have been registered.

permitted to enroll, they may not receive scholarships, grants, or other support to ensure their continued attendance or to help improve learning outcomes. Without adequate identification, they may not be allowed to sit certifying examinations; after all, what use is a test if there is no way to assert the identity of the person who claims to have taken it? Without recognized identification, they may not be able to enroll in higher education, or to get a job in the formal sector.

More fundamentally, an official proof of identity, one that is recognized for official purposes, lies at the heart of the social contract. Who gets to vote, who gets to receive a social grant or pension payment, who gets to be seen by a doctor, who gets to open a bank account or even register a mobile phone number is increasingly a function of who has a recognized identity—an official record of their existence as a unique person—and can validate themselves against their claimed identity. With the consolidation of communities into nation states and the formalization of rules to define membership, as well as the duties and privileges associated with it, identification processes have similarly become more formal. People without an officially recognized identity face myriad barriers to full economic and political participation. Because of KYC requirements, they cannot place their savings in a bank account or receive cash payments electronically. Tighter identity requirements mean that they increasingly are not even able to purchase a prepaid SIM card to operate a mobile phone.[5] Lack of officially recognized identification or identity credentials[6] is also a severe barrier for international travel and migration and for the economic opportunities they afford.

Lack of strong and verifiable identification poses considerable difficulties not only for individuals but also for the broader communities and states where they reside. Government agencies will struggle to administer programs effectively—for example, to ensure that social transfers or pensions are not received multiple times by the same beneficiary, or to eliminate ghost workers or pensioners. Private companies and banks will find it harder to operate profitably in settings where they cannot reliably verify the identities of their em-

5 GSMA (2016) discusses the increasing prevalence of SIM registration and how different countries are managing this.

6 The terms *identification credential* or *ID credential* include any widely accepted proof of identity, generally issued by or on behalf of a state. Common examples include a national identification card, a driver's license, or a passport, but many other types of identification documentation could fall into this category, including the combination of identification number and biometrics in systems that do not rely on cards.

ployees, clients, or business partners, or where they need to develop their own customized and costly systems. The absence of any single consistent identifier makes it difficult for credit bureaus to operate and for banks to offer credit to all but the wealthiest, most well-established, and best-known customers. The use of many different and unrelated identification systems greatly complicates tax administration because it is difficult to combine data on different income sources and assets by an individual taxpayer.

The difficulties in bridging the global identification and identity verification gaps are manifold. In some cases, no official identity may have been established at all. In others, identity credentials may be lost; in still others, credentials may be produced but be of low quality or not easy to verify. Many countries still rely on decentralized paper-based local registries rather than digital databases. Although there is a continuing role for physical records, if these are destroyed by conflict, a natural disaster, or another calamity and have not been backed up—not an uncommon situation in poor countries—those registered have no way of proving that their claimed identities are valid. Without an underlying registry, whether paper or digital, an ID credential may not provide the level of assurance needed to access public services or for some private sector transactions, particularly when the document is easy to alter or falsify. Those whose identification claim is unverifiable or whose credentials are weak may thus face much the same barriers as someone with no established identity at all.

Verification challenges are becoming more complex as populations turn increasingly mobile, both within and between countries. The global migrant total has reached 1 billion, about one in every seven people. About three-quarters are internal migrants; India alone has some 400 million internal migrants who live and work outside their traditional communities. Records in paper-based registries as well as offline digital ones may be difficult to consult and verify remotely even within the same country, while cross-border identity verification can run into even greater obstacles.

Refugees—now at a post–World War II high of 21 million within the total of 65 million people displaced by natural disasters and conflicts—pose another huge identification challenge. Even if they had well-recognized ID credentials in their countries of origin, a paper copy of a birth certificate or other identifying document (even one with recognized security features) may not be adequate to persuade officials in other countries that they are who they claim to be, because these officials may not be able to check the document against a registry and may lack confidence in the issuing process.

How Is the Identification Landscape Changing in the Digital Age?

Of course, the need for identification and the challenges in providing it are not new. The registration of births and deaths goes back centuries in many countries, as do the precursors to many modern national identification systems. China has had an elaborate system of identifying its people for many hundreds of years. The precursor to Japan's civil registry dates from around 1670 and listed the name, age, and sex of each individual in each village by household. Impressively, it was updated annually. Large-scale civil registration in France started in 1792, at the behest of the revolutionary government, while church records of vital events go back far longer. Many of the needs and challenges documented in the outstanding historical compilation by Breckenridge and Szreter (2012) have an eerily familiar ring today.

From the earliest times, identification systems have relied on some subset of the many different attributes that together distinguish each of us as a distinct person. They may be bundled into three main factors and combined in different ways to form the basis for identification:

- **Something you are:** A biometric such as physical appearance, a distinctive voice, or a smell or behavioral pattern. This is surely the oldest form of recognition, as well as the most recent. In modern digital times, it can encompass digital biometrics such as fingerprint, iris or finger-vein-patterns, voice patterns, DNA, dynamic signature, or, on a computer, keystroke rhythms or mouse movement patterns.
- **Something you have:** A birth certificate; an ID card; or a mobile ID, token, or other physical credential. Something you have could also be a person, such as a well-respected and credible individual ready to vouch for you. The best identifier for an infant is still probably its mother.
- **Something you know:** A personal identification number (PIN) or password, or the ability to provide personal information that is unlikely to be known by others.

Modern identification systems often combine all three factors: are, have, and know. Estonia's pioneering digital ID system, which is supported by comprehensive civil registration, is one such case study considered in this book. At the age of 15, fingerprints are taken on registration for the national ID system

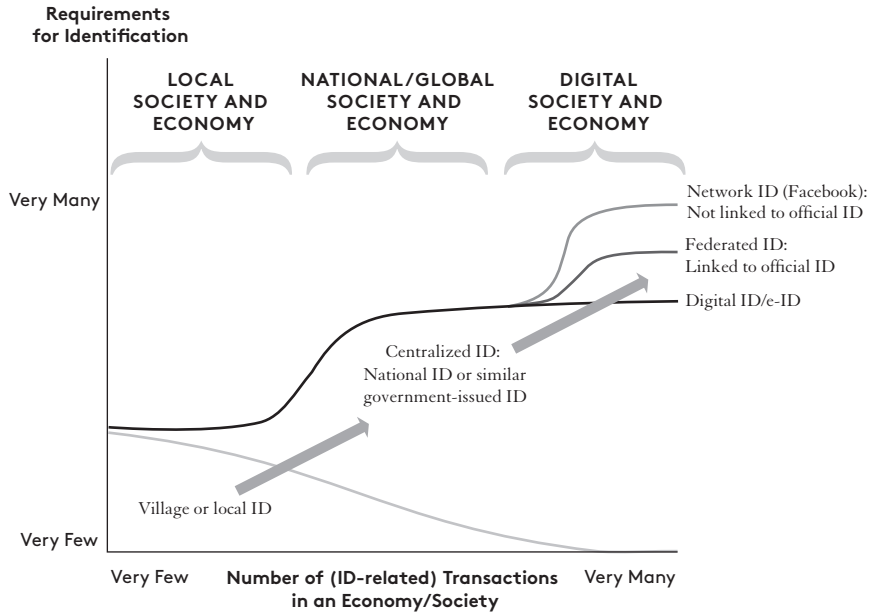
(who you are: to prevent multiple identities). An ID card is issued (what you have); it includes digital certificates to enable the holder to both authenticate his identity and to sign documents electronically. For these purposes, the holder authenticates himself against the card by providing two user-selected and private PINs (what you know), one to authenticate himself and the other to sign. Multifactor authentication offers extra security relative to the use of only one factor. But, as in the case of Martin Guerre, even multiple factors—his appearance (are), testimony from Bertrande (have), and the ability to provide personal information about his life with her (know)—cannot fully eliminate the possibility of identity fraud or error.

Phases of Identification: Village, Central, and the "e-Village"

Identity management systems are evolving over time and with advancing technology and economic development. Although they can differ in many ways, it is useful to think of them in three phases (figure 1-1).

- In the initial "village" phase, most social and economic interaction is local, as is identification. Identities are established and verified based on personal connections—who you know and who knows you—sometimes supplemented by local documentary evidence.
- As societies become more mobile and fluid and wider market-based transactions replace local trade and subsistence economies, countries usually transition to the second phase of centralized national identification and other centrally administered systems. These have traditionally been paper based but are increasingly supported by digital technology and provide identity management services to support a widening range of virtual interaction and transactions. This is the current frontier for identification in the development context.
- However, centralized systems may not be the last word. The shift toward digital societies and economies has created the possibility of a third phase, of "federated" or "e-village" approaches to identification and authentication. In this phase, evidence to support the existence of an identity and to authenticate a claimant is drawn from a wide range of sources that can include databases held by private service providers, such as banks, as well as by membership and active participation in online communities, in addition to official identifying data and ID credentials such as passports.

FIGURE 1-1 Identification Systems, Development, and Technology



The first stage. "Village" identification remains important in many countries despite the rapid adoption of new systems and technologies. One example of "village" identification would be the family card systems in some Asian countries, which predate other forms of identity management such as civil registries or centralized national ID cards. A number of Asian countries, including Cambodia, China, Indonesia, Laos, and Vietnam, have long operated some version of the household registration (hukou) system, with details of all family members included in a family book held by the designated head of the family. These systems have often been driven by a desire to control movement between regions and particularly migration to cities.[7] As another example, Ethiopia's *kebele* ID system is administered by some 16,000 administrative units that each typically includes around 8,000 people.[8] The initial identity is certified and validated by a system of subadministrative units and groups within the kebele

7 For the example of Vietnam, see World Bank and Vietnam Academy of Social Science (2016).

8 See World Bank (2017b, 2017c) for more information on Ethiopia's identification system.

down to the level of ten or so households—a very local form of identification. Each kebele issues its own ID card or booklet to adult residents in Amharic or the local language or both, and the cards and booklets can vary in color and design. In the absence of a functioning civil registration system or a conventional national ID system, the kebele card provides full legal identity to adult citizens. For example, it is the only identity documentation required to apply for an Ethiopian passport.

In other countries with no nationwide system in place, affidavits from local government officials may still be considered to provide the most reliable form of identification. This was the case, for example, in Tanzania, at least until the rollout of the 2015 voter ID card. In countries with weak civil registration systems, local officials and committees may be asked to confirm that an individual enrolling into an identification program is really a member of the community. Identification in Somalia is still based primarily on the clan system. Verification can include exhaustive questioning on clan knowledge and tests of genealogical history extending back many generations (Rader 2016). This process raises severe hurdles for those with unusual or uncertain ancestral histories.

Decentralized "village" systems can work adequately in conditions of limited mobility, but face a number of limitations. One problem is how to ensure the integrity and quality of the processes carried out at local levels and the ID credentials issued by local governments. Usually these will be on paper and vulnerable to alteration or forgery. Poorly maintained local records pose another problem, especially in low-income and rural settings. Most seriously, local systems require tight administrative controls to prevent multiple identities, and begin to break down as people move more frequently, migrating to cities or moving between communities. In Vietnam, at least 5.5 million people lacked permanent ID documents in their place of actual residence (World Bank and Vietnam Academy of Social Sciences 2016).

Centralized identity management. As societies and economies become more complex, geographically fluid, and market based, the demand for portable identity services increases because of the rising frequency with which individuals need to prove their identity in situations where they are not known personally. Transactions become more impersonal and local systems come under pressure. The systems transition to the second phase of centralized identification, usually managed at the national level. Records are standardized and digitized, with personal identifying information consolidated into one or several databases, depending on the country's choice of identification architecture.

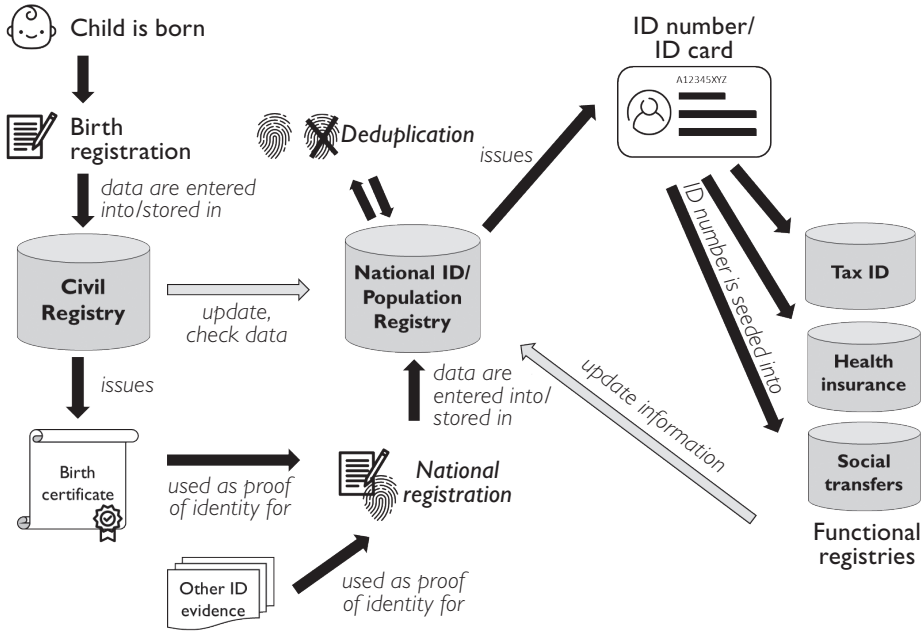
Authentication is then against a centrally issued ID card or other credentials, or directly against the database. Locally administered or issued identification continues to support some transactions, but an increasing number rely on centrally issued proof of identity. Kenya and Malaysia are two of the many examples of countries that have built centralized systems issuing ID cards that are used for virtually all identification purposes.

The essential features of such systems are shown schematically in figure 1-2 for the case in which the country operates a civil registry and a national identification program. Individuals can be registered at two points in life, at birth in the civil registry and at a later age, generally ages 15 to 18, for the national ID. In countries with a strong civil registry, this system can provide a flow of information into the population register that underpins the national ID program; it can also validate a birth certificate and other information presented at registration. Where civil registration is weak and many people lack birth certificates, the national ID will need a separate process to assemble other evidence of identity at the point of enrollment. This could include school or baptism certificates, letters from local authorities, and oral testimony.

The system also checks to ensure that the person is not already registered under the same or another identity; each new enrollee must be compared with all those who have already enrolled. This can include both biographic and biometric deduplication. An ID card with a unique number, or just the number, is issued and the number is then seeded into the databases for various functions, services, and programs. As people engage with these programs the process generates new information so that the central identity data can be updated. Some OECD countries with strong civil registration processes have chosen not to implement a centralized national identification program; they rely on civil registration and other documentary evidence to issue functional ID credentials, such as driver's licenses or passports, for various purposes.

The quality and integrity of centralized identification depend on the features of the system and how it is managed. As depicted by the arrow in figure 1-1 and also in figure 1-2, especially in the many developing countries with weak civil registration systems, centrally managed identification programs still need to rely on local processes to confirm the identities of adults at the point of enrollment. One example is the "introducer" option for enrollment in India's Aadhaar program, whereby a known and respected community figure, such as a local official or a schoolteacher, can vouch for a person's identity. This provision was put in place to enable people with no documentary evidence of

FIGURE 1-2 Centralized Identity Management System



identity to enroll. In the case of Kenya's national identification program, local vetting committees review candidates, particularly in border regions, to ensure that they are who they claim to be. Local systems thus provide the basis for the "official" identification recognized by government agencies, which is used more frequently as countries become richer and the frequency of remote and digital interactions increases.

Decentralized identification and the potential of the e-village. With increasing connectivity and the rise of digital societies and economies, providing identity services remotely has become the new frontier for identification systems. With about 5 billion subscribers, mobile communication is becoming ubiquitous across the globe, and the number of mobile phones in circulation has risen to about 7 billion—close to the population of the planet. Broadband access has become quasi-universal in most developed countries, and though it lags somewhat behind in poorer ones, even there, connectivity is rapidly expanding.[9]

9 In 2016 it was estimated that mobile operators covered 95 percent of the global population with 2G connectivity and 84 percent with 3G mobile signal (ITU 2016).

The growth of the digital society and the digital economy opens up new possibilities for providing services more efficiently. According to the 2016 United Nations (UN) E-Government survey, 148 countries provided at least one form of online transactional service, a substantial increase from previous years (UN 2016). The shift toward digital societies and economies throws up new challenges for providing identification services, in particular how to identify participants for remote transactions. To meet this challenge, a growing number of centralized systems, including those in Estonia and India, offer full remote digital identification. However, the growing "digital cloud" of data, drawn from increased participation in online communities and the rising number of digital transactions, offers a new decentralized approach to managing identities. They can again be established and verified on the basis of "who knows you?" as in the "village" phase of identity management but through the use of digital technology and virtual communities. As before, the level of identity assurance rests on the credibility of the entity that conducts due diligence and the range of evidence considered.

Figure 1-1 distinguishes two different types of third-stage identity management that could allow for remote verification of individuals for online transactions based on digital information. Federated identity providers or assurers, such as those authorized by the British GOV.UK Verify program, are vetted and authorized by the government. They can draw on official databases such as passports, driver's licenses, or gun permits, and can tap into other sources of information, such as financial data or payment records, to verify identities to higher levels of assurance. Banks and mobile companies are perhaps best placed to offer such identification services as they require their own customers to provide official identification for KYC purposes. The strength of this type of system is that it can be "double-blind"—the identity assurer does not know the purpose for which identification is requested, and the requiring entity does not know the range of evidence considered.

A second type of "e-village" identification is that provided by social networks, such as Facebook. These systems do not necessarily require government-issued credentials from those seeking to become members. The identities of their users could be verified, however, based on testimonies from other members and their interactions across the network, as well as pictures and location information that they have shared with the virtual community. The algorithmic processes of social networks may not provide an acceptable level of identity assurance for all purposes, but their power is increasing and other businesses increasingly are using them as references for identification and verification.

This third stage of identity management may not be the first priority for poor countries seeking to endow their citizens with basic identification. It does not provide "foundational identity" in the same sense as the previous stages, and there are still questions about the strength of the business case for private entities to provide high-quality identity assurance services. However, systems of this type have made some important contributions to thinking about identity management. They are bound to become more precise and more important as the volume of digital data continues to grow at the staggering rate of 42 percent per year, as projected by market studies (Rizzatti 2016).

The Explosion in Identity Management Systems

The proliferation of registration and identification systems, the improvements in the precision and affordability of the technologies they rely on, and the growth in the number and scope of government programs and private sector companies that depend on accurate identification have been nothing short of revolutionary. Figure 1-3 offers a broad global picture of the spread of birth registration systems and national-level identification programs[10] based on evolving data from the World Bank's Identification for Development (ID4D) Program, distinguishing high-income countries (HICs) from middle- and low-income countries. In considering the figure, it should be recalled that the number of widely recognized sovereign states has increased over the period: 149 in the 1960s, 171 in the 1970s, 193 in the 2000s, and 195 in 2017.[11]

From figure 1-3, even as far back as 1960, the vast majority of countries maintained a birth registry. The number has increased steadily in subsequent decades to the point where almost all countries have such a system in place today, even if its coverage may be incomplete. In contrast, very few countries, particularly those in the low- and middle-income categories, had a national identification program five decades ago. It was only after 1990, and especially after 2000, that such systems began to be deployed rapidly across the devel-

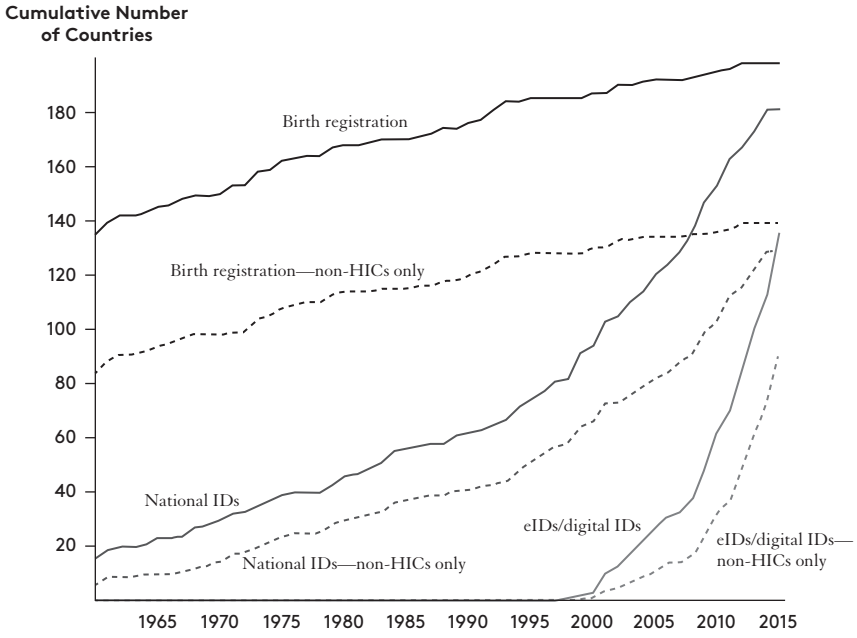
10 The term "national-level" allows for the inclusion of programs administered at the national level that are not conventional national identification programs, such as India's Aadhaar program.

11 Note also that the income categorization of countries over these five decades has also changed considerably. High-income country (HIC) categorizations refer to countries' status as of 2016. For more detailed information, see the World Bank ID4D initiative's 2016 ID4D Global Dataset at http://data.worldbank.org/data-catalog/id4d-dataset.

oping world. As of 2016, World Bank data indicate that all but 12 low- and middle-income countries have established or initiated a national-level identification program. Almost half of existing national ID programs in developing countries—a total of 63—have been launched within the past 15 years. Every country in sub-Saharan Africa, for example, has now implemented or committed to a "foundational" national ID program, with the objective of providing a multipurpose proof of unique identity, although some are still at a preliminary stage.

These multipurpose programs are only part of the picture. Many "functional" ID programs have been launched for particular purposes, such as registering voters, identifying beneficiaries for social transfer programs, or performing due diligence on clients for financial services. Some countries now have multiple large-scale programs—Mexico has at least seven, and Nigeria

FIGURE 1-3 Identification Programs in High-Income Countries (HICs) and Others



Source: World Bank ID4D dataset; January 2016 edition.

has at least a dozen.[12] There are also many smaller programs, such as that launched by the West Africa Examinations Council, to register students biometrically to reduce the incidence of examination fraud.

The rapid proliferation of identification systems reflects several factors integral to the functioning of the modern state. Developing countries are creating ID systems in response to growing perceived needs, whether to strengthen national security in the face of an increase in perceived threats, improve the credibility of elections, or implement large-scale economic or social programs. In some cases, providing national identification services to the population is seen as an integral component of state-building. How have various developments contributed to the explosion of ID systems over the past two decades?

Security. One critical driver has been an increase in perceived security threats. The rise of international terrorism, conflicts in border areas, and growing refugee flows have made knowing who is who a priority for many governments concerned with protecting their citizens. Regulatory authorities have needed to respond to growing international pressure for higher standards. In the aftermath of the events of 9/11, concerns over money laundering and the financing of terrorism have led to more stringent regulatory recommendations from the Financial Action Task Force (FATF). In response, national KYC regulations and processes have become more stringent. A verifiable identity is now a prerequisite for engaging in almost any formal financial transaction. Customers who lack credentials are unable to open financial accounts; likewise, financial institutions that are unable to comply with identity verification requirements risk being cut off from correspondent banking relationships. "Derisking" threatens not only poor countries that have inadequate identification systems but also customers of money transfer organizations that traditionally have relied on less rigorous customer information than that required by banks (CGD 2015).[13] Enhanced security requirements for global travel also have intensified demands for accurate identification, including more secure travel documents.

12 Such a proliferation of identification programs was also characteristic of 18th-century England and Holland, where a strong state and commercial economy was associated with a profusion of registration systems promoted in civil society (Breckenridge and Szreter 2012).

13 Pressure for stronger KYC processes since 9/11, including for poor customers, may seem ironic in the light of the leak of over 11.5 million confidential documents in the Panama Papers scandal of April 2016. These files showed how the rich and powerful continue to be able to conceal their beneficial ownership in offshore tax havens.

Elections. Following the end of the Cold War, the average number of multiparty elections has jumped from one per year to around seven in sub-Saharan Africa alone. Registering voters has become a priority to support the consolidation of democratic processes and state-building, and often has been generously supported by international donors. The mixed record of biometric voter registration, and the less frequent attempts to authenticate voters biometrically at the polls, suggests that these costly programs carry significant risks (see chapter 2, and Gelb and Diofasi 2016a). The use of high-technology identification systems has not been consistently successful, and despite their considerable expense, voter registration drives often have not left much behind in terms of more permanent identity management assets. Nevertheless, elections have certainly been a powerful driver of spending on identity management systems.

Expanding public administration and government transfers. By 2014 over a billion people were receiving government transfers and other payments, with the average developing country operating about 20 different social safety net programs at an annual cost of 1.6 percent of its gross domestic product (GDP) (World Bank 2015). Ensuring that social transfers reach their intended beneficiaries and improving the targeting of social safety net programs—as well as unifying the beneficiary rolls for the programs to reduce overlap—are part of the global identification challenge. So is the need to prevent fraud and diversion in other public payments, including subsidies, government payrolls, and pensions. A general rise in literacy, the spread of communication technologies, and increased data availability probably also have played a role in placing countries' public administration systems and the effectiveness of their public spending under greater scrutiny, and encouraging the use of robust identification systems capable of ensuring that identities are unique.

Digital technology. Technology has also been a driver of the new systems, in both positive and negative ways. On the positive side, the new systems bring new capabilities to support the more effective administration of public programs and service delivery. Digital identification is also a valuable resource for the private sector, whether in banking, health insurance, or other applications. Its adoption is a necessary step toward satisfying the growing private and public service demand for e-identification for remote transactions and for the world's 3.5 billion (and counting) internet users. On the negative side, some programs may have been driven by the opportunities for side payments afforded by less-than-transparent high-value technology procurements. A number of countries have opted to purchase state-of-the-art biometric equipment and introduce high-tech multipurpose smartcards with advanced identity verification capa-

bilities even where the authentication and service delivery infrastructure to effectively use these features had not been put in place. By requiring more demanding identification and raising the prices of passports, driver's licenses, and other credentials to excessive levels, governments can also compel those needing identification to foot the bill at the expense of inclusion.

Transformative Identification Technologies: Catchup and Lags

Whatever the motivation in particular cases, as shown in figure 1-3, the proliferation of national identification systems has gone hand in hand with the adoption of digital technology, especially over the period since 2000, which has seen a sharp uptick in the deployment of digital ID systems (or e-IDs).[14] Virtually all new programs, as well as upgrades to older paper-based ones, use digital technology in some way. Digital biometric identifiers, usually fingerprints (and increasingly face and iris), are used in the vast majority of the new systems. In the first instance, biometrics are taken to limit the possibility of multiple registrations—to ensure that each registrant can only enroll once and thus that each recorded identity is unique, if not absolutely then at least in a statistical sense.[15] At present this is the only known approach to deduplicate enrollments, so as to ensure statistically unique identification in large populations. Their second function is to authenticate people against their claimed identities—but this is not, of course, the only digital approach toward authentication. Other options such as PINs and one-time passwords are widely used and will continue to be so, possibly in combination with biometrics to provide multifactor authentication. Biometric technology has also opened the door to new ways of sequencing identification programs by reducing reliance on detailed biographical information.

Table 1-1 summarizes available information on the diffusion of this technology across countries at different levels of development.[16] At 75 percent, the

14 Digital identity systems or e-IDs refer to identity systems that use digital technology in several ways: electronic databases to store and manage records; electronic credentials to serve mobile, online, and offline applications, including PKI (public key) infrastructure; and digital biometrics to identify and authenticate individuals.

15 The term "statistically unique" refers here to systems where the probability that any individual has multiple identities is very small. No system is able to guarantee absolutely unique identity. See chapter 4.

16 There are still substantial data gaps in these areas; table 1-1 draws on information available as of January 2016. For more detail on the state of indentification systems in Africa, see World Bank (2017b, 2017c).

share of countries using digital identification systems, as opposed to either paper-based systems or no system at all, is about the same for high-income and developing countries. These systems are used for multiple purposes in most countries, including to access services, even if they may not be the only systems in operation. However, the similarities between high-income and developing countries mask important differences in the depth of use of digital technology across countries at different income levels.

In poor countries, civil registration records are still sometimes paper based, with birth, death, and other records bound in thousands of volumes and often dispersed across many centers. Although most national identification systems have shifted to digital databases, data capture and entry in low-income countries is often still paper based. Enrollment forms and supplemental documentation need to be scanned and the information entered manually into data records, increasing the possibility of errors. Information may not flow between databases; for example, deaths recorded by the civil registry may not be transmitted to the authority responsible for issuing ID cards so that those held by deceased people can be cancelled. Even when information is held digitally, sometimes there is no provision for seamless transmission from one data system to another. Systems also differ in terms of the attention paid to data security; some are highly advanced while others have only rudimentary protections in place.

Another frequently lagging area is the ecosystem for authenticating identities. Many of the countries that have deployed digital identification systems and sophisticated cards, often with costly security features, have not rolled out point-of-service devices able to read them, so that identity usually still must be verified through the visual inspection of a card, drawing on simple features such as photograph and signature. Some systems have introduced the capability to check the validity of cards against the central database—Kenya's Integrated Population Registration System (IPRS) reports responding to over one million such queries per day, largely from the financial sector. In most countries the emphasis is more on checking the validity of a credential than on rigorously verifying the identity of the person presenting it, either against the credential or, as in the case of India's Aadhaar, directly against the central database using biometrics.

Although developing countries may have caught up with high-income countries in terms of the percentage that have digital identification systems, they also lag in terms of more sophisticated features and opportunities for remote use. The share of digital ID cards embodying digital signatures is far higher in high-income countries, as is the share of e-ID systems used in practice

TABLE 1-1 The Spread of Digital Identification Systems, by Country Income Level

	Countries with no e-ID in use	Countries with e-ID	Digital signature embedded in e-ID card	e-ID used for remote online transactions
HICs	15	44	26	27
UMICs	11	44	11	7
LMICs	14	36	5	3
LICs	10	24	2	0
Total	50	148	44	37
of which: developing (all non-HICs)	35	104	18	10

Source: World Bank ID4D dataset, January 2016 edition.

HICs = high-income countries; UMICs = upper-middle-income countries; LMICs = lower-middle-income countries; LICs = low-income countries

to support remote online transactions. According to available information, no low-income country system offers these advanced capabilities (table 1-1).

This finding may not be surprising since a country's per capita income remains one of the strongest indicators of internet use despite rapid worldwide gains in connectivity. Pew's 2016 global survey found that a median of 87 percent of individuals in the 11 most advanced economies were internet users, compared with rates below 20 percent in some poor countries. As an example of this lag, Kenya, a leading country in the areas of mobile communications and banking, has rolled out a network of Huduma centers to provide decentralized access to e-services as part of its e-government initiative, but few of these centers have reliably stable broadband service to function effectively. Even as mobile internet infrastructure improves in the poorest regions of the world, the cost of data services remains a major constraint, putting these out of reach of the majority of the population (Pew Research Center 2016). Africa's two largest economies, South Africa and Nigeria, recorded internet use levels of only 42 and 39 percent, respectively, while 1 gigabyte (GB) of mobile data costs around US$5.3 in the former country and US$4.9 in the latter, substantial sums for most people.

Developing countries have thus moved rather quickly to adopt digital tech-

nology, but some of the gains are more superficial than real. Many will need substantial investments in digital infrastructure to complete the transition. They face formidable implementation challenges to build up their digital identification systems and the underlying databases and processes, as well as to put in place authentication ecosystems that are able to take full advantage of the capabilities offered by the new technologies.

From Identification to Development: Challenges and Risks

Despite their development potential and proliferation, identification programs are still controversial. Although countries may be converging toward a broadly similar model, there is no standard system for how identities should be managed or what an "ideal" identification system would look like. Some of the new systems represent a radical departure from traditional approaches to managing identity, in terms of their institutional arrangements as well as the technologies deployed to register and authenticate individuals and to coordinate the sharing of identity data for administrative purposes. There is considerable uncertainty about how these features will affect the development impact of a given system. Even those designed with user needs and development objectives in mind will likely need continuous adjustment as unintended consequences or limitations of the system come to light. Identification programs are also associated with a number of risks, including the erosion of privacy and the possible exclusion of those who are unable to satisfy tightening registration requirements. Wasteful spending on ID systems is also a problem—too often, expensive investments in high-tech identification infrastructure generate no returns as programs languish at low levels of coverage and provide few real opportunities for use.

There Is No Single Formula for Change . . .

Across countries, there are astonishing differences in how people are identified and how they can authenticate their identities, whether for real or virtual transactions. Some countries have strong foundational identification systems whose use is required for virtually all transactions. Others have multiple systems of varying quality serving different purposes. Still others have little in the way of identification infrastructure and issue only low-quality credentials, if

at all. ID credentials are also extremely varied; the only common global standard is for machine-readable travel documents issued by the International Civil Aviation Organization (ICAO).[17]

These differences reflect a host of initial conditions including administrative and technological capacity, past civil registration and identity management efforts, and the institutional and bureaucratic arrangements in place to provide identity services. They also reflect differences in social and political views. National identification systems accepted as normal and useful in some countries are political anathema in others. Some see a centralized, multiuse ID system as empowering, whereas others perceive it as a mechanism to reinforce the control of oppressive regimes. Indeed, many identification systems, even those now accepted as contributing positively to society, had their origins in repressive systems of control and surveillance. Breckenridge (2005) provides the example of South Africa's national population register, which was established to help control movement under the apartheid regime but now supports the administration of a comprehensive system of social grants. Spain offers another example. Its early forms of identification responded to the desire to exclude descendants of Moors and Jews from the Americas. The roots of the current ID system, initiated in 1951, lie in the institutionalized repression of Francoism (Clavell and Ouziel 2014). Today the system is accepted as a matter of course.

All OECD countries have well-established and comprehensive civil registries with birth registration rates at or close to 100 percent, but their arrangements for providing identification services vary. At one extreme is Estonia, which, as already noted, has probably the world's leading e-ID system with a vast array of public and private services provided via remote online access. It is built upon the central national population register and provides a unique ID number used by virtually all public and private service providers. Citizens and residents can use card-based or SIM-based mobile ID to access online services that include voting, submitting and checking tax returns, and starting a business; they can also sign documents digitally with the full legal authority of a handwritten signature. Access to many digital services has been extended to nonresidents through Estonia's e-Residency program, the first "global identification" system in the world.

One of several OECD countries at the other end of the identity management spectrum is the United States. It has no national identification system

17 For more information on the ICAO's Traveller Identification Programme, see the ICAO website at www.icao.int/Security/FAL/TRIP/Pages/default.aspx.

and issues no national credential. The best that most people can count on is a number issued by the Social Security Administration together with a simple paper card (no photo) and/or a state-issued driving permit. Only about 38 percent of citizens hold a passport. About 10 percent of citizens (and 25 percent of African Americans) do not hold any federal or state government-issued photo ID card (Gaskins 2011). The consequences include substantial losses from continuing identity theft and fraud, as well as partisan struggles over state-level efforts to impose photo ID requirements for voting, which are invariably challenged in the courts. In the United Kingdom, even though most of the population holds a driver's license (to drive, not as an identification document) or a passport (to travel), there is no specific credential that establishes or confirms a citizen's identity. Hospitality New Zealand's 18+ photo card is reputedly held not as a general proof of identity but for the specific purpose of proving that the holder is old enough to be allowed to consume alcohol.[18]

The differences in identity management systems are equally stark across less-developed countries. Some have comprehensive systems. During the past 20 years, Peru has created a multipurpose national registration and identification system with almost universal registration of adults and children. In opinion polls, RENIEC, its civil registration and identification agency, is among the most trusted institutions in the country (Reuben and Carbonari 2017). Pakistan has also created a comprehensive central system that is used for all identification purposes, including voting and the administration of social transfers to poor households. In Africa, Kenya has a well-developed though less technically advanced national ID system with origins that date back as far as 1920. Other African countries with long-established systems include Botswana, South Africa, and Zimbabwe. Rwanda and Uganda also have systems with high coverage, but have rolled out their current systems relatively recently. Some other countries, like Ghana, Nigeria, and Tanzania, have been attempting to roll out national ID systems for a number of years, but progress has been fitful, with slow gains in enrollment. Somalia and the Democratic Republic of Congo are examples of countries with still less-developed systems. The identification ecosystem in Somalia is fragmented and undeveloped. Very few births are registered, and there is no consistent countrywide system to establish and verify the identity of citizens. The most advanced system, for voter registration in

18 New Zealanders do, of course, virtually all have birth certificates and could present these to establish their age, but since they do not include a current photograph they do not alone provide credible proof of identity.

Somaliland, covers only between one and two million voters—a fraction of the estimated Somali population of 11.3 million.

In Asia, Malaysia contrasts with the Philippines. The former stands out as the first country to implement a comprehensive digital multiple-application national identification card; the MYKAD card can be used as a driving license, a library card, or a health records repository. Children above the age of 12 are issued a MYKID card as their own official identification document. In the Philippines, efforts to establish the national ID system as the basis for identification have stalled. People need to carry several credentials and permits (out of as many as 28 possibilities), and there are few rigorous cross-checks on the consistency of information. India's distinctive Aadhaar program has already been mentioned.

With such diverse starting points, there is no simple formula for strengthening identity management across all countries. Even though there are many common areas for action and certain universally applicable principles that should be followed, country needs and priorities differ. Some countries can build on a strong base; others need to consolidate diverse systems; still others are almost at the point of needing to start from scratch. The diversity of experience makes it even more important to draw lessons across systems to help shape individual country strategies, to strengthen the systems themselves, and also to understand how the systems can be used to support sustainable development.

. . . And Risks Must Be Recognized

There is widespread consensus on the relevance of civil registration and vital statistics systems and their essential features. In addition to providing a basis for identification, they provide essential statistical demographic and health information. Like statistical systems more generally, they often have not been adequately supported by national governments or their development partners, but this is not because the systems themselves are contentious. Their features have been codified by the UN Statistics Division in the form of handbooks and training manuals (UNSTATS 1998; UNSTATS 2002). Yet some details, such as the target age for birth registration or the role of paper records in an increasingly digital age, are debated.

There is much more debate around identification systems, especially those that facilitate the tracking of transactions and interactions. National population registers and government-issued national ID cards are common in the civil law countries of continental Europe, but have been rejected in many common

law countries like Australia, the United Kingdom, and the United States. Opponents of these national ID systems stress the risk of eroding privacy, arguing that the use of a single national identifying number for all transactions can help to merge individual records across many databases, potentially increasing the ease of surveillance (Hosein and Nyst 2013). Citing examples as diverse as Korea, Israel, and also highly publicized security breaches in the United States and other countries, critics also argue that large centralized identity databases create an irresistible honeypot for hackers. Another concern in some OECD countries is that the costs of such systems will outweigh the benefits of introducing them, especially in contexts where established systems are widely felt to work "well enough" for most people and most purposes. Some of the countries with strong opposition to a national ID system are at the forefront of efforts to create alternative modes of establishing and verifying identities that do not rely on a centralized identity database.

For developing countries, the rapid implementation of sophisticated ID programs raises even more pointed questions about benefits, risks, and costs. On one hand, as an increasing number of cases show (see chapter 3), the potential gains in terms of both individual inclusion and administrative efficiency are probably larger in lower-capacity developing countries than in rich ones. On the other hand, in settings with weak rule of law and limited independent oversight over government programs, identification systems will be more prone to misuse and less likely to offer high returns on what are often substantial investments of public funds. Although these risks must be recognized, there is little prospect of realizing the SDGs if countries are not able to strengthen their capacity to implement policies and programs and deliver services effectively. Neither will the SDGs be achieved if poor and vulnerable people are not able to participate in political, social, and economic life because they lack the recognized identity to do so.

The most relevant risks to the development-enhancing implementation of identification programs fall into three categories:

Exclusion. Vulnerable individuals and groups could be excluded if new ID systems are deployed and linked to various applications without considering their needs and limitations. The new systems may be too costly or difficult to access—for example, if registration involves high fees or lengthy travel to a registration office. Where remote authentication is required to access essential subsidies or services, beneficiaries could be seriously inconvenienced and even excluded if the quality of connectivity is too low to use

the system reliably. Manual workers who are unable to provide high-quality fingerprints for authentication could also be marginalized if no alternatives are made available. If the formalization of identity is associated with the formalization of national status, an unknown but considerable number of people face the prospect of statelessness.

Misuse. Many countries lack the legal and regulatory underpinnings to ensure that ID systems manage data securely and do not pose a threat to privacy. Only around half of all developing countries have data privacy protection laws that conform to global standards for fair information practices. Though the number is rising, those that do not have such a framework—or lack the capacity to implement its provisions—are mostly lower-income countries. The implementation of digital ID systems may pose particularly serious risks in countries where the rule of law is weak and there is little prospect for holding individuals, the government, or private entities accountable when personal data are accessed or used unlawfully. No system is completely proof against misuse, including identity theft, even if some appear to be more robust than others.

Ineffective investments. A further concern is the balance of benefits versus costs. ID systems require substantial investments as well as an ongoing operations budget. For a medium-size developing country, the costs of setting up the system and the initial enrollment phase alone can easily run into the hundreds of millions of dollars. The rapid expansion of technically sophisticated systems has not always taken place using the most suitable or cost-effective identification solutions. High-value technology procurements offer lucrative opportunities to both vendors and officials in client governments. Combined with weak oversight by national authorities as well as donors, this has helped to reinforce the natural bureaucratic tendency to work in silos. The consequence has often been costly and sometimes overengineered programs that are not interoperable with each other. Donor support for individual functional ID programs in the context of a specific operation may have reinforced fragmentation. Programs have sometimes been implemented under undue time pressure, increasing their cost. Voter registration programs are one such example; their expense (often around US$20 per voter per election) suggests that without generous continued donor support or a change in the model, elections will not be financially sustainable for some poor countries.

Nonetheless, in addition to supporting many SDGs and targets, effective and well-used ID programs should be high-return public investments for developing country governments. Not many ID applications have been fully assessed, but several appear to have generated a high rate of financial return. However, many countries have been wasting large sums in this area because of redundant programs, slow implementation, excessive costs, or simply because they have not used their ID programs to strengthen capacity and deliver services. Although to date there have not been any comprehensive assessments of the financial and economic benefits and costs of ID programs, these cases almost certainly would show negative rates of financial return to their investments, and probably also negative economic rates of return.

What Does the Identification Revolution Mean for Development Organizations?

Development partners have supported a wide range of identification programs. In a survey of 160 biometric ID programs of many different types, Gelb and Clark (2013a) found that at least half had been supported by development partners and donors. However, foundational identification, or the provision of multipurpose identification services, typically has not been supported as an end in itself. This may not be surprising in light of the Millennium Development Goals (MDGs), the precursor to the SDGs, which do not signify identity management as a broader strategic goal or legal identity as a development target. With the notable exception of the Inter-American Development Bank, which has a long record of support for civil registration and identification in Central and South America and the Caribbean, both IFIs and bilateral donors have viewed identification programs merely as a mechanism to help implement individual projects, depending on the donor's mandate.

In spite of their limitations, these fragmented projects have provided some useful experience. They have supported experimentation and innovation and have also provided "proof of concept" for the use of technically advanced approaches in low-income, fragile contexts. For example, as early as 2006, iris recognition was successfully used to help deliver demobilization payments to 110,000 ex-combatants in the Democratic Republic of Congo (Gelb and Decker 2011). Such an unsystematic and diverse engagement is perhaps inevitable in the early stages of work on a new area and with rapidly evolving technology, but it is now an opportune time to build on this experience to develop a more

integrated, forward-looking approach to managing identity in the context of development.

Development partners are beginning to establish such a strategic approach, and some other important initiatives are under way, such as the ID4Africa movement.[19] This is a promising start, but these initiatives are at an early stage and there is still a long way to go to develop a coordinated approach. The first step must be to work toward a common understanding of the ways in which identification systems should contribute to development. As discussed in more detail in chapter 7, some 21 organizations have endorsed a set of principles for the application of identification to development (Principles 2017). The 10 principles for the coverage, design, and governance of ID systems can serve as a valuable starting point for planning and implementing inclusive, robust, and trusted systems, as well as a benchmark for evaluating them (see box 1-1).

Considering the uncertainties, the fast-evolving identity management landscape, the close association of many programs with law enforcement and security, and the repressive origins of many identification systems, it would not be surprising if some development partners felt that the area poses too many risks to be involved in it. But this perspective sidesteps the challenge. By their nature, ID programs are multiple-use systems and multiple factors are propelling them forward. The practical question is not *whether* they should be implemented, but rather *how*, and how they should move forward in a way that maximizes their positive impact on sustainable development.

Summary Overview

As already emphasized, this is a fast-moving area and one with many large information gaps. It is still not possible to come to a definitive view on the impact of many new identification systems. Far more data collection and analysis is needed to understand their implications for the exercise of rights, for strengthening state capacity, for the functioning of markets and creation of new opportunities, and for sustainable development in general, as defined by the SDGs. Implementation and impact are high priorities, requiring careful

19 ID4Africa is now in its fourth year. Its 2017 meeting in Namibia followed annual conferences in 2015 and 2016 in Tanzania and Rwanda, respectively. The 2018 conference will take place in Abuja, Nigeria. For more information, see the program's website at www.id4africa.com/.

BOX 1-1 Principles on Identification for Sustainable Development

Inclusion: Universal Coverage and Accessibility

1. Ensuring universal coverage for individuals from birth to death, free from discrimination.
2. Removing barriers to access and usage and disparities in the availability of information and technology.

Design: Robust, Secure, Responsive, and Sustainable

3. Establishing a robust—unique, secure, and accurate—identity.
4. Creating a platform that is interoperable and responsive to the needs of various users.
5. Using open standards and ensuring vendor and technology neutrality.
6. Protecting user privacy and control through system design.
7. Planning for financial and operational sustainability without compromising accessibility.

Governance: Building Trust by Protecting Privacy and User Rights

8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.
9. Establishing clear institutional mandates and accountability.
10. Enforcing legal and trust frameworks through independent oversight and adjudication of grievances.

Source: Principles (2017).

monitoring and research as the frontier shifts from creating the new digital systems toward integrating them into a wide range of programs. This book could look quite different if it were written 10 years in the future. With these strong caveats, it nonetheless provides a concise picture of the evolving situation and sets out some of the choices that developing countries and their partners might consider.

Chapter 2 considers how to interpret "legal identity" from the perspective of sustainable development as encapsulated in the SDGs and estimates of the global identity gap. The size of this gap depends on how legal identity is defined in the development context. National status is not particularly relevant for many of the developmental applications of identification, but it is important not to ignore the dimension of nationality, particularly with the inclusive framing of the SDGs. Recognizing the ambiguities surrounding what constitutes an official proof of legal identity, the rest of chapter 2 summarizes evidence on the coverage of birth registration, national identification programs, and voter registration. There are many large data gaps, especially on the live coverage of national ID programs, and also some anomalies because similar credentials issued by different countries may not convey equal rights and privileges, either in-country or internationally. From the perspective of development, the identity gap is more a matter of the extent to which ID systems empower individuals, strengthen state capacity to administer programs, and create opportunities, rather than simply a matter of the numbers enrolled—although the extent of a program's coverage is nevertheless important information.

Chapter 3 provides an overview of the large number of SDGs and targets whose achievements will be closely related to individuals' ability to assert their identities as well as the presence of robust identification systems to facilitate the effective delivery of services and programs. Not all of these applications rest on having one single ID system for every purpose, but robust and inclusive ID programs can support progress across a wide range of areas, including access to financial and economic resources, gender equality and empowerment, social protection, and tax collection. But will even effective ID programs be used for the highest-payoff applications? The potential risks and barriers will be discussed in more detail in chapter 5.

Chapter 4 considers five areas of innovation in identification systems, focusing on transformative applications of technology and new approaches to the institutional architecture of identification services. The first three areas are driven primarily by advances in digital technology. The first area is biometric technology, which has revolutionized the provision of identity services in developing countries, particularly those with weak underlying civil registration systems. Digital biometrics are certainly not a solution on their own and they introduce their own concerns and vulnerabilities, but their use is instrumental to the achievement of many of the identification-linked development outcomes described in chapter 3. Technology is also at the heart of the second innova-

tion, the "identity first" approach pioneered by India's Aadhaar program. This offers many lessons for other countries even if they do not adopt the entire model. Steadily advancing technology is also disrupting the identification of infants and young children, by making it possible to "lock in" identification at ever-earlier ages to provide a unique "identity for life." This has the potential to strengthen identity management and reduce fraud arising from registration later in life, while also increasing the importance of ensuring that civil (birth) registration and identification work in an integrated way. The remaining two areas concern institutional innovations and options in the architecture of ID systems. Arrangements for providing identification services, both civil registration and national identification, differ across countries. In an effort to streamline identification services and build trust in their provision, a number of countries have established autonomous public agencies with the specific and limited mandate to provide foundational national identification. Autonomy offers advantages, but also raises important questions about the governance structure of the ID system and how it should be financed, if it is not included in the budget of a government ministry. The final question is that of integration—the degree to which the country operates a single integrated identity management system—and the paths taken to get there. Some countries are working to integrate their systems through "reverse engineering," whereby one or more high-coverage functional ID registries are transformed to become the basis for a multipurpose, foundational program. Such an approach further raises the importance of common technical standards. Even if the current fragmentation of ID systems is mainly transitional rather than a coherent policy choice, countries may still have different views on how integrated their ID system(s) should be and whether "one number for everything" is the way they want to go.

Chapter 5 considers the three broad categories of risks identified above: exclusion, misuse of personal data, and ineffective investments. Identification systems are not necessarily themselves the source of these risks; data privacy, for example, is threatened by the growth of large databases in countries with and without national ID systems. However, under some conditions these systems can exacerbate existing risks as well as introduce new ones.

Looking to the future, chapter 6 summarizes five cases of particular relevance for their institutional innovations and their use of technology: the multipurpose identification systems of Peru, Estonia, and India (Aadhaar); the United Kingdom's federated ID system for online verification; and the potential of social networks for providing digital identities. (Many other programs

also have valuable lessons to offer.) The first three cases offer interesting lessons for centralized ID systems. Starting from a civil registration and ID system greatly damaged by the Shining Path insurgency, Peru set out to identify its people as a priority for national reconstruction. It has created one of the strongest and most integrated ID systems in the world with an institutional and financial model that can be relevant to many countries. Estonia has been the world's leader in e-ID. Proving that digital identity knows no boundaries, it has also extended its service to nonresidents through the e-Residency program to provide the world's first global service. As mentioned earlier, India's unique identification or Aadhaar program is truly unique in multiple dimensions and offers lessons for many other countries. The other two cases, GOV.UK Verify and social networks, are more speculative but offer some intriguing prospects. Neither provides "foundational" legal identity or can be considered as the "first stage" option for poor countries seeking to establish an identity baseline and mechanisms to authenticate against it. Indeed, they demonstrate the difficulty of managing identities without some such foundational system, even if it is not a fully integrated one. However, they raise the important point that identity assurance need not always be "gold plated," but can be calibrated to the needs of the particular application at hand.

Chapter 7 concludes with the implications for designing and implementing identification systems that can work as effective tools for achieving the SDGs, while ensuring that risks are mitigated. Countries and development partners are evolving toward a more strategic approach on this front, but it is still early days. The first step is to reach agreement on a set of common principles, which this chapter presents by drawing on the previously discussed cases and examples. It also considers some further necessary steps and the need for more research on the functioning, use, and impact of the rapidly evolving systems of identification, particularly in developing countries.