McKinsey Global Institute

Executive summary

Digital identification

A key to inclusive growth

April 2019

McKinsey Global Institute

Since its founding in 1990, the McKinsey Global Institute (MGI) has sought to develop a deeper understanding of the evolving global economy. As the business and economics research arm of McKinsey & Company, MGI aims to provide leaders in the commercial, public, and social sectors with the facts and insights on which to base management and policy decisions.

MGI research combines the disciplines of economics and management, employing the analytical tools of economics with the insights of business leaders. Our "micro-to-macro" methodology examines microeconomic industry trends to better understand the broad macroeconomic forces affecting business strategy and public policy. MGI's in-depth reports have covered more than 20 countries and 30 industries. Current research focuses on six themes: productivity and growth, natural resources, labor markets, the evolution of global financial markets, the economic impact of technology and innovation, and urbanization. Recent reports have assessed the digital economy, the impact of AI and automation on employment, income inequality, the productivity puzzle, the economic benefits of tackling gender inequality, a new era of global competition, Chinese innovation, and digital and financial globalization.

MGI is led by three McKinsey & Company senior partners: Jacques Bughin, Jonathan Woetzel, and James Manyika, who also serves as the chairman of MGI. Michael Chui, Susan Lund, Anu Madgavkar, Jan Mischke, Sree Ramaswamy, and Jaana Remes are MGI partners, and Mekala Krishnan and Jeongmin Seong are MGI senior fellows.

Project teams are led by the MGI partners and a group of senior fellows and include consultants from McKinsey offices around the world. These teams draw on McKinsey's global network of partners and industry and management experts. The MGI Council, which includes leaders from McKinsey offices around the world and the firm's sector practices, includes Michael Birshan, Andrés Cadena, Sandrine Devillard, André Dua, Kweilin Ellingrud, Tarek Elmasry, Katy George, Rajat Gupta, Eric Hazan, Acha Leke, Scott Nyquist, Gary Pinkus, Sven Smit, Oliver Tonby, and Eckart Windhagen. In addition, leading economists, including Nobel laureates, advise MGI research.

The partners of McKinsey fund MGI's research; it is not commissioned by any business, government, or other institution. For further information about MGI and to download reports, please visit www.mckinsey.com/mgi.

Digital identification: A key to inclusive growth

Executive summary

April 2019

Authors
Olivia White, San Francisco
Anu Madgavkar, Mumbai
James Manyika, San Francisco
Deepa Mahajan, Silicon Valley
Jacques Bughin, Brussels
Michael McCarthy, London
Owen Sperling, San Francisco

In brief

Digital identification: A key to inclusive growth

Digital identification, or "digital ID," can be authenticated unambiguously through a digital channel, unlocking access to banking, government benefits, education, and many other critical services. Programs employing this relatively new technology have had mixed success to date—many have failed to attain even modest levels of usage, while a few have achieved large-scale implementation. Yet well-designed digital ID not only enables civic and social empowerment, but also makes possible real and inclusive economic gains—a less well understood aspect of the technology. The political risks and benefits of digital ID are potentially significant and deserve careful attention but are beyond the scope of this report. Here, we develop a framework to understand the potential economic impact of digital ID, informed by an analysis of nearly 100 ways in which digital ID can be used in Brazil, China, Ethiopia, India, Nigeria, the United Kingdom, and the United States. We find:

— Digital ID is a foundational set of enabling technologies that can be pivotal in a wide range of interactions between individuals and institutions. Digital ID technologies are also akin to "dual use" technologies that can be employed both to benefit society and for undesirable purposes by governments, institutions, or individual actors. Our research focuses on how "good" use of digital ID can create value and societal benefit, while being clear-eyed about the chance of misuse and other risks, and the need to mitigate them.

— Digital ID enables individuals to unlock value and benefit as they interact with firms, governments, and other individuals in six roles: as consumers, workers, microenterprises, taxpayers and beneficiaries, civically engaged individuals, and asset owners. For example, digital ID could contribute to providing access to financial services for the 1.7 billion-plus individuals who are currently financially excluded, according to the World Bank, and could help save about 110 billion hours through streamlined e-government services, including social protection and direct benefit transfers. Institutions, for example, could benefit from improved customer registration, reducing onboarding costs by up to 90 percent, and reduced payroll fraud, saving up to $1.6 trillion globally.

— In our seven focus countries, extending full digital ID coverage could unlock economic value equivalent to 3 to 13 percent of GDP in 2030—if the digital ID program enables multiple high-value use cases and attains high levels of adoption and usage. The potential varies by country based on the portion of the economy with bottlenecks that digital ID can address as well as the scope for improvement in formalization, inclusion, and digitization. Not all of these potential sources of economic value may translate into GDP, although we use GDP as a base to give a sense of the order of magnitude of impact possible.

— For emerging economies, while the share of the economy that digital ID can address tends to be modest, scope for improvement can be sizable, leading to average potential per-country benefit of roughly 6 percent of GDP in 2030. Much of this value could be captured through digital ID with authentication alone. For mature economies, many processes are already digital, so the potential for improvement is more limited and largely requires digital ID programs that enable additional data-sharing features. Average per-country benefit of 3 percent could be possible, assuming high usage rates.

— Just over half of the potential economic value of digital ID could accrue to individuals, making it a powerful key to inclusive growth, while the rest could flow to private-sector and government institutions. Beyond quantifiable economic benefits, digital ID can offer noneconomic value to individuals through social and political inclusion, rights protection, and transparency. For example, robust identity programs could help guard against child marriage, slavery, and human trafficking.

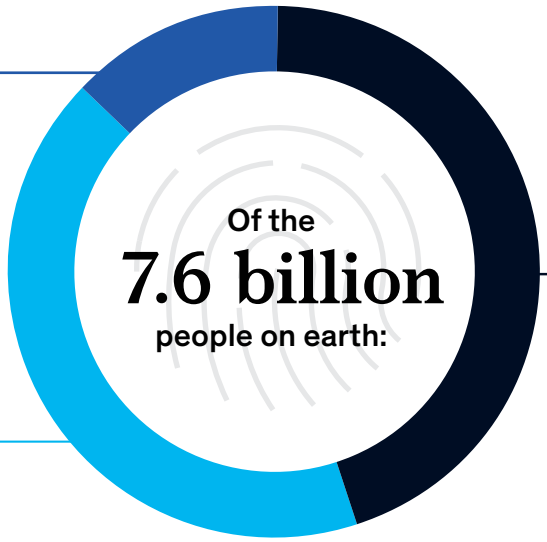
— Capturing the value of good digital ID is by no means certain or automatic. Careful system design and well-considered government policies are needed to promote uptake, mitigate risks like those associated with large-scale capture of personal data or systematic exclusion, and guard against the challenges of digital ID as a potential dual use technology.

What is good digital ID?

Good digital ID is identification that is verified and authenticated to a high degree of assurance over digital channels, is unique, is established with individual consent, and protects user privacy and ensures control over personal data.

1 billion
people are estimated to lack a legally recognized form of ID

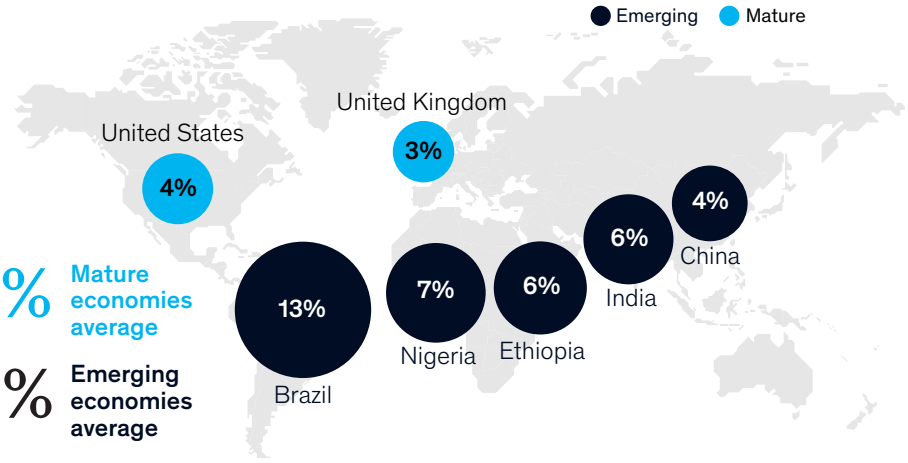
3.2 billion
have some form of ID and a digital trail



3.4 billion
people have some form of ID but no digital trail

Unlocking global economic value

Across our focus countries, digital ID could unlock economic value equivalent of 3–13% of GDP in 2030.



3% Mature economies average

6% Emerging economies average

65%

of potential value could accrue to individuals on average in emerging economies in our focus group, making it a powerful tool for inclusive growth.

Potential for misuse and possible risk elements

While digital ID can reduce risks associated with conventional ID programs, such as manual error, it could be ...

... **misused without the proper controls**, akin to dual-use technologies such as social media, GPS, or even nuclear energy.

... **exposed to risks already present** in any digital technology with large-scale population-level usage such as system failures, cybersecurity breaches, and privacy violations.

... **potentially exposed to some risks** found in conventional ID programs such as the exclusion of individuals.

Note: Value estimates assume the digital ID program enables multiple high value use cases, attains high levels of usage, is established with individual consent, and protects user privacy and ensures control over personal data.

Source: World Bank; ID4D; We Are Social *Global Digital Report 2018;* ITU; WDI; Findex; McKinsey Global Institute Analysis

McKinsey Global Institute


Please
Sign

Executive summary

It is easy to take identification for granted, particularly in mature economies.[1] However, close to one billion people in the world have no form of legal identification and may be denied access to critical government and economic services.[2] The rest of the world's inhabitants, about 6.6 billion people, either have some form of identification but limited ability to use it in the digital world, or are active online but face growing complexity that makes it hard to keep track of their digital footprint securely and efficiently. Digital identification, or "digital ID," could help all three groups authenticate their identity through a digital channel, unlocking access to the digital world in the economic, social, and political realms (see Box E1, "What is digital ID?").

In this report, we take a comprehensive approach to understanding the potential economic value created by "good" digital ID for both individuals and institutions, while highlighting the potential for misuse and other challenges and risks. We establish a clear framework characterizing the ways digital ID can be used, which can help identify potential sources of value from digital ID, informing decisions about how it should be implemented and to what purpose. Our estimate of potential value builds upon nearly 100 ways digital ID can be used and deep-dive analysis of seven diverse economies—Brazil, China, Ethiopia, India, Nigeria, the United Kingdom, and the United States. We also take into account previous MGI research focused on the digital economy as well as MGI analysis of sectors and geographies.[3]

In our seven focus countries, we find that digital ID has the potential to unlock economic value equivalent to 3 to 13 percent of GDP in 2030, assuming high adoption rates. The range of potential value depends on the portion of economic activity where digital ID–based use cases could be deployed to address bottlenecks and inefficiencies, as well as the scope for improvement in formalization, inclusion, and digitization over current levels. Based on these considerations, we estimate that among emerging economies, the average country could achieve economic value equivalent to 6 percent of GDP in 2030, while in mature economies, the average country could achieve economic value equivalent to roughly 3 percent—both assuming high levels of adoption and use in multiple domains.

High adoption of digital ID is possible but not automatic. So far, digital ID programs implemented by both national governments and private companies have had adoption rates ranging from single-digit levels to over 90 percent in a few cases. Yet good digital ID programs, implemented thoughtfully, offer significant inclusion benefits and higher standards of privacy and security with limited costs. When scaled to high adoption rates across multiple use cases, the economic value to individuals and institutions could be significant. Despite its mixed success so far, digital ID can represent an important key to unlocking inclusive growth.

Digital ID can unlock value by promoting inclusion, formalization, and digitization

According to estimates from the World Bank's ID4D database, almost one billion people globally lack any form of legally recognized identification. An additional 3.4 billion who have some type of legally recognized identification have limited ability to use it in the digital world. The remaining 3.2 billion have a legally recognized identity and participate in the digital economy but may not be able to use that ID effectively and efficiently online (Exhibit E1). Digital ID holds the promise of enabling economic value creation for each of these three groups by fostering increased inclusion, which provides greater access to goods and services; by increasing formalization, which helps reduce fraud, protects rights, and increases transparency; and by promoting digitization, which drives efficiencies and ease of use.

---

1 Throughout this paper, we use the term "mature economies" to mean economies that are classified by the World Bank as high-income countries; the term "emerging economies" includes all others.

2 Global ID4D Dataset, World Bank, 2018.

3 *Digital finance for all: Powering inclusive growth in emerging economies,* McKinsey Global Institute, September 2016; *A labor market that works: Connecting talent with opportunity in the digital age,* McKinsey Global Institute, June 2015; *The age of analytics: Competing in a data-driven world,* McKinsey Global Institute, December 2016.

Box E1.

What is digital ID?

Unlike a paper-based ID such as most driver's licenses and passports, a digital ID can be authenticated remotely over digital channels. We adopt this outcome-based definition of digital ID, regardless of the ID-issuing entity. For example, a digital ID could be issued by a national or local government, by a consortium of private or nonprofit organizations, or by an individual entity. Our definition also applies regardless of the specific technology used to perform digital authentication, which could range from the use of biometric data to passwords, PINs, or smart devices and security tokens.

Furthermore, this report specifically examines "good" digital ID, which we refer to throughout this report as "digital ID." Good digital ID requires the following four attributes:

— **Verified and authenticated to a high degree of assurance.**[1] High-assurance digital ID meets both government and private-sector institutions' standards for initial registration and subsequent acceptance for a multitude of important civic and economic uses, such as gaining access to education, opening a bank account, and establishing credentials for a job. High-assurance authentication maintains these same standards each time the digital ID is authenticated. This attribute does not rely on any particular underlying technology. A range of credentials could be used to achieve unique high-assurance authentication and verification, including biometrics, passwords, QR codes, and smart devices with identity information embedded in them.

— **Unique.** With a unique digital ID, an individual has only one identity within a system, and every system identity corresponds to only one individual. This is not characteristic of most social media identities today, for example.

— **Established with individual consent.** Consent means that individuals knowingly register for and use the digital ID with knowledge of what personal data will be captured and how they will be used.

— **Protects user privacy and ensures control over personal data.** Built-in safeguards to ensure privacy and security while also giving users access to their personal data, decision rights over who has access to that data, with transparency into who has accessed it.

Our understanding of good ID was informed by extensive consultations with our research collaboration partners Omidyar Network, the Open Society Foundations, and the Rockefeller Foundation. We also conducted in-depth discussions on the opportunities and challenges associated with digital ID with experts from the Bill & Melinda Gates Foundation, the Center for Global Development, iSPIRT, the United Nations Development Programme, the World Bank Group's ID4D initiative, and the World Economic Forum.

Digital ID can form the foundation of a host of applications in many aspects of an individual's life, work, and social interactions. The potentially pervasive nature of digital ID makes it akin to dual use technologies—like nuclear energy and GPS—that are designed to generate benefit but are also capable of being used for harmful or undesirable purposes.[2] For example, a government might misuse digital ID programs by deploying them for political and social control, while a private-sector firm might misuse digital ID for commercial gain by influencing consumers in ways that they do not understand or desire. The nature of this trade-off for information technology broadly is explored in a range of academic literature. Examples include *The Dark Side of Digital Technology*, by Peter Townsend (Oxford University Press, 2017), and *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, edited by Colin J. Bennett and David Lyon (Routledge, 2008), which focuses on identification.

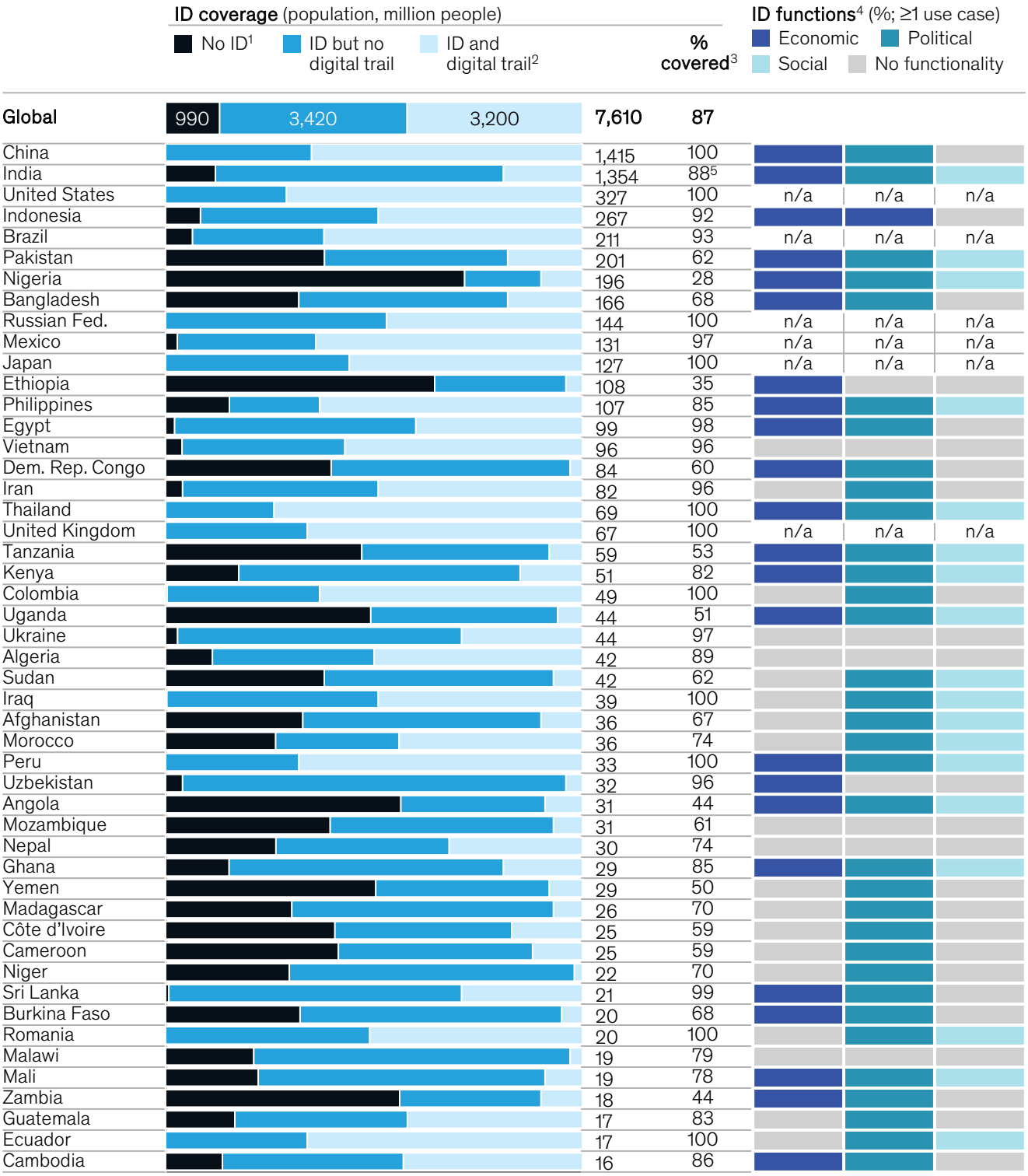
In this report, we *focus on the potential of good digital ID* to create value. The attributes of good ID, including high *assurance and consent-based creation and use, promote trust and protect privacy.* The design and governance of digital ID programs should incorporate these attributes and guard against the potential for misuse, to avoid outcomes contrary to the best interests of users.

[1] Verification means to check that an individual's underlying information establishes his or her identity and occurs during initial registration of a digital ID or updating of an individual's information in the ID system. Authentication means the process of validating an identity previously established during the registration process and occurs when an individual uses his or her ID with requesting parties.

[2] Koos van der Bruggen, "Possibilities, intentions and threats: Dual use in the life sciences reconsidered," *Science and Engineering Ethics*, 2011, Volume 18, Issue 4, pp. 741–56.

Exhibit E1

Across the globe, one billion people lack ID, and existing ID schemes vary widely.



1. "No ID" population figures are based on World Bank ID4D reporting of the latest registration levels for national ID, with voter registration used as a proxy where national ID does not exist or data are not available. Where available registration data exceed population or where data are limited, as in China, this number is set to zero. It is also reported as zero in all high-income countries that have a birth registration rate of over 99.9% (United States, Japan, and United Kingdom in this table). The World Bank's ID4D global data set was created to measure the scale of the overall global identification gap; estimates for individual economies are subject to considerable uncertainty.
2. Calculated as population with active social media use, as reported in the We Are Social *Global Digital Report 2018*. These social media users are presumed to have some form of legally recognized ID.
3. Percentage of total population that has an ID.
4. Data from International Telecommunication Union analysis based on review of academic and gray literature for 48 conventional and digital national identity programs or initiatives across 43 countries (includes two programs for each of Burkina Faso, Cambodia, Nigeria, Ukraine, and Zambia) to determine which use cases they are connected to, out of 18 functions identified. We have grouped these functions into three categories: economic (eg, financial services KYC), political (eg, voting), and social (eg, health services).
5. This percentage does not include individuals who adopted Aadhaar digital ID in the second half of 2018; according to data from the Unique Identification Authority of India, Aadhaar covered ~90% of the population as of January 2019.

Source: World Bank ID4D; ITU; We Are Social; McKinsey Global Institute analysis

Digital ID benefits a wide range of individuals, from those who lack ID to those who have ID but cannot use it effectively in the digital world

For the estimated one billion people globally who lack any form of legally recognized identification, digital ID represents a path to rapid inclusion by helping to provide access to critical government and economic services that they may currently be denied, including financial services, government benefits, and labor markets.[4] For example, of the roughly 1.7 billion people without a bank account in 2017, nearly one in five attributed the situation to a lack of necessary identification documents.[5] Women disproportionately lack identification in low-income countries, contributing to their higher levels of exclusion. For example, 45 percent of women over the age of 15 lack identification in low-income countries, compared with only 30 percent of men.[6]

Digital ID also unlocks new opportunity for the 3.4 billion individuals who have some form of high-assurance ID but limited ability to use it in the digital world.[7] Moving from purely physical ID to digital ID programs, and creating digital infrastructure and applications that use digital ID for authentication, could enable these users to take advantage of the efficiency and inclusion benefits that digital interactions offer. Examples include more convenient services, such as e-government, and improved sharing of personal information, such as medical data. Digital ID can also provide the convenience of a multiuse form of identification, not a feature of many conventional national identity programs today. For example, a 2016 study of 48 national identity programs found that very few could be used in a wide variety of sectors.[8]

3.4b

People who have some form of ID but limited ability to use it in the digital world

Finally, good digital ID has the potential to benefit most of the 3.2 billion individuals who are already active in the digital world by facilitating greater user control of data, privacy protections, security for online interactions, and reduced friction in managing online accounts. Individuals around the world have significant privacy-related concerns that high-assurance digital ID could help address.[9] Low-assurance interactions contribute to the potential of cybersecurity breaches, which pose increasing risk for the digital economy. For example, in 2017, $16.8 billion was lost in the United States due to identity fraud, and since 2013, more than 6.2 billion customer data records have been breached in the United States alone.[10] Security concerns aside, many internet users struggle to keep track of their digital footprint—costing time and money—and could benefit from the greater control and integrity that a digital ID could enable. For example, one study found that about 30 percent of calls to banks' call centers were requests for account access due to misplaced or forgotten passwords.[11] Further, by enabling improved user control of digital footprints, digital ID can also facilitate institutional adoption of and compliance with data privacy regulations such as GDPR.

Forty or more national or non-national digital identity programs exist today (Exhibit E2). Roughly 1.2 billion people with digital IDs live in India and are registered in the Aadhaar program, which began in 2009. Yet many digital ID programs have only achieved low coverage levels, with the percentage of the population included as low as single digits, and most enable only a small fraction of the nearly 100 ways we have identified that digital ID can be used. As a result, most existing digital ID programs do not yet capture all potential value; additional opportunity exists for greater value creation.

4 The United Nations General Assembly incorporated identification coverage for all by 2030 into the 2015 Sustainable Development Goals.
5 *Global Findex Database 2017: Measuring financial inclusion and the fintech revolution*, World Bank, 2018.
6 *ID4D-Findex survey data 2017*, World Bank.
7 The population with access to the digital world is proxied by active social media users, captured in the We Are Social *Global Digital Report 2018*.
8 *Review of national identity programs,* International Telecommunication Union, May 2016.
9 Several bodies of digital ID research have focused on privacy-related requirements and guidelines. These include *Identities: New practices in a connected age,* Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2017; *Digital Identity: Issue Analysis,* Consult Hyperion, June 2016, identitiesproject.com.
10 *Better identity in America: A blueprint for policymakers,* The Better Identity Coalition, July 2018; *Inside Out Security,* "The world in data breaches," blog entry by Rob Sobers, July 16, 2018, varonis.com/blog/the-world-in-data-breaches.
11 *The future of identity in banking*, Accenture, 2013.

Exhibit E2

Digital ID systems operate around the world.

Examples of digital ID systems can be found in Argentina, Canada, Estonia, India, Nigeria, Sweden, and the United Kingdom[1]

SecureKey Concierge, Canada
~50% adoption
- Federated system launched in 2012 led and operated by financial institutions
- Enables authentication only with a range of public- and private-sector institutions through online login

UK Verify, United Kingdom
<10% adoption
- Federated system launched in 2016 by public sector, with private identity providers
- Enables authentication with a set of public-sector departments through online login

BankID, Sweden
~75% adoption
- Launched in 2003 by financial institutions, now recognized by the government
- Enables digital authentication and signature with limited data sharing for use with public- and private-sector institutions through smart card or digital device (mobile or computer)

e-ID, Estonia
>90% adoption
- Launched by public sector in 2000, with over 940 public- and private-sector institutions connected today
- Facilitates authentication, data storage and sharing, and digital signature through chip-based card or digital keys

Mobile Connect, global
- Launched in 2014 by GSMA, and now provided by 52 mobile operators in 29 countries
- Enables mobile operator–facilitated, user-controlled authentication and data-sharing functionality, with applications including e-commerce, e-government, and banking

Digital Identification System (SID), Argentina
<10% adoption
- Recently launched by government in coordination with private sector
- Will enable remote biometric authentication across public- and private-sector services

National eID, Nigeria
<10% adoption
- National eID card launched by public sector in partnership with Mastercard in 2014
- Enables authentication through chip-based card and data sharing for KYC, with potential additional future use cases under consideration

Aadhaar, India
>90% adoption[2]
- Launched in 2009 by agency established by public sector
- Enables biometric digital authentication as part of broader digital ecosystems with additional functionality
- Key use cases include direct transfer of benefits to bank accounts, e-KYC, digital document storage

1. All details provided reflect a snapshot in time based on latest available published figures and policies, ranging from April 2017 to January 2019.
2. Adoption figures reflect data from the Unique Identification Authority of India (UIDAI) as of January 2019.

Source: GSMA.com; BankID.com; Securekeyconcierge.com; Gov.uk; E-estonia.com; Argentina.gob.ar; Nimc.gov.ng; Uidai.gov (updated as of 1/2/2019); McKinsey Global Institute analysis

Technology needed to expand digital ID exists and is growing ever more affordable

The opportunity for value creation through digital ID is growing as technology improves, implementation costs decline, and access to smartphones and the internet increases daily. The foundational digital infrastructure that supports digital ID grows in reach and drops in cost every day. More than four billion people currently have access to the internet, and nearly a quarter-billion new users came online for the first time in 2017. Africa is experiencing the fastest growth rates in internet usage, with a 20 percent increase each year.[12] Meanwhile, the price of a smartphone, the primary entry point for access to the internet in many emerging markets, fell by 20 to 30 percent in most emerging economies between 2008 and 2016.[13]

20%

The annual growth in internet usage in Africa

The technology needed for digital ID is now ready and more affordable than ever, making it possible for emerging economies to leapfrog paper-based approaches to identification.[14] Biometric technology for registration and authentication is becoming more accurate and less expensive.[15] For example, iris-based authentication technologies can give false rejection rates as low as 0.2 percent and false acceptance rates of 0.0001 percent.[16] The average selling price of a fingerprint sensor found in a mobile phone fell by 30 percent in 2017 alone.[17] Bar codes on cards, which once stored only numerical data, can now secure signature, fingerprint, or facial data.[18] Blockchain technologies, with appropriate design and governance, could potentially help decentralize information storage so there is no single point of failure in case of cyberintrusion or internal fraud.[19]

Digital ID has the potential to be used for good or for bad, and comes with risks even when intended for shared value creation

Digital ID, much like other technological innovations such as nuclear energy and even the ubiquitous GPS, can be used to create value or inflict harm. Without proper controls, digital ID system administrators with nefarious aims, whether they work for private-sector firms or governments, would gain access to and control over data. History provides ugly examples of misuse of traditional identification programs, including tracking or persecuting ethnic and religious groups. Digital ID, if improperly designed, could be used in yet more targeted ways against the interests of individuals or groups by government or the private sector. Potential motivations could include financial profit from the collection and storage of personal data, political manipulation of an electorate, and social control of particular groups through surveillance and restriction of access to uses such as payments, travel, and social media. Thoughtful system design with built-in privacy provisions like data minimization and proportionality, well-controlled processes, and robust governance, together with established rule of law, are essential to guard against such risks.[20]

Yet even when digital ID is used expressly for creating value and promoting inclusive growth, risks of two major sorts must be addressed. First, digital ID is inherently exposed to risks already present in other digital technologies with large-scale population-level usage. Indeed, the connectivity and information sharing that create the value of digital ID also contribute to potential dangers. Whether data breaches at credit agencies or on social media, failure of technical systems, or concerns over the control and misuse of personal data, policy makers around the world today are grappling with a host of potential new dangers related to the digital ecosystem. Technological failure could include problems with the functionality of

[12] *Global Digital Report 2018*, We Are Social, January 2018; *Technology Landscape for Digital Identification*, Identification for Development, World Bank, 2017.
[13] *The 2015–16 affordability report*, Alliance for Affordable Internet, 2016.
[14] Luda Bujoreanu, Anita Mittal, and Wameek Noor, "Demystifying technologies for digital identification," World Bank, February 27, 2018.
[15] *Technology landscape for digital identification*, Identification for Development, World Bank, 2017.
[16] Ibid.
[17] Chris Burt, "Fingerprint Cards reports cost cutting and changing focus after tough 2017," BiometricUpdate.com, February 9, 2018; Danny Thakkar, *Biometric devices: Cost, types, and comparative analysis*, Bayometric.
[18] Ibid.
[19] *Blockchain technology overview,* National Institute of Standards and Technology, US Department of Commerce, https://doi.org/10.6028/NIST.IR.8202.
[20] The World Bank Group and the Center for Global Development have developed ten principles on identification for sustainable development. They are endorsed by many organizations, such as the Bill & Melinda Gates Foundation and Omidyar Network, and provide guidelines for managing the downsides and promoting sustainable development of a digital ID.

163zb

The forecast size of the global datasphere by 2025

the hardware or software associated with a digital ID as well as infrastructure problems preventing uninterrupted and effective system use. Cybersecurity threats also pose an increasing risk across the digital ecosystem, and digital ID programs are no exception. The number of accounts online and the amount of data created are rapidly increasing. The International Data Corporation forecasts that by 2025 the global datasphere will grow to 163 zettabytes (one zettabyte is a trillion gigabytes), ten times the level in 2016.[21] In addition, shifting regulations and consumer preferences are placing increasing emphasis on data privacy and control for all digital systems. Examples of new privacy measures include the General Data Protection Regulation in the EU, the California Consumer Privacy Act in the United States, the Data Privacy Act of 2012 in the Philippines, and South Korea's Personal Information Protection Act.

Second, some risks associated with conventional ID programs also pertain to digital ID. They include human execution error, unauthorized credential use, and the exclusion of individuals. Digital ID could meaningfully reduce those risks by minimizing opportunity for manual error or breaches of conduct. For example, for conventional ID programs, reconciliation of data between databases may be impossible or error prone, while digital ID programs can more readily integrate data sources and implement data quality checks and controls. High-assurance digital ID programs also reduce the risk of forgery and unauthorized use, which are relatively easier with conventional IDs, like driver's licenses and passports. Furthermore, some risks associated with conventional IDs will manifest in new ways as individuals use digital interfaces. For example, individuals without sufficient technological access or savvy and those who do not trust a digital ID system could be completely excluded, unless alternative manual options also exist.

Individuals and institutions can benefit from digital ID in a range of interactions

Individuals can use identification to interact with businesses, governments, and other individuals in six roles: as consumers, workers, microenterprises, taxpayers and beneficiaries, civically engaged individuals, and asset owners (Exhibit E3). Correspondingly, institutions can use an individual's identity in a variety of positions: as commercial providers of goods and services, interacting with consumers; as employers, interacting with workers; as public providers of goods and services, interacting with beneficiaries; as governments, interacting with civically minded individuals; and as asset registers, interacting with individual asset owners. In our analysis, we quantify the benefits of digital ID through bottom-up microanalysis of nearly 100 ways of using digital ID, organized by the roles played by individuals and institutions (see Box 3, "Our methodology," and the technical appendix).

Individuals benefit most from increased access to financial services and employment

The four largest contributors to direct economic value for individuals globally are increased use of financial services, improved access to employment, increased agricultural productivity, and time savings.

— **Increased use of financial services.** Digital ID helps individuals meet Know Your Customer (KYC) requirements and enables remote customer registration for financial services.[22] According to the World Bank, lack of documentation, distance to financial institutions, and cost of financial services are each cited by 20 to 30 percent of respondents as a reason for not having access to a bank account.[23] We estimate that in Brazil, for example, digital ID could help 39 million adults improve access to financial services and facilitate increased extension of credit to both individuals and micro, small, and medium-size enterprises (MSMEs).[24]

— **Improved access to employment.** Better digital talent matching and contracting platforms are enabled by digital ID programs, which allow job seekers to authenticate

[21] *Data age 2025: The evolution of data to life-critical*, Seagate, March 2017.
[22] Ibid.
[23] *ID4D-Findex survey data 2017*, World Bank.
[24] *ID4D-Findex survey data 2017*, World Bank; World Development Indicators 2018, World Bank.

themselves online. Such platforms could streamline access to labor markets for inactive and unemployed workers. The combination of identification coverage and high-assurance digital platforms could also boost labor productivity. For example, we estimate a 1.8 percent boost in productivity for existing workers in Nigeria from increased access to formal labor markets and better matching of skills with jobs. As a result, both workers and microproducers could see higher earnings.

— **Greater agricultural productivity from formalized landownership.** By enabling formal land titling, digital ID could help improve incentives to make larger and longer-term investments in farming. This could increase farm yields by roughly 10 percent. In Nigeria, agriculture represents approximately 21 percent of GDP, but nearly 90 percent of land titles are not formally registered.[25] Agricultural output could increase by as much as 8 percent if 90 percent of farmers utilize digital ID to formalize land titles by 2030. Digital ID could also bring benefits to farmers through better targeting of agricultural support, including through crop insurance or agricultural subsidies, especially when combined with location information and remote sensing.

— **Time savings.** Digitization of sensitive identity-related interactions enables process streamlining and automation while reducing the need for travel, a particular benefit for people who live in rural areas. For example, in Estonia, digital ID today enables voting online, saving 11,000 working days per election.[26] Digital ID also could facilitate streamlined tax filing by providing the ability to connect information across sectors to prepopulate forms, while separately saving time for tax departments in processing and auditing.

90%

The potential cost reduction in customer onboarding from digital ID

Both private and public institutions benefit most from cost savings and reduced fraud

The five largest sources of value for institutions—in both government and the private sector—are cost savings, reduced fraud, increased sales of goods and services, improved labor productivity, and higher tax revenue.

— **Time and cost savings.** Institutions using high-assurance ID for registration could see up to 90 percent cost reduction in customer onboarding, with the time taken for these interactions reduced from days or weeks to minutes. By enabling streamlined authentication to improve the customer experience in digital channels, institutions could also influence customers to choose digital offerings that are cheaper to provide. For example, for financial services providers, the cost of offering customers digital accounts can be 80 to 90 percent lower than the cost of using physical branches.[27]

— **Reduced fraud.** Digital ID can help reduce fraud in a wide range of transactions, from decreased payroll fraud in worker interactions to reduced identity fraud in consumer and taxpayer and beneficiary interactions. In the United States, approximately 16.7 million Americans were victims of identity fraud in 2017, an increase of 8 percent from 2016.[28] Worldwide, theft of consumers' identities cost businesses an estimated $148 on average per person in the 12 months to June 2018.[29] We estimate that by 2030, governments in Brazil, Nigeria, and the United States could reduce leakage in public benefits alone by $90 billion, $3 billion, and $56 billion, respectively.[30]

— **Increased sales of goods and services.** Through digital onboarding, which enables streamlined authentication and improves customer experience in digital channels, institutions could increase uptake of new products and services. For example, the Indian telecom provider Jio onboarded some 160 million new customers in less than 18 months

[25] Olusegun Olaopin Olanrele and Samson E. Agbato, "Land right registration and property development for poverty eradication and slum clearance in Nigeria," *Journal of Design and Built Environment,* December 2014, Volume 14, Number 2.
[26] "e-Identity: ID card," e-Estonia, e-estonia.com/solutions/e-identity/id-card.
[27] *Digital finance for all: Powering inclusive growth in emerging economies,* McKinsey Global Institute, September 2016.
[28] "Identity fraud hits all time high with 16.7 million US victims in 2017, according to new Javelin Strategy & Research study," Javelin Strategy & Research, February 6, 2018.
[29] *2018 cost of data breach study: Global overview,* Ponemon Institute, June 2018.
[30] Estimates are in 2018 real dollars. This calculation conservatively assumed that a digital ID will reduce only a fraction of leakage. In Zambia, for instance, some studies have suggested that leakage in social transfer programs may be between 25 and 35 percent. See *Public sector savings and revenue from identification systems: Opportunities and constraints,* World Bank, 2018.

using e-KYC, enabled by India's national digital ID system, Aadhaar.[31] Digital ID could also reduce opportunity costs; in the United Kingdom, for example, nearly 25 percent of all financial applications are abandoned due to difficulties in the registration process.[32] Institutions that already rely on some form of high-assurance identities, such as banks and digital gig economy platforms like Uber, have the most to gain. Institutions that interact with individuals without the use of any identities, for example online merchants and informal employers, also will profit, but to a lesser degree.

— **Greater employment and labor productivity.** Digital ID can help expand and improve talent matching, streamline employee authentication, and enable contracting with nontraditional workers, such as contract and gig workers. As a result, businesses could more rapidly fill open positions and find the right employee for a given position, leading to higher productivity. The need for streamlined employee authentication processes is rising. Glassdoor found that 25 percent of US job applicants said they had undergone background checks in 2010, compared with 42 percent in 2015, and hiring time increased by 3.4 days, or 15 percent of the average hiring cycle.[33]

— **Increased tax collection.** Greater revenue facilitated by digital ID could expand the tax base, helping promote formalization of the economy and more effective tax collection.[34] Emerging economies in particular could experience substantial benefits—although to realize such benefits, they would first need to make it an explicit goal and then build the requisite tax collection tools enabled by digital ID programs. In Tanzania, for example, the National Identification Authority estimates that of 14 million people capable of paying taxes, only 1.5 million, or around 10 percent, do so.[35] In India, the Ministry of Finance estimates that only 35 million people, less than 3 percent of the total population, are in the taxpayer base.[36] In Latin American countries, some studies have estimated that approximately half of potential tax revenues are lost to tax evasion.[37]

13%

The economic value equivalent of GDP in 2030 that digital ID could unlock in Brazil

Countries implementing digital ID could unlock value equivalent to 3 to 13 percent of GDP by 2030

Digital ID can create economic value for countries primarily by enabling greater formalization of economic flows, promoting higher inclusion of individuals in a range of services, and allowing incremental digitization of sensitive interactions that require high levels of trust. Our analysis of Brazil, China, Ethiopia, India, Nigeria, the United Kingdom, and the United States indicates that individual countries could unlock economic value equivalent to between 3 and 13 percent of GDP in 2030 from the implementation of digital ID programs (Exhibits E4 and E5).

We make a distinction between basic digital ID, which enables verification and authentication, and digital ID with advanced applications, which we call advanced digital ID or advanced ID. Advanced ID enables storing or linking additional information about individual ID owners and thus can facilitate advanced data sharing, with informed user consent. For example, when an individual pays taxes, an advanced ID system would allow the individual to give the tax authority consent to digitally access the relevant bank information, investment accounts, and employment records necessary for filing quickly and without error. Advanced ID programs like these should be designed with principles of data minimization and owner agency in mind. Public and private data aggregators need to protect user privacy and be responsible about

[31] "Jio propels India to top in mobile broadband consumption by automating world's first all-IP network with Cisco," Cisco, April 2018. Note with the recent Supreme Court ruling in India, alternative methods of reducing the verification process in hiring are likely to emerge. In a ruling in September 2018, India's Supreme Court upheld the constitutional validity of Aadhaar and held that it could remain mandatory for those receiving government benefits or filing taxes. However, it struck down a section of the Aadhaar Act that permitted use by private companies, including telecoms. Going forward, such uses would need to be made permissible, on a voluntary basis, by amendments to relevant laws or the use of modified authentication processes.

[32] *Private sector economic impacts from identification systems*, World Bank, 2018.

[33] *Why is hiring taking longer? New insights from Glassdoor data*, Glassdoor, June 2015.

[34] *Digital revolutions in public finance*, IMF, November 2017.

[35] Joseph J. Atick, *Digital identity: The essential guide,* ID4Africa Identity Forum, 2014.

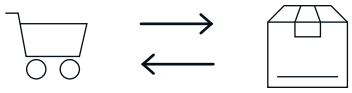
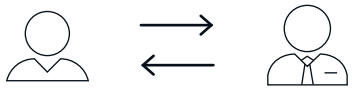
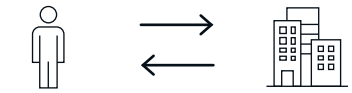
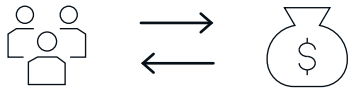
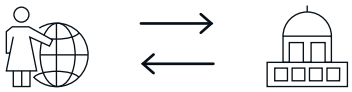
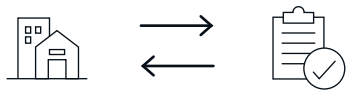
[36] Ibid.

[37] Eduardo Cavallo et al., *Saving for development: How Latin America and the Caribbean can save more and better*, Inter-American Development Bank, June 2016.

the data they collect and process, while owners of data—in this case the digital ID holders—need to be educated and empowered to provide informed consent and exercise control over the use of their data. In many cases, the lines between basic and advanced digital ID may blur because broader digital ecosystems can be built on top of a basic digital ID that enables an underlying ability to authenticate over digital channels.

Exhibit E3

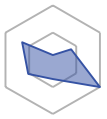
Individuals use digital ID in six roles to interact with institutions and create shared value.

	Example use cases associated with each role Our analysis examined in detail nearly 100 use cases in six roles
 Consumers ⇄ Commercial providers of goods and services	■ Streamlined registration and authentication ■ Secure digital payments ■ e-KYC for financial services
 Workers ⇄ Employers	■ Facilitated talent matching ■ Automated background verification ■ Efficient payroll services
 Micro-enterprises ⇄ Consumers and broad range of institutions	■ Formalized business registration ■ High-assurance contracting and transacting
 Taxpayers and beneficiaries ⇄ Public providers of goods and services	■ Streamlined e-government services ■ Digital tax filing ■ Direct disbursement of government benefits
 Civically minded individuals ⇄ Governments and other individuals	■ Online voting ■ Verification of political donations ■ School enrollment
 Asset owners ⇄ Asset-based service providers and buyers	■ Formalized land ownership ■ Facilitated sales and purchases

Source: McKinsey Global Institute analysis

Exhibit E4

The magnitude and nature of potential value creation vary across focus countries.

	Addressable share of economy	Potential for improvement	Potential economic value enabled		
	Wage base[1]; Capital investment efficiency[4]; Healthcare spending[2]; Government benefits[3]	Population without ID[5]; Fraud levels[10]; Offline population[6]; Informal economy and workforce[9]; Unmet financial needs[7]; Unemployed and inactive[8]	% GDP equivalent value by 2030[11]: Basic (authorization only); Advanced (data sharing)	Potential value, 2030E 2018 $ billion	Additional FTEs, 2030E Million
Brazil			8–13	347	1.9
Nigeria			5–7	59	1.2
Ethiopia			4–6	12	1.5
India			4–6	409	7.7
China			2–4	1,058	7.8
United States			<0.5–4	995	2.4
United Kingdom			<0.5–3	97	0.4

1. Measured by wages divided by GDP.
2. Current health expenditures as a share of GDP.
3. Current government expenditures as a share of GDP.
4. Measured by GDP divided by fixed capital.
5. Measured by the unregistered population (all ages).
6. Offline population is measured based on the percentage of the population not using the internet.
7. Measured by potential for increased capital investment as a result of expanded potential for new credit driven by an increased deposit base and/or improved ability to underwrite new loans from financial inclusion.
8. Includes individuals participating in the labor force but unemployed and those not participating in the labor force.
9. Measured by a composite of the informal share of GDP and the informal share of the workforce.
10. Measured by Corruption Perceptions Index.
11. Our estimates include the full value from use cases of digital ID, assuming high levels of adoption by 2030, the necessary digital infrastructure and ecosystems to enable usage, and complementary investments required.

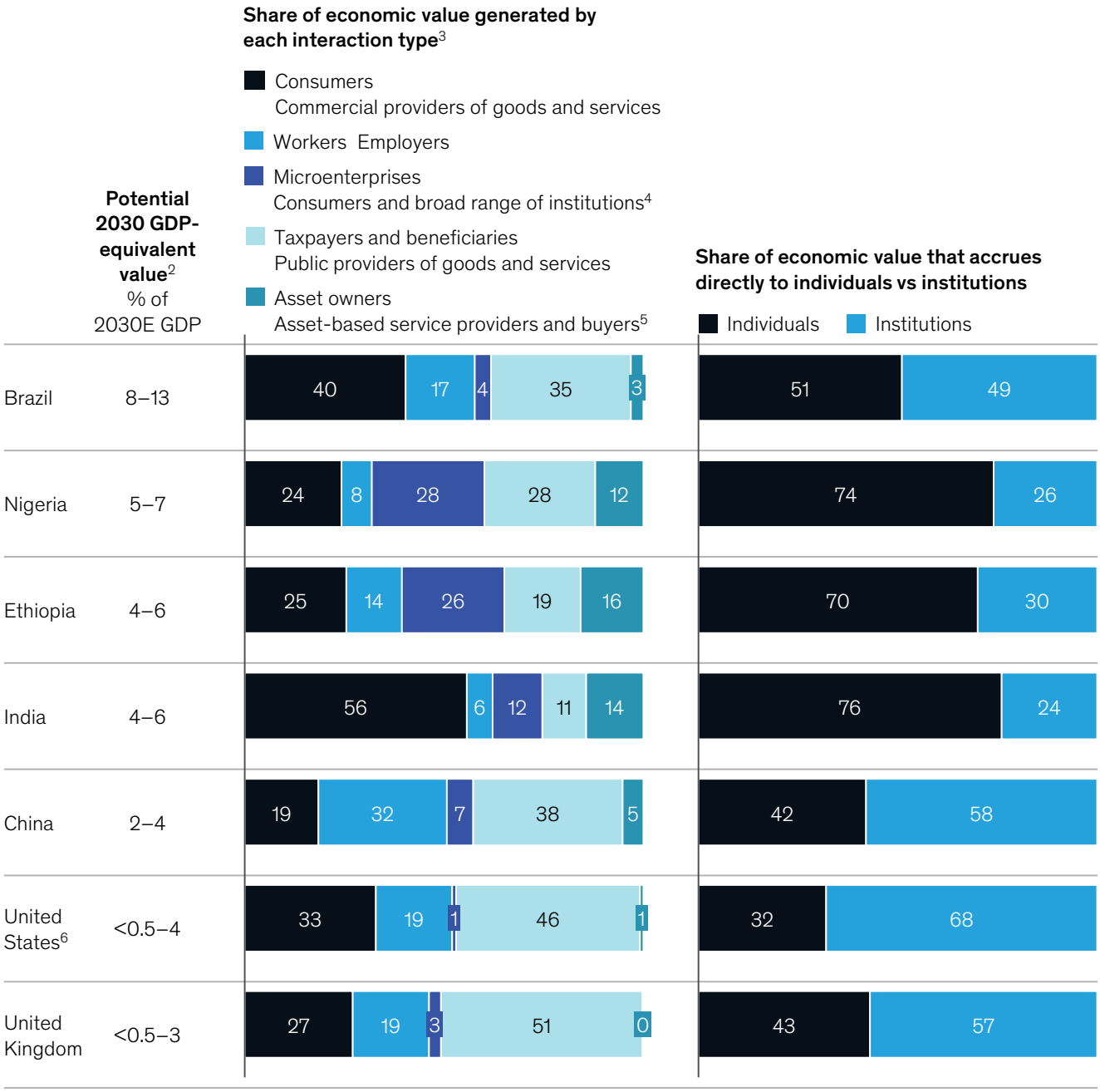
Note: For each chart, a larger shaded area reflects a higher contribution to economic value while a smaller shaded area reflects a smaller contribution to economic value. The charts are normalized on each dimension across a set of 217 countries. Calculation for potential economic value enabled is performed for focus countries using over 100 use cases (see Box 3, "Our methodology"). Addressable share of economy and potential for improvement variables help explain the macro drivers of this value and how they vary by country. Addressable share of economy and potential for improvement based on latest available data whereas economic value estimates are for 2030. Addressable share metrics represent ratios relative to GDP in a country.

Source: ITU; World Bank; ID4D; Findex; WDI; IMF; Transparency International; McKinsey Global Institute analysis

Exhibit E5

Individuals stand to gain about 50 percent of the total potential value of digital ID in our focus countries, generated through different interaction types.

% of country-level economic value potential estimate[1]



1. Calculations for share of economic value are based on our sizing of the potential value from advanced digital ID schemes with full data sharing.
2. Range of potential value based on whether digital ID is basic (ie, authorization only) or advanced (full data sharing). Our estimates include the full value from use cases of digital ID, assuming high levels of adoption by 2030, the necessary digital infrastructure and ecosystems to enable usage, and complementary investments required.
3. We do not size economic value generated through civically engaged individual interactions with governments and other individuals.
4. Includes all institutions or individuals that contract with, purchase goods or services from, or provide services to microenterprises.
5. Includes a range of asset-based service providers including those involved in services such as titling, financing, and leasing.
6. In the United States, we allocate 55% of the economic value generated through secure sharing of medical data to the consumer role and the remaining 45% to the taxpayer and beneficiary role, reflecting the private-public breakdown of healthcare spending as reported by the Centers for Medicare and Medicaid Services in 2017. In other focus countries, we consider value generated through healthcare use cases under taxpayer and beneficiary.

Note: Figures may not sum to 100% because of rounding.

Source: McKinsey Global Institute analysis

In the emerging economies we examine, we find that basic digital ID alone could unlock 50 to 70 percent of the full economic potential, assuming adoption rates of about 70 percent. In the United States and United Kingdom, where conventional alternatives and robust digital ecosystems already exist, nearly all potential value requires advanced digital ID.

Both the magnitude of economic potential from digital ID and the way in which value distributes across types of interaction between individuals and institutions differ significantly in our focus countries. Two factors help explain the variations:

— **Addressable share.** This is the share of the economy consisting of those types of interactions that digital ID could improve or, in other words, the bottlenecks that digital ID can address. It is characterized by indicators such as government spending on benefits, overall wages, and healthcare spending. The share of investment-led output, which determines the economic impact of new sources of capital from financial inclusion, also contributes.

— **Potential for value creation.** This is the aggregate potential for greater formalization, inclusion, and digitization. It measures the degree to which digital ID could directly improve economic interactions. It is characterized by indicators such as current levels of coverage of digital and conventional ID, informal share of GDP and of employment, employment level, potential for new deposits and loans from financial inclusion, and fraud rate.

Overall, we find that the potential for value creation is greatest in Brazil, which could unlock value equivalent to 8 to 13 percent of GDP in 2030 from digital ID. With basic digital ID, the potential could be 8 percent of GDP; with advanced digital ID, it could be as high as 13 percent. Consumer interactions are responsible for 40 percent of the economic potential, which is driven by a large credit gap that could be partially addressed through increased financial inclusion of individuals previously unable to access the financial system. Interactions by taxpayers and beneficiaries account for an additional 35 percent of the potential economic value, coming from increased government revenue from taxation of newly formalized income and reduction in tax fraud. In addition, we found that digital ID could help meaningfully reduce payroll fraud. The overall value from digital ID could accrue relatively equally to individuals and institutions, with individuals receiving 51 percent of the value potential by our estimates.

30%

The amount that the average selling price of a fingerprint sensor found in a mobile phone fell in 2017

Nigeria could capture economic value equivalent to 5 to 7 percent of GDP in 2030. This value is largely generated by microenterprise interactions and taxpayer and beneficiary interactions, which each drive 28 percent of the total value potential. Reduced fraud accounts for most of the value generated by interactions involving taxpayers and beneficiaries. Nigeria could capture significant value from microenterprises due to the importance of the informal sector to the economy. The large informal sector also skews the overall benefits of digital ID toward individuals, who could receive 74 percent of the overall value. Eighty-one percent of Nigeria's workforce is estimated to be self-employed, and the informal economy generates 52 percent of GDP.[38] Digital ID could play a critical role in generating value for microenterprises by giving them access to formal recognition as a business, efficient contracting, and streamlined hiring.

Ethiopia's profile is similar to Nigeria's; we estimate that it could capture economic value equivalent to 4 to 6 percent of GDP in 2030. As in Nigeria, the economy is heavily informal, with the International Labour Organization estimating that 89 percent of the workforce is self-employed. This is the primary reason Ethiopia's value from microenterprise interactions is the main driver of value, generating 26 percent of the economic potential.

While India shares some characteristics with Nigeria and Ethiopia, its benefit fingerprint differs because the roll-out of Aadhaar has already enabled some benefits to be realized, while additional benefits are expected in the future. Aadhaar covers about 1.2 billion people; in 2008 it was estimated that only 40 million had a passport, 70 million a Pan card (with a Permanent Account Number from the Income Tax Department), 220 million a ration card, and

[38] ILOSTAT database, International Labour Organization, September 2018; Leandro Medina and Friedrich Schneider, *Shadow economies around the world: What did we learn over the last 20 years?*, IMF working paper, January 2018.

500 million a voter ID.[39] The use of Aadhaar-enabled e-KYC for registration led to an increase in financial accounts from 48 million in 2016–17 to 138 million in 2017–18.[40] Eighty-four percent of those surveyed for the most recent State of Aadhaar report who opened a bank account between 2014 and 2017 used Aadhaar, although many used it in analog form. India has also seeded 82 percent of public benefits disbursement accounts with Aadhaar, which has reduced fraud and leakage.[41] We calculate that India could capture additional economic potential equivalent to 4 to 6 percent of GDP in 2030 from digital ID. Most of the value derives from consumer interactions, including resolution of the credit gap and increased cost savings to government and businesses as the use of digital ID is expanded and integrated into service delivery. In particular, we expect India to benefit from labor market use cases of digital ID, such as talent matching and the formalization of contracts, as well as growing financial inclusion, which increases in value over time as the benefits of growth in deposits and credit materialize. Systems for digital ID–based authentication will also evolve as policies evolve.[42]

We find that the economic potential of digital ID in China is not as large as in the other emerging economies in our focus group, with a total potential value unlocked by digital ID equivalent to 2 to 4 percent of GDP in 2030. The economic value of digital ID in China is driven primarily by transactions involving taxpayers and beneficiaries and those involving workers. China's relatively high existing level of ID coverage, at 98 percent of the population according to World Bank analysis, reduces the relative gains experienced by microenterprises and asset owners compared with their counterparts in emerging economies like Nigeria and Ethiopia. As a result, value is driven by digital efficiencies, and the majority of the overall benefits of digital ID in China will be captured by institutions, particularly by employers through more efficient hiring and by government through reduced fraud and tax leakage.

In the United States, the potential value enabled by digital ID could be up to the equivalent of 4 percent of GDP, with as much as one-quarter of that potential value coming from healthcare.[43] According to the World Bank, 2015 healthcare spending in the United States was 16.8 percent of GDP, compared with 9.8 percent in the United Kingdom, for example. Digital ID can create significant efficiencies in healthcare through facilitated sharing of records, and therefore the economic impact of these efficiencies in the United States would be greater as a percentage of total GDP. The increased savings are directly captured by healthcare providers and government, which explains why institutions capture more of the economic benefit in the United States than they do in the United Kingdom. Some of the savings are likely to be distributed to individuals through price reductions.

In the United Kingdom, we estimate that total economic value equivalent could be less than 0.5 to 3 percent from high adoption of digital ID. These gains are mostly derived from interactions involving taxpayers and beneficiaries—more than 50 percent of the potential—and secondarily from interactions involving workers. Taxpayer and beneficiary transactions often require high-assurance identification, creating the potential for digital ID to unlock digitization of interactions that previously required in-person authentication. Digitizing these interactions could unlock significant time savings and reduce fraud associated with tax filing. Overall, individuals could receive 43 percent of the benefit from digital ID in the United Kingdom.

[39] *Aadhaar: Inclusive by design: A look at India's national identity programme and its role in the JAM trinity,* GSMA, March 2017.

[40] Ronald Abraham et al., *State of Aadhaar report, 2017–18,* IDinsight, May 2018.

[41] Ibid.

[42] In a ruling in September 2018, India's Supreme Court upheld the constitutional validity of Aadhaar and held that it could remain mandatory for those receiving government benefits or filing taxes. However, it struck down a section of the Aadhaar Act that permitted use by private companies. Going forward, such uses would need to be made permissible, on a voluntary basis, by amendments to relevant laws or the use of modified authentication processes.

[43] In the United States, we allocate 55 percent of the economic value generated through secure sharing of medical data to the consumer role and the remaining 45 percent to the taxpayer and beneficiary role, reflecting the private-public breakdown of healthcare spending as reported by the Centers for Medicare and Medicaid Services in 2017. In other focus countries, we consider value generated through healthcare use cases under taxpayer and beneficiary.

Digital ID helps create economic value differently in emerging versus mature economies

We assess a broader set of 23 countries on the factors that drive potential value from digital ID—addressable share of the economy and potential for improvement in inclusion, formalization, digitization, and ID coverage (Exhibit E6). Based on country-level patterns of these factors, we develop directional estimates of the potential economic value of both basic and advanced digital ID for each of these countries, using the seven focus countries as a guide.

4%

The economic value equivalent of GDP in 2030 that digital ID could unlock in the United States

6%

The economic value equivalent of GDP in 2030 that digital ID could unlock in emerging economies on a per-country basis

3%

The economic value equivalent of GDP in 2030 that digital ID could unlock in mature economies on a per-country basis

We find that in 2030, digital ID has the potential to create economic value equivalent to 6 percent of GDP in emerging economies on a per-country basis and 3 percent in mature economies, assuming high levels of adoption. In emerging economies, much of the value could be captured even through basic digital ID with essential functionalities. For mature economies, many processes are already digital and potential for improvement is more limited, necessitating advanced digital ID programs with data-sharing features. Of the potential value, we estimate that in emerging economies, some 65 percent could accrue to individuals, while in mature economies, about 40 percent could flow to individuals.

As we noted earlier, achieving high rates of adoption in multiple use cases is neither automatic nor certain. India's Aadhaar system achieved over 90 percent coverage, while Nigeria's National eID, launched in 2014, has adoption rates below 10 percent.[44] Yet even in India, digital ID addresses a relatively small portion of the potential use cases. In mature economies, basic digital ID programs that lack advanced data-sharing functionality have seen low adoption in the United Kingdom, Germany, and Austria, while higher-functionality digital IDs have achieved adoption rates of more than 70 percent in Estonia, Sweden, and Norway, among others.[45] Despite the mixed success, however, the upside benefits of digital ID, in terms of economic value, can be significant.

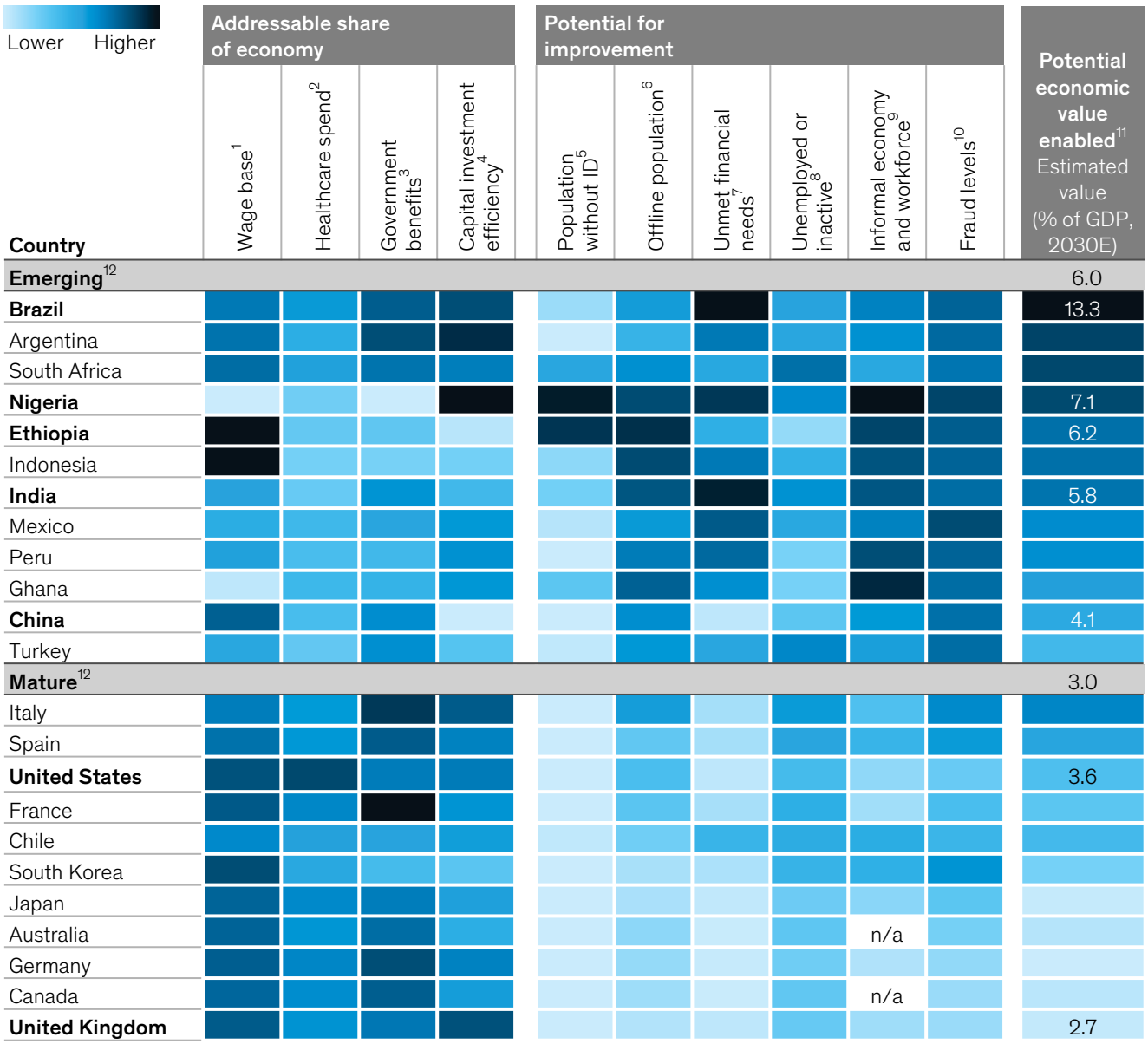
Digital ID can also unlock noneconomic value, potentially furthering progress toward ideals that cannot be captured through quantitative analysis, including those of inclusion, rights protection, and transparency. Digital ID can promote increased and more inclusive access to education, healthcare, and labor markets; can aid safe migration; and can contribute to greater levels of civic participation. For example, in Estonia, over 30 percent of individuals vote online, of whom 20 percent say they would not vote at a physical polling place.[46] Digital ID can also help enforce rights nominally enshrined in law. For example, in India, the right of residents to claim subsidized food through ration shops is protected because their identity—and claim—is authenticated through a remote digital ID system, rather than at the discretion of local officials. By providing greater legal protection, digital ID could help in the elimination of child labor and help enforce laws against child marriage.[47] Transparency is another benefit of digital ID. An accurate, up-to-date death registration system can help curb social protection fraud, and a reliable, authentic voter registry is essential to reduce voter fraud and ensure the overall integrity of the electoral process.

[44] "AADHAAR Dashboard," Unique Identification Authority of India, Uidai.gov; "About the e-ID Card," Nigeria National Identity Management Commission, nimc.gov.ng, updated as of 1/2/2019.
[45] "GOV.UK Verify Dashboard," Gov.UK; *Overview of the German identity card project and lessons learned (2017 update)*, Gemalto; *National Mobile ID schemes*, Gemalto, 2014; "e-Identity," e-Estonia.com; "This is Bank ID," BankID.com; "About us," BankID.no.
[46] *A comparative assessment of electronic voting*, Elections Canada, February 2010.
[47] Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?*, Center for Global Development, October 2017.

Exhibit E6

Value creation potential from digital ID varies across countries.

Variation based on factors related to addressable share of the economy and potential for improvement in inclusion, formalization, digitization, and ID coverage



1. Measured by wages divided by GDP.
2. Current health expenditures as a share of GDP.
3. Current government expenditures as a share of GDP.
4. Measured by GDP divided by fixed capital.
5. Measured by the unregistered population (all ages).
6. Offline population is measured based on the percentage of the population not using the internet.
7. Measured by potential for increased capital investment as a result of expanded potential for new credit driven by an increased deposit base and/or improved ability to underwrite new loans from financial inclusion.
8. Includes individuals participating in the labor force but unemployed and those not participating in the labor force.
9. Measured by a composite of the informal share of GDP and the informal share of the workforce.
10. Measured by Corruption Perceptions Index.
11. Our estimates include the full value from use cases of digital ID, assuming high levels of adoption by 2030, the necessary digital infrastructure and ecosystems to enable usage, and complementary investments required.
12. We refer to "mature economies" as economies that are classified by the World Bank as high-income countries; the term "emerging economies" includes all others.

Note: For each box, a deeper shade reflects a higher contribution to economic value while a lighter shade area reflects a smaller contribution to economic value. The charts are normalized on each dimension across a set of 217 countries. Calculation for potential economic value enabled is performed for the seven focus (shown in bold) using over 100 use cases (see Box 3, "Our methodology"). Using an exponential fit, the economic value for all other countries was determined based on the fitted line. Addressable share of the economy and potential for impact based on latest available data; economic value estimates are for 2030. Addressable share metrics represent ratios relative to GDP in a country.

Source: ITU; World Bank; ID4D; WDI; Findex; Transparency International; McKinsey Global Institute analysis

Capturing the value requires careful system design and deliberate government policies that both foster uptake and mitigate risk

Individuals will use a digital ID system only if it provides value and engenders trust. In this section, we highlight the key areas that must be considered carefully to mitigate risk and promote adoption.

Preconditions for digital ID include a minimal level of digital infrastructure, sufficient trust in the ID provider, and a policy landscape that provides safeguards to individuals

Digital ID infrastructure relies on some basic level of general digital infrastructure, both to support digital ID and to enable the gains that digital ID helps unlock. Infrastructure to support digital ID includes level of internet access, degree of smartphone penetration, and reliability of electricity. For example, programs requiring remote access by users rely on widespread internet access, at a minimum, covering internet-enabled hotspots that allow for authentication. In cases where infrastructure is limited, digital ID might first be extended to parts of the country with more robust infrastructure.

For digital ID to successfully unlock value for each use, additional infrastructure may also be necessary. For example, for digital ID to help increase levels of financial inclusion, basic digital payments infrastructure must also be in place. Many employment-related benefits rely on the existence of digital talent matching and contracting platforms, tied into the digital ID system. E-government services, digital health records, and digital asset registries are all infrastructure preconditions for important ways of using digital ID involving government service provision, medical care, and landownership, respectively.

Adoption by individuals and institutions can be accelerated if these entities trust the digital ID program. Studies have found that in general, individuals trust healthcare providers, financial institutions, and government the most with their personal data.[48] However, this varies across geographies, with implications for the optimal implementation approach and the ability of an ID provider to garner adequate adoption. [49]

The policy landscape in a country will be important to set the framework for the ID system and as a means to address systemic risk. Multiple types of regulation may shape the way a digital ID system works. Legal protections and recognition for use of digital identity enable digital ID to serve its basic purpose. Data privacy policies establish the degree of individuals' control over their data as well as standards of care institutions must meet in handling individuals' data. Rules and regulations requiring individuals to show identification in order to receive products and services—such as KYC requirements to open financial services or telecom accounts—shape some of the ways digital ID can be used. However, if digital ID is used to satisfy such rules and regulations, it becomes important to actively minimize the risks of excluding anyone who does not have, or does not want to use, a digital ID.

Digital identification programs can promote adoption and usage through high-value use cases, well-designed user experience, and seamless initial registration

To unlock the potential value described in this report, individuals and institutions will need to broadly adopt and use digital ID programs. While the path to do this varies by country, both successful programs and costly scrapped failed systems provide broad general lessons. Adoption and usage will happen only if the digital ID provides more value than the status quo, if the user experience is positive, and if initial registration is relatively easy.

Digital ID programs should prioritize use cases that generate meaningful value for both individuals and institutions and that entail frequent use, to quickly generate a critical mass of users. For individuals, this means generating cost or time savings or making access to products and services easier or newly possible. Meanwhile, institutions will be drawn to digital ID uses that reduce costs, increase revenue, or, in the case of public institutions like government, improve economic or social welfare. We find that government and financial

[48] *Open Data Institute Knowledge & Opinion,* "Who do we trust with personal data?," blog entry by Leigh Dodds, July 5, 2018, theodi.org/article/who-do-we-trust-with-personal-data-odi-commissioned-survey-reveals-most-and-least-trusted-sectors-across-europe.

[49] "Trust and privacy," Omidyar Network, October 2, 2017.

1.2b

The number of people Aadhaar successfully onboarded

services uses have the greatest potential to provide value to both institutions and individuals simultaneously, through high-frequency use cases.

User experience for both individuals and institutions must be positive. This means that digital ID providers should prioritize continuous improvement of individual user experience and program accessibility. Privacy is also a growing contributor to individual user experience, though detailed preferences vary by country. For example, in a Pew survey following the Cambridge Analytica data breach, 26 percent of respondents reported having deleted the Facebook app from their mobile device in the previous year.[50] Experience also matters for institutional users. Easily accessible technical support, flexible integration with back-end systems, and availability of value-added services such as fraud protection can all contribute.

Finally, initial digital ID registration should be as easy as possible for both individuals and institutions. The process for individuals should be intuitive, straightforward, convenient, and fast. For example, in India, Aadhaar successfully onboarded about 1.2 billion people by rapidly creating about 50,000 enrollment points, located to be accessible even to rural residents, creating an ecosystem of competition among public- and private-sector entities as registrars, incentivizing them by paying them per successful unique registration rather than hourly, and designing extremely inclusive and flexible documentation requirements.[51]

Digital ID programs that unlock value while addressing risk require careful design, appropriate infrastructure, and well-controlled governance

Realizing value while controlling for risk relies on considered decisions on scope of use cases provided, system ownership, front- and back-end infrastructure and processes, and program governance. Whether the digital ID system is basic or advanced shapes all further decisions about system design, infrastructure, and governance. Advanced digital IDs can unlock significantly more value than basic ones, particularly in mature economies, but may be harder to implement. In addition, because advanced ID programs entail storage of larger amounts of personal data, they demand particularly stringent controls to guard against both misuse and associated risks. Essential elements include a robust approach to what data are collected, very high standards for safe data storage to guard against cyberintrusions, and mandated collection of user consent for all use of personal data.

Digital ID system ownership takes one of three forms: centralized (a single provider), federated (ownership is shared among multiple stand-alone systems), or decentralized (no owner but depends on a distributed ledger). All three have both advantages and disadvantages for advanced ID. Hybrid models are also possible—for example, a centralized basic digital ID with federated add-on services.

Infrastructure and processes will shape user experience, implementation and maintenance costs, and risk profile. Several basic elements of identification infrastructure are necessary, including the ID credential, the IT infrastructure used for enrollment, back-end data processing, and authentication, as well as the physical features needed for user interaction and registration. The existence and level of these infrastructure elements will inform decisions on how people register, for example, through physical or remote digital channels.

Digital ID programs will also need to implement critical governance mechanisms to ensure a safe, secure, and transparent system. Four central governance elements of any digital ID system are decision rights, access rights, enforcement mechanisms, and contingency planning.

Governments, businesses, and civil society institutions can take action now as ID providers, requesting parties, users, and regulators

Governments, businesses, and civil society actors should think through several important questions as they shape the course of digital ID programs in their countries. These include how to address potential misuse of the digital ID system, approaches to safeguard user

[50] *Americans are changing their relationship with Facebook*, Pew Research Center, 2018.

[51] Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?*, Center for Global Development, October 2017; "AADHAAR Dashboard," Unique Identification Authority of India, Government of India, uidai.gov.in/aadhaar_dashboard/.

privacy and ensure control over personal data, what may be an optimal approach to system design or a standard that can be developed regardless of varying country characteristics, and how to accelerate implementation and adoption. Some immediate steps that stakeholders can take to help capture the value of digital ID include:

— Governments can consider developing policies and legal frameworks to enable acceptance of digital identities, while protecting user privacy and other rights, collaborating with international bodies to develop cross-border standardization, and partnering with private-sector institutions to understand country-specific economics of digital ID and to explore public-private and consortium-led models of provision.

— Businesses can innovate processes that could leverage digital ID to boost efficiency and improve customer experience, work to facilitate development of global standards, and collaborate with governments to conduct bespoke cost-benefit analysis of digital identity and develop new digital ID programs.

— Civil society institutions could help ensure that individuals capture the value of digital ID while retaining control over how their data are used and also being protected from misuse. For example, they could petition politicians, regulators, and institutions to develop digital ID programs that are safe, accessible, and socially beneficial along with policies that support and foster good digital ID.

Digital ID offers individuals social, civic, and political benefits, from increased inclusion, formalization, and transparency to better control of online data. Designed carefully and scaled to high levels of adoption in multiple application areas, it can also create significant economic value, particularly in emerging economies, with benefits for both individuals and institutions. Yet with that potential comes risk from deliberate misuse of digital ID programs by government and commercial actors as well as broader risks common to other large-scale digital interactions, such as technology failure and security breaches. These risks must be taken into account in the design, implementation, and governance of any digital ID system. As the landscape evolves, more research will help clarify the upsides and downsides of digital ID, and the effort will be well worth it. After all, digital ID may be the next frontier in global value creation and a new force for inclusive growth.

Related MGI and McKinsey research

Digital India: Technology to transform a connected nation (March 2019)

India is one of the largest and fastest-growing markets for digital consumers, with more than half a billion internet subscribers and rapidly growing data usage. Business adoption is more uneven for now, but digital applications have the potential to proliferate across most sectors of the economy, including both core digital sectors such as IT, newly digitizing ones including agriculture, financial services, and healthcare, as well as government services.

India's labour market: A new emphasis on gainful employment (June 2017)

India's labour markets are experiencing structural change, but attention tends to focus narrowly on creating jobs for its workforce of 460 million. We see the need to emphasize improved quality of work and the income derived from it.

Digital China: Powering the economy to global competitiveness (December 2017)

China is already a global leader in the digital economy. It is a major investor in and one of the leading adopters of digital technologies in the consumer sector. Chinese consumers are enthusiastic about e-commerce and mobile payments. But more is to come.

The new dynamics of financial globalization (August 2017)

Since the global financial crisis began, cross-border capital flows have fallen by 65 percent in absolute terms. But financial globalization is still very much alive—and could prove to be more stable and inclusive in the future.

Digital America: A tale of the haves and have-mores (December 2015)

While the most advanced sectors, companies, and individuals continually push the boundaries of technology use, the US economy overall is realizing only 18 percent of what we calculate to be its full digital potential.

Jobs lost, jobs gained: Workforce transitions in a time of automation (December 2017)

Automation and AI technologies will create new prosperity and millions of jobs, but as many as 375 million people will need to shift occupational categories and upgrade skills during the transition.

Digital finance for all: Powering inclusive growth in emerging economies (September 2016)

Delivering financial services by mobile phone could benefit billions of people by spurring inclusive growth that adds $3.7 trillion to the GDP of emerging economies within a decade.

www.mckinsey.com/mgi

Download and listen to MGI podcasts on iTunes or at www.mckinsey.com/mgi/publications/multimedia/

Cover image: Getty Images

McKinsey Global Institute
April 2019

Designed by McKinsey Global institute

www.mckinsey.com/mgi

@McKinsey
@McKinsey