McKinsey Global Institute

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

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

Preface

This report focuses on the economic potential of good digital ID. As an enabler of economic, social, and political activity in a digital age, good digital ID is a new frontier in value creation for individuals and institutions. We acknowledge that our research is not the last word on digital ID. For example, the design, governance, and use of digital ID is a rapidly evolving area deserving additional research. However, we hope our initial research effort contributes to a greater understanding of how digital ID, designed with the right principles, implemented with strong controls, and enforced with well-considered policies, can create significant economic benefits for individuals and institutions and can protect individuals from the risk of abuse.

This research was led by James Manyika, Anu Madgavkar, and Jacques Bughin of the McKinsey Global Institute, and Olivia White, Deepa Mahajan, and Michael McCarthy of McKinsey & Company. The project team was led by Sarang Parikh and Owen Sperling and consisted of Andrew Hickey, Andrew Margrave, and Michael Starr. In addition, Alan Fitzgerald and Krzysztof Kwiatkowski helped with the analysis.

This independent MGI initiative is based on our own research and collaboration with Omidyar Network, the Open Society Foundations, and the Rockefeller Foundation. We owe a debt of gratitude to Magdi Amin, Subhashish Bhadra, Yasmin Lamy, CV Madhukar, Paige Nicol, and Abiah Weaver of Omidyar Network; Darius Cuplinskas, Sean Hinton, Andrew Kramer, and Julie McCarthy of the Open Society Foundations; and Zia Khan, Kevin O'Neil, and Durva Trivedi of the Rockefeller Foundation.

Many other experts provided valuable insights and challenged our thinking. We extend our thanks to the team at Identification for Development (ID4D), a global, multisectoral initiative of the World Bank, including Luda Bujoreanu, Kamya Chandra, Julia Clark, Vyjayanti T. Desai, and Jonathan Marskell; Alan Gelb, senior fellow and director of studies, Center for Global Development; Manju George, head of Platform Services, Digital Economy & Society, World Economic Forum; Jeremy Grant, coordinator, the Better Identity Coalition; Gus Hosein, executive director at Privacy International; Sanjay Jain, fellow, iSPIRT, and chief innovation officer at the Centre for Innovation Incubation and Entrepreneurship, IIMA; Niall McCann, policy adviser, electoral assistance, Bureau for Policy and Programme Support, United Nations Development Programme; Rakesh Mohan, professor in the practice of international economics of finance, Yale University School of Management, and senior fellow of the Jackson Institute at Yale; Nandan Nilekani, co-founder and chairman of Infosys and founding chairman of the Unique Identification Authority of India (UIDAI); Hal Varian, chief economist at Google and professor emeritus at the University of California, Berkeley; and Michael Wiegand, director of the Financial Services for the Poor strategy at the Bill & Melinda Gates Foundation.

We are very grateful for all the help we received from current and former McKinsey and MGI colleagues, including Darius Chehrzard, Michael Chui, Ian De Bode, David Fine, Amanda Ganske, Shishir Gupta, Salim Hasham, Vikram Iyer, Somesh Khanna, Acha Leke, Linda Liu, Susan Lund, Ritesh Jain, Merlina Manocaran, Daniel Mikkelsen, Fiyinfolu Oladiran, Philip Osafo-Kwaako, Thomas Poppensieker, Kelsey Robinson, Hamid Samandari, Jon Steitz, Alexis Trittipo, Adam Tyra, Roshan Varadarajan, Daniel Wallance, John Walsh, and Dan Williams.

This report was edited and produced by senior editor Anna Bernasek, editorial production manager Julie Philpot, and senior graphic designers Marisa Carder and Patrick White. We also thank our colleagues Tim Beacom, Nienke Beuwer, Cathy Gui, Deadra Henderson, Richard Johnson, Lauren Meling, Rebeca Robboy, and Margo Shimasaki for their valuable contributions and support.

We are grateful for all the input we have received, but the final report is ours, and all errors are our own. We welcome comments on this research at MGI@mckinsey.com.

Jacques Bughin
Director, McKinsey Global Institute
Senior Partner, McKinsey & Company, Brussels

James Manyika
Director and Chairman, McKinsey Global Institute
Senior Partner, McKinsey & Company, San Francisco

Jonathan Woetzel
Director, McKinsey Global Institute
Senior Partner, McKinsey & Company, Shanghai

April 2019


FT10

Contents

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.

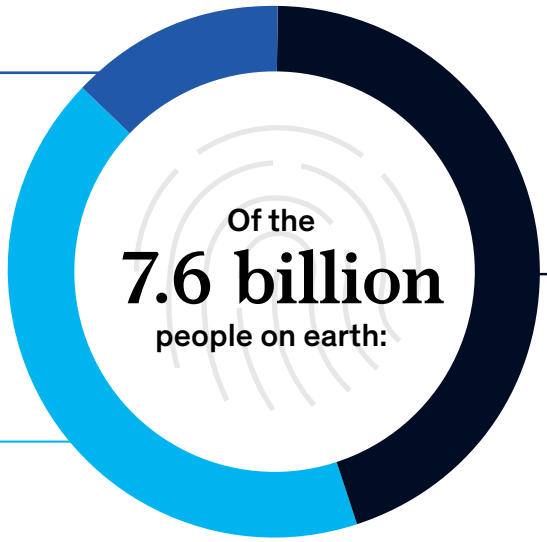
— Capturing the value of good digital ID is by no means certain or automatic. Careful system design and well-considered government policies are needed to promote uptake, mitigate risks like those associated with large-scale capture of personal data or systematic exclusion, and guard against the challenges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

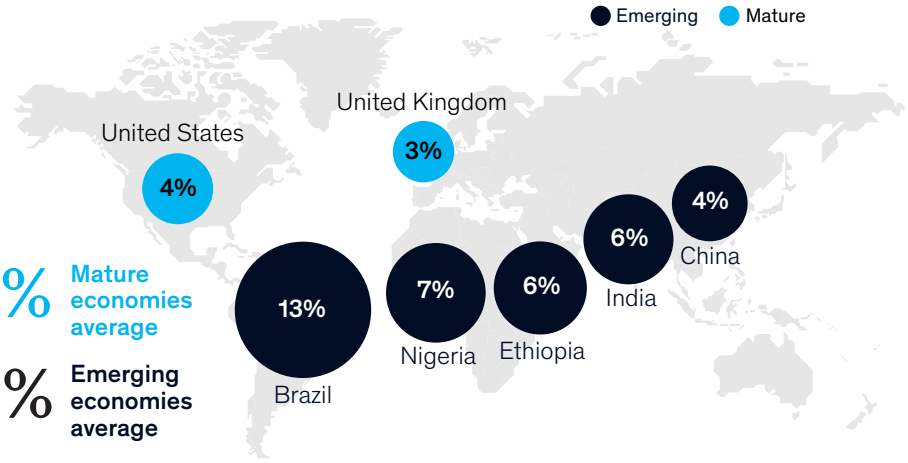
3.2 billion
have some form of ID and a digital trail



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.

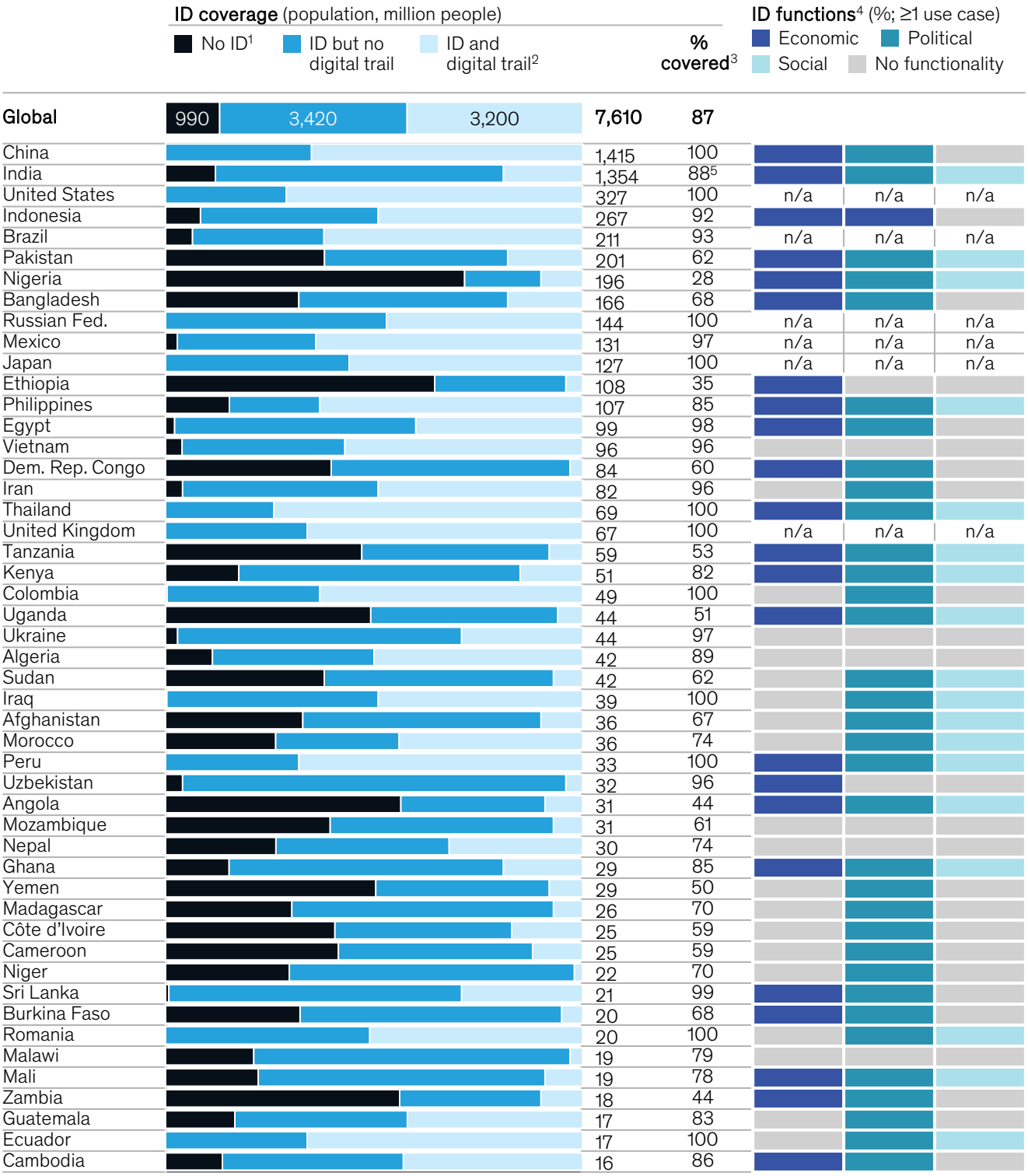
In this report, we *focus on the potential of good digital ID* to create value. The attributes of good ID, including high *assurance and consent-based creation and use, promote trust and protect privacy.* The design and governance of digital ID programs should incorporate these attributes and guard against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

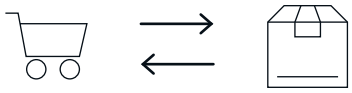
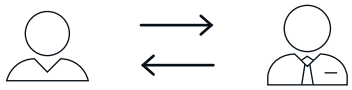
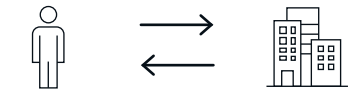
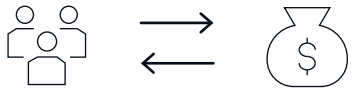
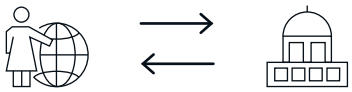
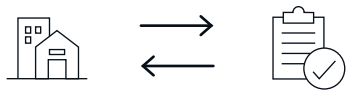
[36] Ibid.

[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

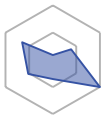
Individuals use digital ID in six roles to interact with institutions and create shared value.

	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.

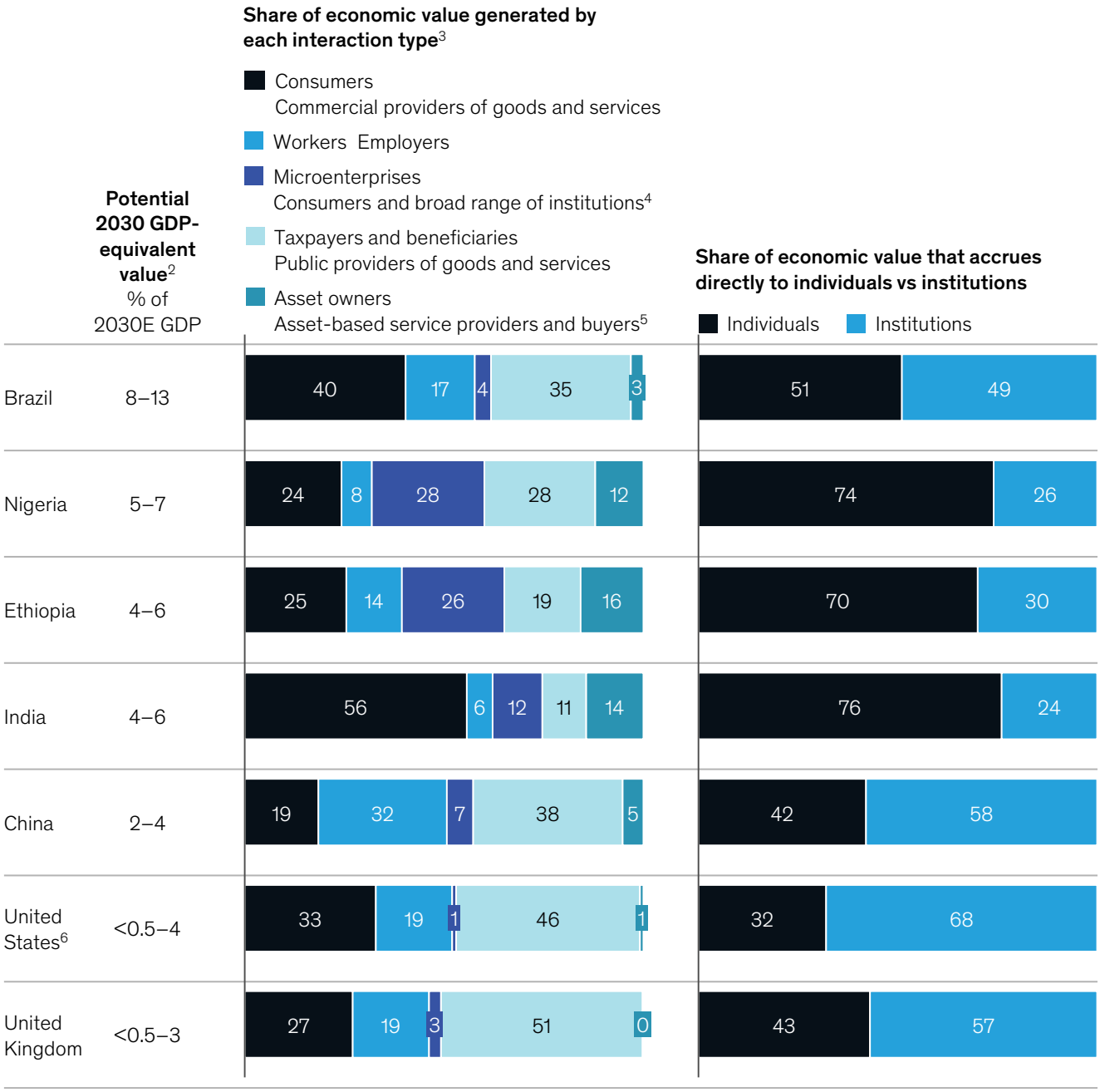
Note: For each chart, a larger shaded area reflects a higher contribution to economic value while a smaller shaded area reflects a smaller contribution to economic value. The charts are normalized on each dimension across a set of 217 countries. Calculation for potential economic value enabled is performed 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.

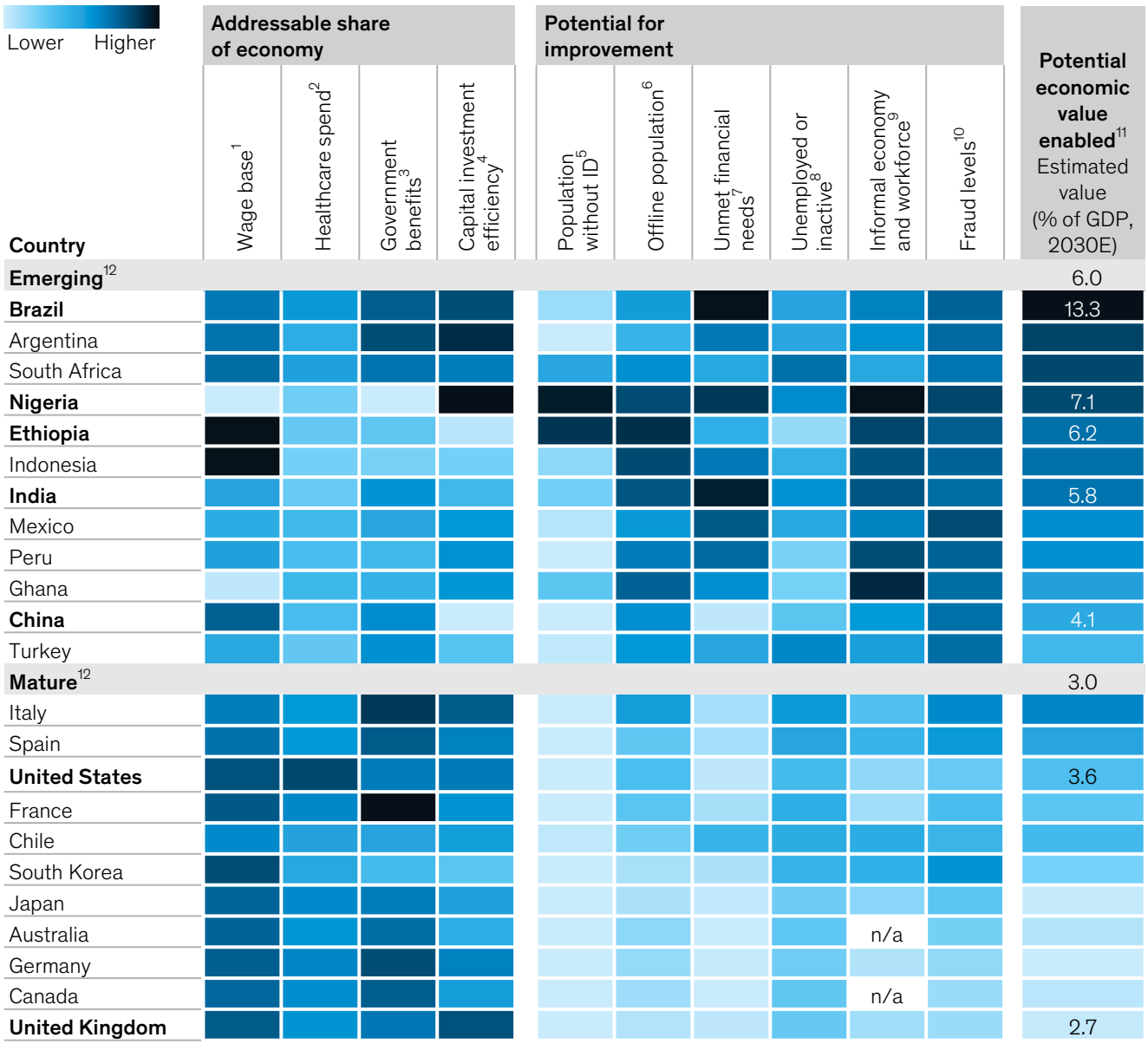
Digital ID can also unlock noneconomic value, potentially furthering progress toward ideals that cannot be captured through quantitative analysis, including those of inclusion, rights protection, and transparency. Digital ID can promote increased and more inclusive access to education, healthcare, and 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.

1 The potential of digital ID

Identification helps establish trust in our economic, social, and political interactions. Proving we are who we say we are lends legitimacy to the provision and distribution of goods and services and can foster inclusion and promote efficiencies. Close to one billion people in the world today, mainly in emerging economies, have no form of legal identification and may be denied access to critical government benefits, healthcare, financial services, and the labor market, or may be prevented from securing property rights or registering a business.[52] Digital ID can help. Given the falling costs of technologies like smartphones and scanners, rising access to internet infrastructure in emerging economies, and the shift online of more consumer and government services, identification that can be used securely over digital channels will be more important than ever to facilitate economic transactions, social interactions, and political involvement.

In addition to the estimated 1.0 billion people who lack ID, digital ID also offers value for the rest of the world's 6.6 billion people, who either have some form of identification but with limited ability to use it in the digital world or are active online but find it hard to keep track of their digital footprint securely and efficiently.

Unlike a paper-based ID such as most driver's licenses and passports, a digital ID can be authenticated remotely over digital channels, often at a lower cost. At the same time, digital ID that has attributes like high assurance and consent-based creation and use helps promote trust and protect privacy. However, digital ID technologies are also akin to "dual use" technologies that can be employed both to benefit society and for undesirable purposes by governments and other institutions as well as individual actors. Our research focuses on how "good" use of digital ID can create value and societal benefit, while being clear-eyed about the possibility of misuse, the associated risks and challenges, and the need to mitigate them. 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.

In this chapter, we lay out what digital identification is, explain why it matters, and highlight its potential for value creation for individuals, institutions, and countries.

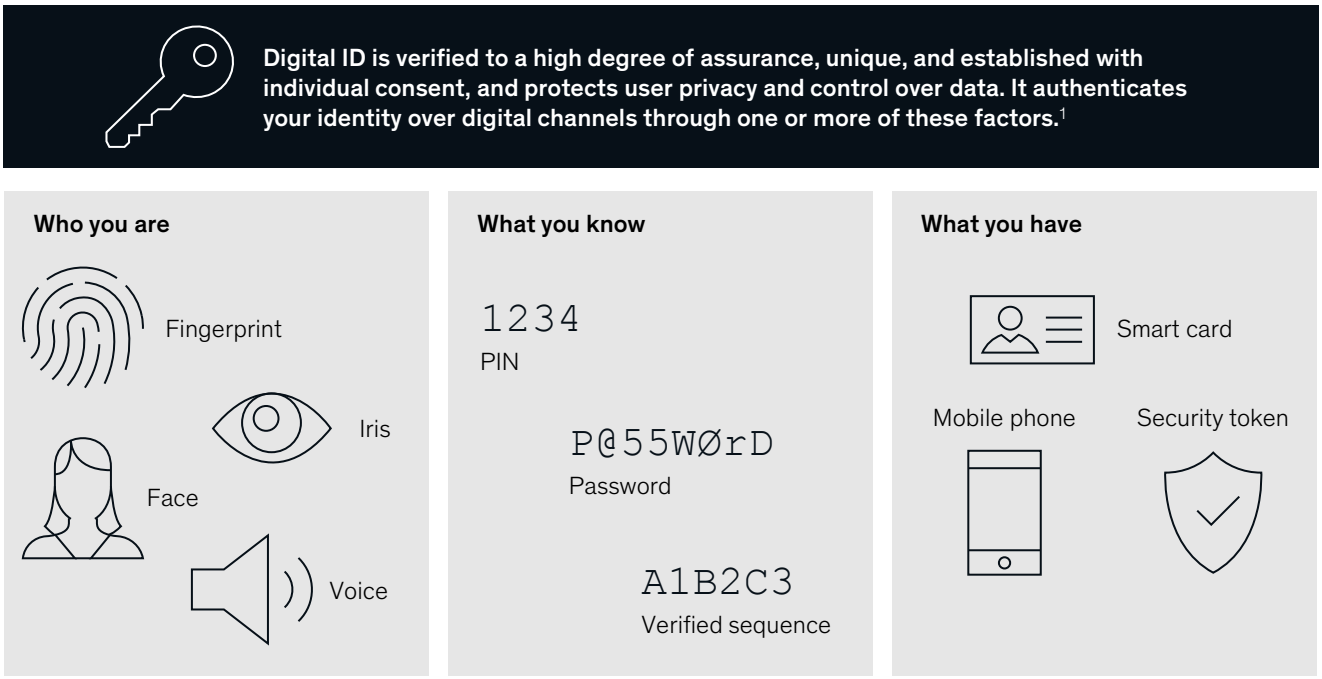
What is digital ID?

Identification is the means by which we prove we are who we say we are. This is distinct from identity, which is an individual's unique set of attributes. Identification provides a mechanism to authenticate identity. Digital ID programs let us authenticate who we are over digital channels, including mobile interfaces, internet browsers, or internet-enabled central authentication points. A digital ID can authenticate an individual's identity through a variety of factors such as who a person is—for example, a fingerprint; what they know—such as a PIN; and what they have—for instance, a smart card or mobile phone (Exhibit 1).

[52] Global ID4D Dataset, World Bank, 2018.

Exhibit 1

Digital ID can verify and authenticate your identity through a variety or combination of factors.



1. These authentication factors are illustrative and not comprehensive.

Source: McKinsey Global Institute analysis

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 include the use of biometric data, passwords, PINs, smart devices, and security tokens.

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

— **Is verified and authenticated to a high degree of assurance.**[53] 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. This attribute does not rely on any particular underlying technology. To achieve unique high-assurance authentication and verification, a range of credentials can be used, including biometrics, passwords, QR codes, and smart devices with identity information embedded in them.

— **Is 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.

[53] 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.

— **Is 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 ensure privacy and security while also giving users access to their personal data, decision rights over who has access to that data, and transparency into who has accessed it.

In this report, we make a distinction between basic and advanced digital ID. Basic ID is used only for authentication, while advanced ID stores or links to additional information. For example, when an individual pays taxes, an advanced ID system could allow a tax authority to digitally access the relevant bank information, investment accounts, and employment records necessary for filing with the individual's consent. However, the lines between basic and advanced digital ID are not necessarily clear, because even basic ID can be used to link to other databases. All digital ID programs should be designed and executed with principles of data minimization, owner agency, and privacy safeguards in mind.

3.2b

The number of people who have a form of ID, digital or otherwise, but may not be able to use it effectively online

People across the globe stand to gain from digital ID

Roughly one billion people globally lack any form of identification.[54] As a result, they can be denied access to critical services and cannot fully participate in social, economic, or political systems. An additional 3.4 billion have some type of high-assurance identification but limited ability to use it in the digital world.[55] For example, they may have no access to the internet or a smartphone. The remaining 3.2 billion participate in the digital economy and have a form of identification, digital or otherwise, but may not be able to use that identification effectively and efficiently online (Exhibit 2). All of these people stand to gain from digital ID, which can unlock value by promoting inclusion, formalization, and digitization.

The digital ID opportunity starts with the one billion individuals who lack identification

About one billion people are estimated to lack any form of legally recognized identification, hampering their economic, social, and political participation. These individuals primarily live in lower middle-income countries, with 82 percent living in South Asia and sub-Saharan Africa and 16 percent living in other middle-income countries. The identification gap is comparable across gender and income in high- and middle-income countries, but in lower-income countries it disproportionately affects women and low-income individuals. About 45 percent of women in low-income countries lack identification, compared with 30 percent of men.[56] In this case, political, social, and cultural factors influence each gender's ability to get identification.[57]

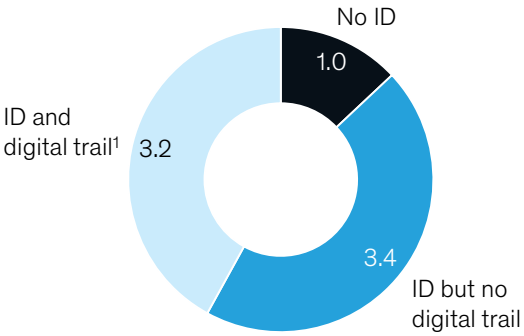
Lack of identification can perpetuate the economic exclusion threatening the livelihood and well-being of billions of people around the world today. High-assurance identification is often required to participate commercially, whether to access financial services, enter labor or property markets, or even to purchase a mobile phone. In response, the United Nations' Sustainable Development Goals promote legal identity for all, especially birth registration, by 2030.[58] Furthermore, digital ID is increasingly seen as a prerequisite to participate in the digital economy, for example in digital finance. Digital inclusion is considered so important to promote economic development that the United Nations has highlighted digital inclusion as a key enabler for 13 of the 17 Sustainable Development Goals.[59] Examples range from improving quality of education through digital payments to teachers that help to reduce leakages and absenteeism, to increasing access to affordable and clean energy via mobile pay-as-you-go methods for solar panels and other clean technologies.

[54] Global ID4D Dataset, World Bank, 2018.
[55] 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 be among the population with some form of legally recognized ID.
[56] Global ID4D Dataset, World Bank; "Global ID coverage by the numbers: Insights from the ID4D Findex survey," World Bank, 2018.
[57] *Digital finance for all: Powering inclusive growth in emerging economies,* McKinsey Global Institute, September 2016; *The power of parity: How advancing women's equality can add $12 trillion to global growth*, September 2015.
[58] Sustainable Development Goal 16: Targets and indicators, 16.9, United Nations, sustainabledevelopment.un.org/sdg16.
[59] *Igniting SDG progress through digital financial inclusion,* Office of the United Nations Secretary-General's Special Advocate for Inclusive Finance for Development, September 2018.

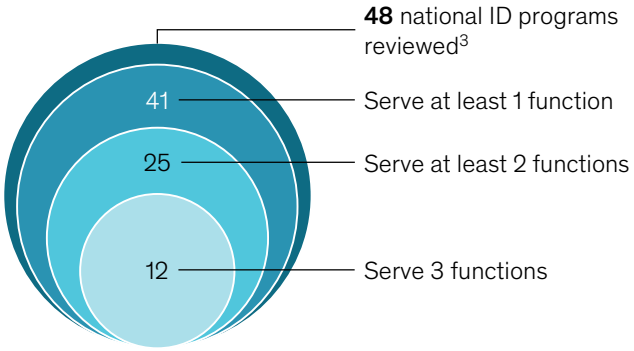
Exhibit 2

Across the globe, an estimated one billion people lack a legal form of identification.

ID coverage
Population, billion people



ID functions
Number of reviewed ID programs serving functions in economic, social, and political use cases



1. 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.
2. "No ID" population figures are based upon 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.
3. Data from ITU 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 examined into three categories: economic (eg, financial services KYC), social (eg, health services), and political (eg, voting). The ID programs in Algeria, Malawi, Mozambique, Nepal, Ukraine, and Vietnam did not have any linkages to the economic, social, or political use cases analyzed and serve primarily as foundational IDs.

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

People cannot use formal financial services—including deposit accounts, payment services, and credit—without some form of identification that enables providers to authenticate their identity, thereby minimizing fraud and satisfying KYC regulations. Even when people have identification, they cannot register remotely for financial products if their ID cannot be authenticated online or through another digital mechanism. Indeed, of the approximately 1.7 billion people without a bank account in 2017, one in five attributed the absence to a lack of necessary identification documents.[60]

Identification is also often required for legal employment in formal labor markets, for recognition as a business, to buy or sell property, or to assert the right to an inheritance.[61] This can lead to the exclusion of unidentified people from economic life. For example, in Nepal a citizenship certificate is required to register land or property ownership or open a bank account, restricting economic activity for the 13 percent of men and 26 percent of women who do not have the necessary identification. [62]

Adequate identification can be a requirement for access to the digital economy, cutting off individuals without an ID. Registration of individuals using prepaid SIM cards is mandatory across 147 countries, and telecom companies are required to validate identification documents or biometrics in countries such as China, India, Indonesia, and Peru.[63] As a result, individuals without an ID are often excluded from mobile ownership and internet connectivity.

Lack of identification can also contribute to social exclusion. High-assurance identification is often required to prove a right to live within a country as well as to gain access to basic goods and services such as education, healthcare, and government benefits, a core underpinning of physical well-being and economic and social participation. For example, a study by the Center for Global Development found evidence that the introduction of identification requirements

60 *Global Findex Database 2017: Measuring financial inclusion and the fintech revolution*, World Bank, 2018.
61 Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?*, Center for Global Development, October 2017.
62 Ibid.
63 *Access to mobile services and proof-of-identity: Global policy trends, dependencies, and risks*, GSMA, 2018.

for health and nutrition programs in Peru led to significant decreases in enrollment of vulnerable infants.[64] The link between identification and medical access has been identified around the world, including in a recent study that found a relationship between birth registration and childhood vaccinations in the Dominican Republic.[65] Providing ID could make the delivery of these critical services more effective.

An inability to reliably identify intended beneficiaries also introduces significant barriers for people who rely on government benefits. Governments in developing nations, such as Tanzania, often use community monitoring to ensure that disbursements are made to their intended recipients in communities with low ID coverage. Although such processes can make disbursements more effective and reduce waste, they significantly reduce the financial flexibility of beneficiaries and create unnecessary hardship by increasing time and transportation costs.[66] In India, widespread lack of effective identification before the introduction of the Aadhaar ID had a significant impact on the subsidy system for liquefied petroleum gas cylinders for household use. Since cylinders were sold to households at heavily subsidized rates but businesses were required to pay market prices and taxes, buyers on the extensive black market leveraged the lack of identification among citizens to illegally divert a significant number of cylinders to commercial use, and therefore reduced energy access for poor households while inflating government expenses. The launch of the Aadhaar digital ID has had a dramatic effect on this issue by allowing the government to replace the subsidies with targeted direct payments to needy families, providing significant government savings while improving energy access for the worst off.[67]

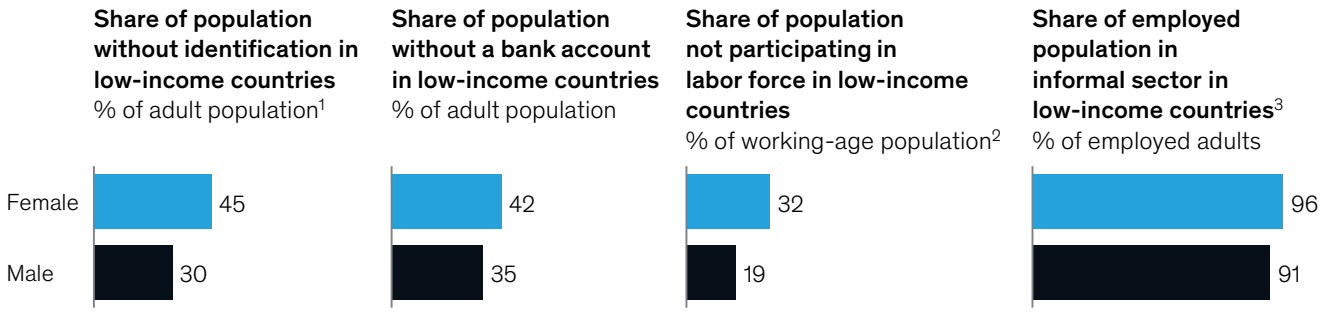
Finally, high-assurance identification is required to participate politically, barring many individuals from voting. This problem can be pervasive in developing economies as well as developed economies, highlighted by the recent intense political debate in the United States over voter ID laws. A 2007 study by the National Democratic Institute and Latin American Faculty of Social Sciences found that lack of proper identification was the main reason that indigenous voters in Guatemala voted at a significantly lower rate than other ethnic groups.[68] Strict and complicated identification requirements for voter registration also contributed to extremely low voter registration in Burkina Faso's 2010 election and had a large impact on female voters, who faced disproportionate difficulties acquiring the necessary documentation.[69]

Women disproportionately lack identification across the world, contributing to their higher levels of economic, social, and political exclusion (see Exhibit 3). In low-income countries, 45 percent of women over the age of 15 lack identification, compared with only 30 percent of men. MGI research has found that women are often unable to set up their own businesses because they lack access to financial services and property titles, and are more likely to be in the informal labor market without being able to develop portable skills and experience as they move from one temporary job to another.[70] Exclusion from formal labor markets means that while women make up more than half of the world's working population, they generate only a fraction of global GDP. A lack of identification is also a major barrier to financial inclusion for women, as illustrated in a global study that found 17 percent of unbanked women cite a lack of documentation as the primary barrier to opening an account.[71] In Pakistan, where the government emphasized female registration for its biometric program that provided IDs to 40 million women, program managers reported that women who received IDs were

[64] William Reuben and Flávia Carbonari, *Identification as a national priority: The unique case of Peru,* Center for Global Development, working paper number 454, May 2017.
[65] Steve Brito, Ana Corbacho, and Rene Osorio, "Does birth under-registration reduce childhood immunization? Evidence from the Dominican Republic," *Health Economics Review,* 2017, Volume 7, Number 14.
[66] Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?*, Center for Global Development, October 2017.
[67] Ibid.
[68] *Barriers to electoral participation in Guatemala: Diagnostic of 4 municipalities*, FLACSO-Guatemala, 2007.
[69] "Burkina Faso campaign brings 16,000 women closer to voter registration," National Democratic Institute, October 2012.
[70] *The power of parity: How advancing women's equality can add $12 trillion to global growth*, McKinsey Global Institute, September 2015.
[71] Mariana Dahan and Lucia C. Hanmer, *The identification for development (ID4D) agenda: Its potential for empowering women and girls—background paper,* World Bank working paper number 99543, September 17, 2015.

Exhibit 3

Women in low-income countries face barriers in identification, financial inclusion, and labor market participation.



1. Adult population defined as individuals above age 15. Based on a World Bank survey of foundational ID in 18 low-income countries.
2. Working-age population defined as individuals between the ages of 15 and 64.
3. Based on latest available data on the formal and informal economies for 16 low-income countries from the International Labour Organization (ILO).

Source: World Bank ID4D; Findex; ILO; McKinsey Global Institute analysis

significantly more likely to exercise their right to vote and express their individual identity while enjoying legal protection as registered citizens of the country.[72]

Digital ID unlocks new opportunity for the 3.4 billion individuals who have an ID but have limited ability to use it in the digital world

Digital ID can provide new uses and added convenience to the 3.4 billion individuals who have an ID but are limited in their ability to use it online. More than 500 million Africans, or 45 percent of the total population, fit into this category, including almost 60 percent of people in both Egypt and the Democratic Republic of Congo. This group encompasses people with both conventional and digital IDs, including approximately 900 million people in India, but limited participation in or access to digital ecosystems via smartphones.

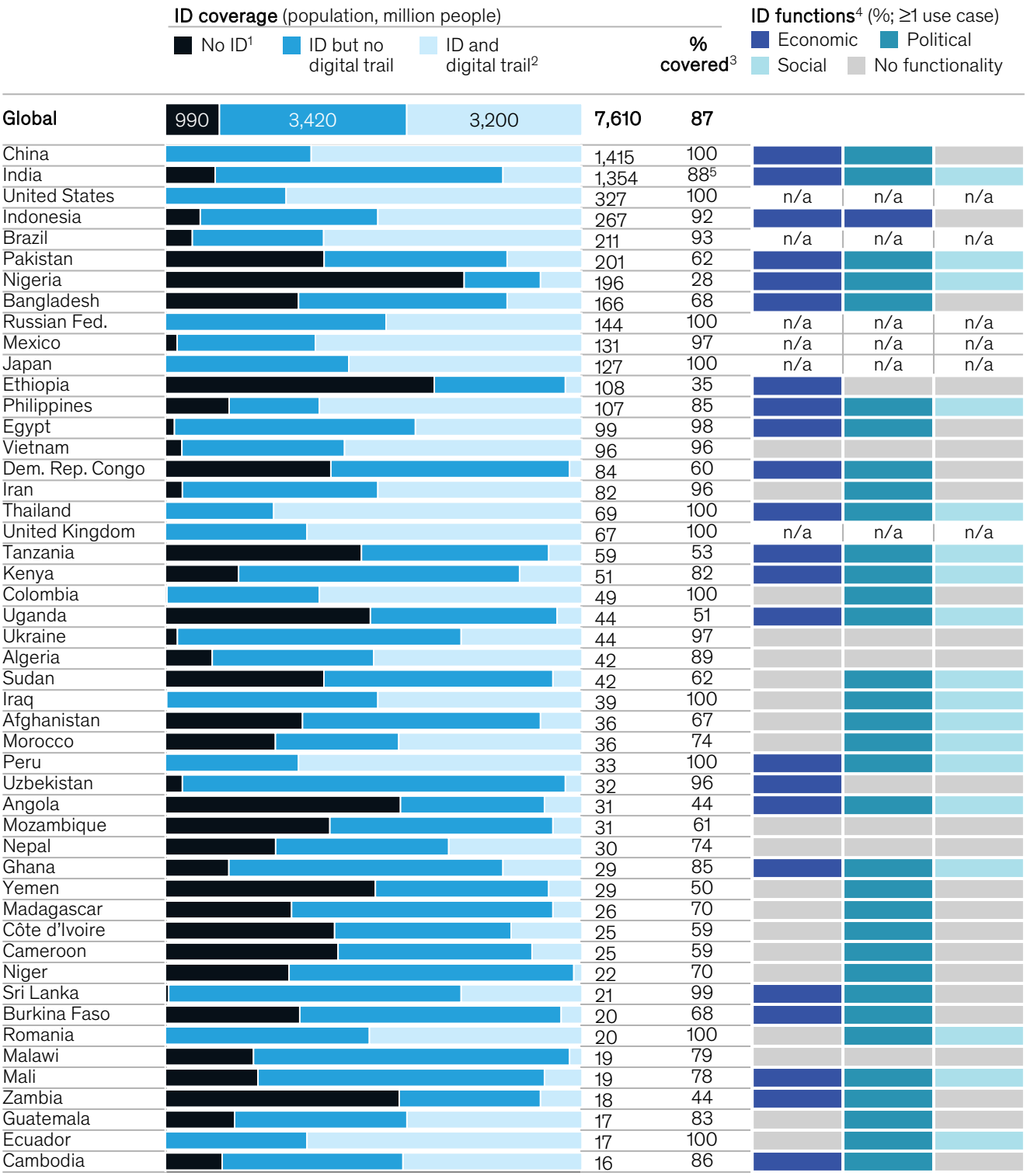
While this group of people has some form of high-assurance physical identification, this is often insufficient for some use cases and has limited utility. Businesses and governments typically take a pragmatic approach to creating identification systems, focusing on the particular instance they are trying to solve for. National identification systems also tend to be narrow in scope, typically unlocking only a narrow range of use cases. Research prepared for the International Telecommunication Union and the Gates Foundation reviewed 48 national identification programs, including digital and nondigital programs, and found that more than 30 percent of them were focused on use cases in only one sphere analyzed: economic, social, or political (Exhibit 4).[73] Just 12 of the systems reviewed addressed use cases across all three of these functions—for example, the National Database and Registration Authority (NADRA) in Pakistan issues IDs that enable digital banking, are linked to government transfer programs, and are used for voter registration. Due to its inherent flexibility and adaptability, a digital ID system could be utilized across use cases and help address the functionality gap in existing ID programs.

Beyond consolidation of uses, moving from physical identification to digital ID systems enables users to take advantage of benefits from digital systems, which can reduce time and cost while improving convenience and quality. Examples include more convenient services, such as through e-government or streamlined customer onboarding, and improved sharing of personal information, such as medical data or employment records. In addition, the security benefits of high-assurance digital ID can help ensure that the approximately 800 million people projected to join the ranks of internet users by 2022 can enter the digital world with control over their data and online identity.[74]

[72] Ibid.
[73] *Review of national identity programs,* International Telecommunication Union, May 2016.
[74] *By the numbers: Projecting the future of digital transformation (2017-2022),* Cisco.

Exhibit 4

Existing ID systems vary widely around the world.



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 can improve efficiency and experience for the 3.2 billion individuals who already participate in the digital economy

About 3.2 billion people with high-assurance identities participate in a rich digital ecosystem, but in that digital world, they typically use a patchwork of disaggregated identities characterized by security flaws, limited user control, and inefficiencies.[75] These people are primarily concentrated in North America and Europe, with millions more in India and China. This group includes many of the roughly 2.2 billion individuals enrolled in one of the over 40 national or non-national digital identity systems that we estimate exist today.

The rapid expansion of digital ecosystems means that individuals are increasingly sharing large amounts of personal data through low-assurance digital interactions, sacrificing privacy and security. The amount of online data created, stored, and transmitted is rapidly increasing. The International Data Corporation forecasts that by 2025 the global datasphere will grow to 163 zettabytes (trillion gigabytes), ten times the 16.1 zettabytes of data generated in 2016.[76] This growth in the amount of data used by individuals is global and occurring in both developed and developing markets. For example, India's monthly mobile data consumption per user reached 8.3 GB in 2018, over 54 times the level in 2016.[77]

Few individuals are in control of their digital identities. For example, only 10 percent of respondents in a global survey had ever done six or more of eight common privacy-protecting activities such as private browsing, disabling cookies, and opt-in/out functions.[78] Well-designed digital ID explicitly builds in mechanisms to help people manage their privacy settings and minimizes the amount of personal information they need to enter. Furthermore, the credentials that people use to establish online identities are typically insecure. For example, phone numbers and email addresses are often used and easily stolen, providing access to a range of personal information from social media to online shopping and financial services.[79] When multiple credentials, such as a phone number and a username, are compromised, even security measures such as two-factor authentication can be circumvented.[80] Digital ID, however, uses secure credentials such as biometrics, PINs and passwords, or smart cards to provide high-assurance authentication and to ensure security across critical applications in the digital world.

Increased digitization and insecure accounts combine to pose increasing risk for the digital economy and for individual privacy. For example, in 2017, $16.8 billion was lost in the United States due to identity fraud, and since 2013, the United States and India have experienced the breach of more than 6.2 billion and 394 million customer data records, respectively.[81] Such breaches create additional cost for individuals and providers in both money and time. Personal information is also at risk from unauthorized access. For example, Equifax, a massive credit rating agency in the United States, stores highly personal information such as addresses, financial documents, and Social Security numbers. An external party that breached Equifax's systems gained access to 146 million individuals' private information. Digital ID can help reduce these risks by providing high-assurance verification and authentication.

Beyond security concerns, many active internet users are unable to keep track of their digital footprint and find it inconvenient and time-consuming to register, authenticate, and manage their online accounts. The average number of online accounts registered to one email address ranges from 90 to 130 and is roughly doubling every five years.[82] Individuals forget 11 passwords per year; about 30 percent of calls to banks' call centers are requests for account access due to misplaced or forgotten passwords.[83] Digital ID could deliver time savings to

[75] Calculated as the population with active social media use as captured in the We Are Social *Global Digital Report 2018*. These social media users are presumed to be among the population with some form of legally recognized ID.
[76] *Data age 2025: The evolution of data to life-critical,* Seagate, March 2017.
[77] *Indian telecom services performance indicators*, Telecom Regulatory Authority of India, as of September 2018, and June 2016.
[78] *The value of our digital identity,* BCG, November 2012.
[79] Nelson Cicchitto, "Why do we use user names and passwords?," *Forbes,* October 31, 2017.
[80] Lily Hay Newman, "Phone numbers were never meant as ID. Now we're all at risk," *Wired,* August 25, 2018.
[81] *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.
[82] Tom Le Bras, "Online overload—it's worse than you thought," Dashlane, July 21, 2015.
[83] *The future of identity in banking,* Accenture, 2013.

individuals by consolidating access to online accounts as well as savings for institutions, for example from reduced costs associated with online customer support. 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.

The state of adoption of digital ID so far is mixed, indicating room for improvement and growth

Forty or more national or non-national digital identity programs exist today (Exhibit 5). Roughly 1.2 billion people with digital IDs live in India alone, registered in the Aadhaar program, which began in 2009. Programs led by banking consortiums have been successfully integrated into financial and government services in Norway and Sweden, and the Estonian e-ID has led a successful transition to e-government services.

Yet many digital ID programs have achieved low coverage levels, with the percentage of the population included as low as single digits. Most enable only a small fraction of the nearly 100 uses we have identified for digital ID. Several existing programs with low adoption rates have been affected by limited functionality, poor user experience, and difficulties coordinating across stakeholders. Adoption of the eID in Nigeria stalled in 2017 amid issues with public-private partnerships used to launch the program and difficulty integrating uses and functionality of more than 13 separate identification systems run by separate government agencies.[84] Gov.UK Verify in the United Kingdom has experienced slower than expected adoption—currently less than 10 percent of the population—and has so far been limited to a relatively small set of government-related uses.[85] Overall, most existing digital ID programs do not yet capture all potential value, and additional opportunity exists for greater value creation.

The digital-ID opportunity grows as technology improves, costs decrease, and access to the internet and smartphones rises

30%

The amount the price of a smartphone fell from 2008 to 2016 in Asia

The opportunity created by digital ID has grown significantly as technology for digital registration and authentication, such as biometric capture and recognition, and electronic card-based data storage and sharing have improved. At the same time, the costs associated with the technology and implementation of digital ID have fallen dramatically, and access to the technology necessary for individual participation is growing every day—more than four billion people have access to the internet and one billion to a biometrically enabled smart mobile device.[86]

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. Nearly a quarter-billion new users came online for the first time in 2017. Africa is experiencing the fastest growth in internet usage, with a 20 percent increase each year.[87] From 2008 to 2016, the price of a smartphone, the primary entry point for access to the internet in many emerging markets, fell by 30 percent in Asia, about 25 percent in Latin America and the Caribbean, and about 20 percent in Africa.[88] Improved technology can facilitate increased and more secure storage and sharing of data. For example, near-field communication, a set of protocols that permits two electronic devices to transfer information when close together, allows contactless sharing and could be integrated with digital ID.

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.[89] Biometric technology for registration and authentication is becoming more accurate and less expensive.[90] For example, iris-based authentication technologies can give false rejection

[84] *The state of identification systems in Africa: A synthesis of country assessments,* World Bank, 2017.
[85] "GOV.UK Verify Dashboard," Gov.UK.
[86] *Global digital report 2018*, We Are Social, January 2018; *Technology Landscape for Digital Identification*, Identification for Development, World Bank, 2017.
[87] Ibid.
[88] *The 2015–16 affordability report,* Alliance for Affordable Internet, 2016.
[89] *Voices,* "Demystifying technologies for digital identification," blog entry by Luda Bujoreanu, Anita Mittal, and Wameek Noor, February 27, 2018, blogs.worldbank.org/voices/demystifying-technologies-digital-identification.
[90] *Technology landscape for digital identification,* Identification for Development, World Bank, 2017.

Exhibit 5

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

rates as low as 0.2 percent and false acceptance rates of 0.0001 percent.[91] The average selling price of a fingerprint sensor found in a mobile phone fell by 30 percent in 2017 alone.[92] Bar codes on cards, which once stored only numerical data, can now secure signature, fingerprint, or facial data.[93] 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.[94]

30%

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

Digital ID has the potential for misuse without the right governance and controls in place

Digital ID, much like other technological innovations such as social media, the ubiquitous GPS, and even nuclear energy, can be used to create value or inflict harm. Digitization could enable an ID provider to know vast quantities of information about an individual, while analytics could enable the provider to predict an individual's behavior. This type of knowledge is largely unprecedented and could tilt the balance of power to those who collect and hold that information. Without proper controls, digital ID system administrators with nefarious aims, whether they work for private-sector firms or governments, could gain access to and control over personal data and use it against the interests of individuals in the system.

Administrators of a digital ID system could misuse digital ID for economic or noneconomic reasons—for example, to profit from the collection and storage of personal data or for surveillance, targeting, and persecution of individuals or groups. Such misuse could affect individuals and institutions in a number of ways. ID providers could access data to exert control over both individuals and institutions that they interact with by identifying constituent or consumer behaviors and targeting both individual and institutional rights.

The unauthorized use of personal data for economic gain has been an issue of rising concern for individuals globally. One study identified more than 40 popular smartphone applications that were exploiting personal information of individuals without their consent or knowledge.[95] In a widely publicized incident, the political analysis firm Cambridge Analytica was accused of misusing voter data during the lead-up to the 2016 UK "Brexit" referendum on leaving the European Union to target potential voters with highly effective social media ads.[96] The wide publicizing of this incident and others like it may be indicative of growing concern about data privacy and systemic misuse that could potentially be highly relevant to digital ID programs. If institutions, whether as ID providers or as requesting parties, are able to use consolidated data tied to an individual's digital ID for economic or other gain without user consent, then digital ID could increase the magnitude of the risk of misuse. Digital ID programs that enable data sharing and are tied to large amounts of user data would be at significant risk, and they are likely to face the same issues with data misuse that have already been seen throughout other elements of the digital ecosystem.

In political or economic environments where governments or private actors are intentionally targeting individuals, digital ID could provide the tools necessary to make such targeting more subtle and efficient. Whereas traditional IDs place some technical limits on the control that institutions can enforce on individuals, due to the difficulty of identifying targeted individuals in all situations and purposefully excluding them from critical services, digital ID might allow for surveillance and political control to manifest in new ways. For example, authoritarian regimes could use digital ID systems to tie political loyalty to access to critical government or private-sector services. Through purposeful exclusion of targeted individuals, such as political dissidents or ethnic minorities, regimes could dramatically increase the efficacy of existing systems of surveillance and repression.

---

91 Ibid.
92 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.
93 Ibid.
94 Dylan Yaga et al., *Blockchain technology overview,* National Institute of Standards and Technology, US Department of Commerce, https://doi.org/10.6028/NIST.IR.8202.
95 Shawn Salamone, "Student, faculty researchers expose secret misuse of personal data by mobile apps," Baldwin Wallace University, September 21, 2017.
96 Jamie Doward, Carole Cadwalladr, and Alice Gibbs, "Watchdog to launch inquiry into misuse of data in politics," *Guardian,* March 4, 2017.

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, or social media.

Digital ID would not necessarily increase the magnitude of abuses tied to an identity, but it does have the potential to open up new options for control of individuals and misuse of their personal information. Digital ID can form the foundation of a host of applications related to many aspects of an individual's life, work, and social interactions. The potentially pervasive nature of digital ID makes it akin to other dual use technologies, like nuclear energy, that are designed to generate benefit but are also capable of being used for harmful or undesirable purposes.[97] Modern history is a reminder that atrocities can occur when people are persecuted based on factors such as race or ethnic identity. In the wrong hands, digital ID might facilitate such persecution.

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. The World Bank Group and the Center for Global Development facilitated the development of ten principles on identification for sustainable development endorsed by 24 organizations such as the Bill & Melinda Gates Foundation and Omidyar Network.[98] These principles provide guidelines for managing the risks and promoting sustainable development of a digital ID system (see Box 1, "The World Bank and the Center for Global Development facilitated the development of ten principles for a sustainable digital ID system"). The organizations endorsing these shared principles recognize the potential of strengthened identification systems to support development and the achievement of the UN Sustainable Development Goals.

Significant gaps in the current use and quality of identification globally indicate the potential for digital ID to create value for individuals, institutions, and countries. Digital ID can increase high-assurance ID coverage and facilitate greater inclusion, formalization, and digitization. In the next chapter, we present a clear framework of 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.

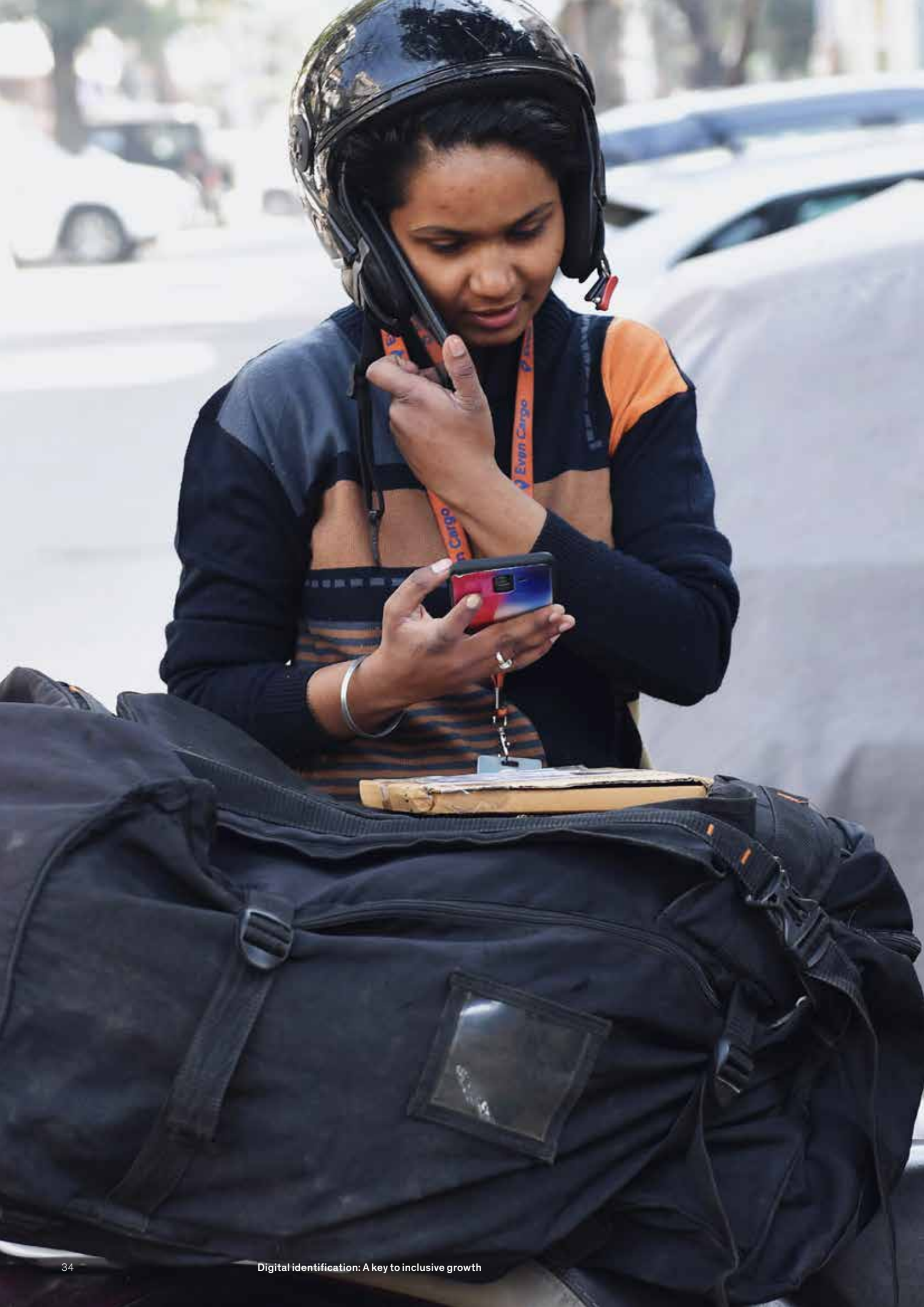
[97] Koos van der Bruggen, "Possibilities, intentions and threats: Dual use in the life sciences reconsidered," *Science and Engineering Ethics*, 2011, Volume 18, Issue 4, pp. 741–56.

[98] *Principles on identification for sustainable development: Toward the digital age*, World Bank, 2018. The endorsing organizations are: African Development Bank; Asian Development Bank; Bill & Melinda Gates Foundation; Center for Global Development; Digital Impact Alliance; FHI 360; ID4Africa; International Organization for Migration; International Union of Notaries; Mastercard; Omidyar Network; Open Identity Exchange UK/Europe; Organization of American States; OSCE Office for Democratic Institutions and Human Rights; Plan International; Privacy and Consumer Advisory Group to the Government Digital Service and GOV.UK; Secure Identity Alliance; GSMA; UN World Food Programme; UNHCR, The UN Refugee Agency; United Nations Children's Fund; United Nations Development Programme; United Nations Economic Commission for Africa; and World Bank Group.

Box 1

The World Bank and the Center for Global Development facilitated the development of ten principles for a sustainable digital ID system

1. Ensure universal coverage for individuals from birth to death, free from discrimination
2. Remove barriers to access and usage and disparities in the availability of information and technology
3. Establish a robust—unique, secure, and accurate—identity
4. Create a platform that is interoperable and responsive to the needs of various users
5. Use open standards and ensure vendor and technology neutrality
6. Protect user privacy and control through system design
7. Plan for financial and operational sustainability without compromising accessibility
8. Safeguard data privacy, security, and user rights through a comprehensive legal and regulatory framework
9. Establish clear institutional mandates and accountability
10. Enforce legal and trust frameworks though independent oversight and adjudication of grievances, privacy, and user rights


Evon Cargo

2 The economic value of digital ID

Digital ID facilitates many types of interactions between two parties, most often individuals and institutions, producing benefits for both. Individuals can use identification to interact with businesses, governments, and other individuals in six roles: as consumers, workers, microenterprises, taxpayers and beneficiaries, civically minded individuals, and asset owners. Correspondingly, institutions can utilize 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 including citizens and residents; and as asset-based service providers and buyers, interacting with individual asset owners.

In this chapter, we develop a framework to understand and analyze the economic, social, and other benefits from digital ID informed by the many ways individuals and institutions interact with digital ID. After establishing the framework for how digital ID is used, we then examine the value generated by individual use cases associated with different interaction types. We find that individuals benefit most from greater inclusion in financial services and through greater access to employment. Public and private institutions benefit most from cost savings due to more efficient service provision and from reduced fraud related to benefits, payroll, and taxes.

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 minded individuals, and asset owners (Exhibit 6). All individuals can use digital ID as consumers. Consumers can interact with commercial providers of goods and services and can use their ID in a variety of ways, from registration and authentication to payments and account management. Examples include interactions between individuals who would like a bank account and a bank that requires proof of identity in order to control fraud and to satisfy KYC regulations.

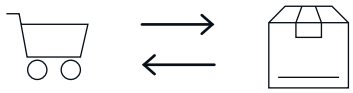
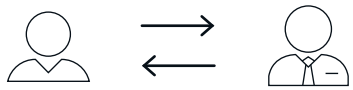
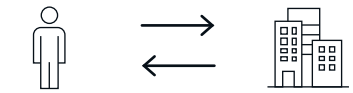
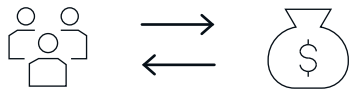
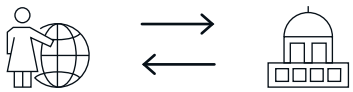
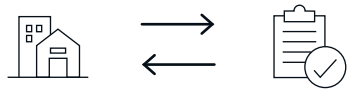
The working population could use digital ID in many ways, for example on talent matching platforms, for onboarding, and for authenticating payroll. Individuals who are self-employed or engaged in microenterprises could use digital ID to facilitate customer interactions as well as connections with the platform or institution they contract with, helping to formalize their business and increase their efficiency.

People around the world could use digital ID as taxpayers and beneficiaries in public-sector interactions. In this case, digital ID could be used to facilitate e-government services, fraud reduction from ghost benefits recipients and ineligible beneficiaries, and reduction of tax evasion. Civically engaged individuals could use digital ID to vote online, for example, or verify their political donations.

Lastly, asset owners could use digital ID to connect with buyers of their assets and asset-based service providers. Our analysis concentrates primarily on interactions of this type in the agricultural sector: individuals could use digital ID to formalize ownership of land, access land-based credit, and improve agricultural productivity through long-term investment.

Exhibit 6

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

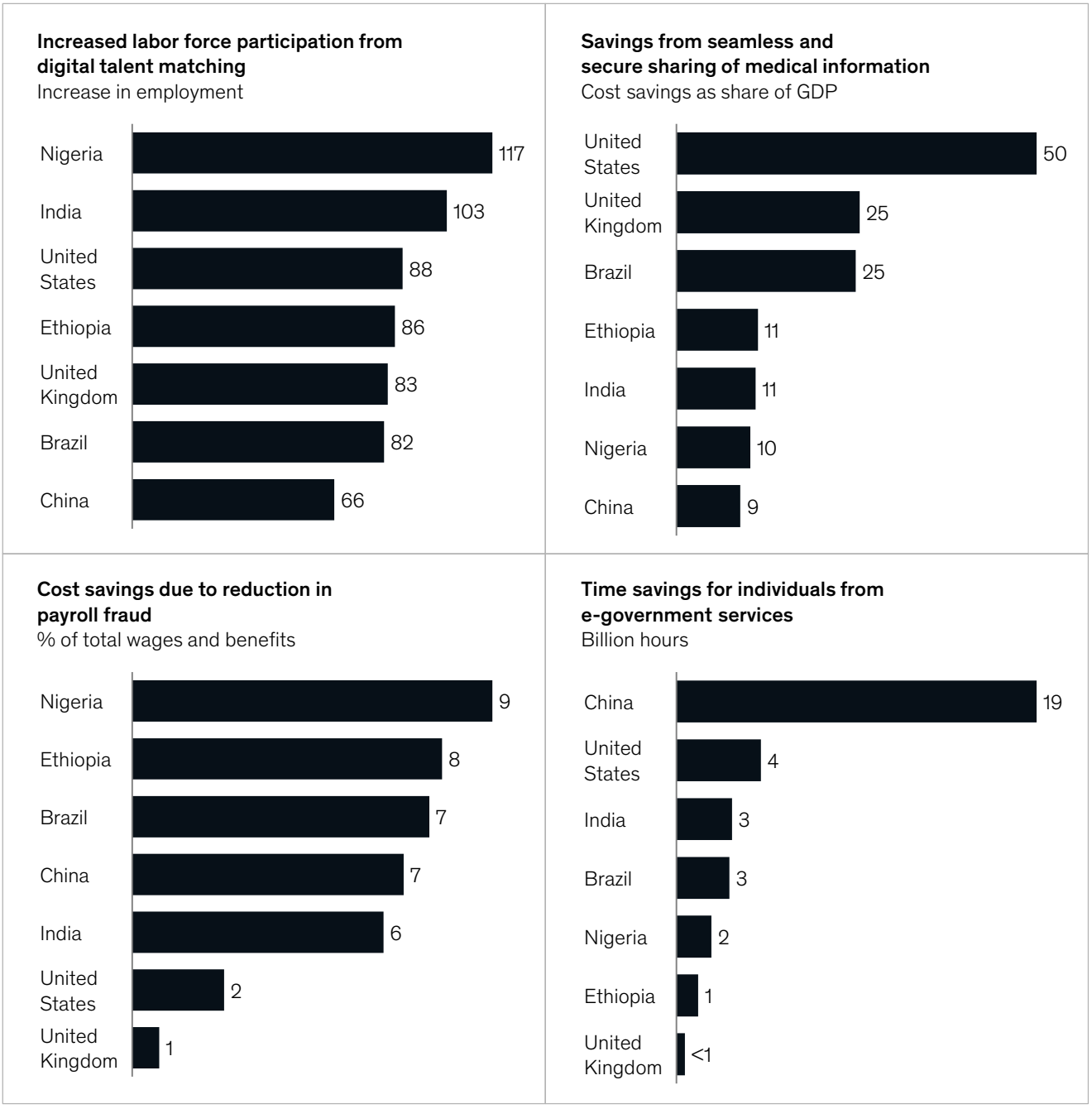
Source: McKinsey Global Institute analysis

Our analysis of all of these interactions allows us to pinpoint the most important benefits of digital ID. These include increased financial inclusion, cost savings, improved labor market efficiency, time savings, and fraud reduction (Exhibit 7). Increased financial inclusion, particularly in emerging economies, is the most significant benefit associated with consumer interactions—in this case with financial services providers. Improved labor market efficiency stems from the way digital ID can facilitate interactions between workers and employers as well as those between microenterprises and their prospective customers. Time and cost savings and fraud reduction span many types of interactions.

Exhibit 7

Countries adopting digital ID schemes have the potential to capture significant value in a wide variety of use cases.

Four examples of how digital ID can create value
Potential benefits, 2030E



Source: McKinsey Global Institute analysis

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.

Digital ID can increase access to financial services, particularly in emerging economies

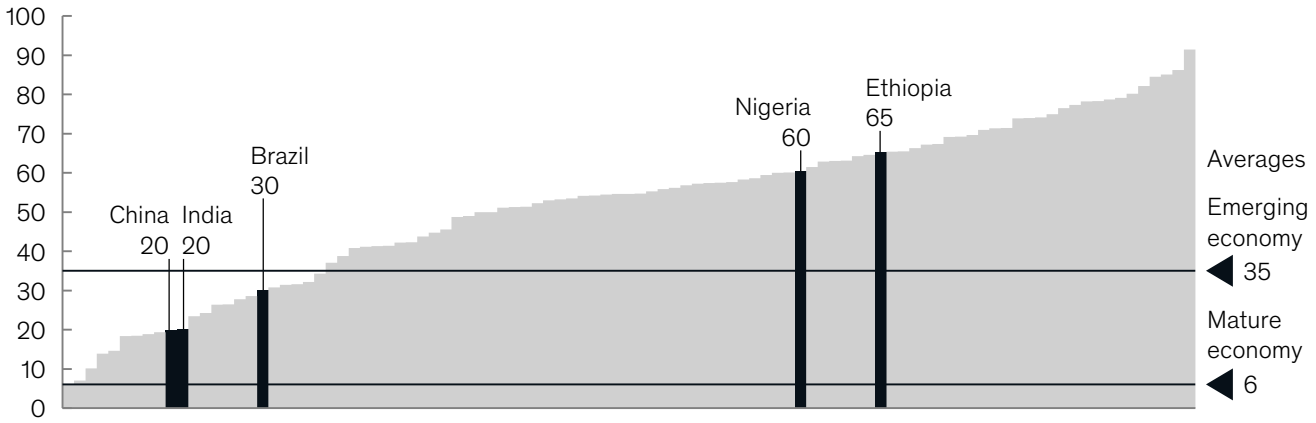
About two billion individuals currently lack access to a bank account, according to the World Bank, with many more able to access only a limited range of products, often at high cost.[99] Across the Middle East and Africa, more than half the adult population (a total of 500 million people) does not have a bank account, while 35 percent of the entire adult population in emerging economies lacks a bank account (Exhibit 8).[100] Previous MGI research found that rapidly spreading digital technologies create an opportunity to provide financial services at much lower cost, and therefore profitably boost financial inclusion, enabling large productivity gains across the economy (see Box 2, "The benefits of financial inclusion").[101] Digital ID can promote the spread of digital financial services by allowing banks to use high-assurance authentication to enable remote customer registration and satisfy Know Your Customer, or KYC, requirements that mandate due diligence by banks on the identity of account holders. In this report, we estimate that digital ID could increase access to digital financial services, including bank accounts, digital payments, insurance, and credit for more than one billion individuals who are financially excluded today.[102]

Exhibit 8

Digital ID can help reduce barriers to financial access in emerging economies and help foster financial inclusion for the 35 percent of the population without a bank account.

35% of people in emerging economies do not have a bank account

% of people ages 15+ without a bank account[1]



Factors contributing to financial exclusion in emerging economies

% of unbanked individuals citing as a primary reason

18% Lack of necessary documentation

21% Financial institutions too far away

27% Financial services too expensive

1. Set of 70 emerging countries, defined as countries not classified as high income by the World Bank. Highlighted countries represent emerging economies within our set of focus countries.

Source: Global Findex Survey, 2018; McKinsey Global Institute analysis

According to MGI's report on digital finance, most people and small businesses in emerging economies today transact exclusively in cash, have no safe way to save or invest money, and do not have access to credit beyond information lenders and personal networks. Consequently, a significant amount of wealth is stored outside the financial system and credit is scarce and expensive, thus preventing individuals from engaging in economic activities.[103] Overall, the research estimated that widespread use of digital finance could boost the annual GDP of all emerging economies by $3.7 trillion by 2025, a 6 percent increase over the status quo. Digital identification could be a critical tool in unlocking this value.

For individuals, there are often three main barriers to opening a bank account: a lack of necessary documentation, branches that are too far away, and accounts that are too expensive. Across emerging economies, 18 percent of unbanked individuals cite lack of documentation as a primary account barrier, with 21 percent citing distance from branches and 27 percent citing the costs of financial services.[104] Digital ID can address a lack of documentation by providing individuals high-assurance identification. For the approximately one billion people who currently have no ID, a digital ID could provide the foundational ID necessary to authenticate their identity with financial institutions. For people with an ID,

[103] *Digital finance for all: Powering inclusive growth in emerging economies*, McKinsey Global Institute, September 2016.
[104] Responses based on the World Bank's Findex survey allowed individuals to choose multiple primary barriers to opening an account. See *Global Findex Database 2017: Measuring financial inclusion and the fintech revolution*, World Bank, 2018.

Box 2

The benefits of financial inclusion

Financial inclusion benefits individuals, microenterprises, financial service providers, and governments. Access to financial services enables people to save for big ticket items, smooth seasonal income, manage unexpected economic shocks, and use credit to invest in their farms, businesses, and children. Financial inclusion also helps promote gender equality, as women around the world disproportionally lack financial access. Previous MGI research has found that when women open bank accounts, they tend to spend more than men on food, education, and healthcare, improving family welfare and productivity for families.[1] Beyond access to financial accounts, digital ID use cases that provide direct utility to customers, such as low-cost remittances or direct transfers of government benefits, could encourage new bank account holders to actually use those accounts.

Microenterprises benefit from credit availability and the ability to undertake digital transactions. Today, 40 percent of the roughly 140 million microenterprises in emerging economies lack full access to credit.[2] The associated credit gap—the gap between credit that microenterprises currently can obtain and what they need—amounts to an estimated $718 billion.[3] Financial inclusion helps bridge this gap, giving microenterprises financing they need to thrive. It also enables them to shift away from cash-only businesses, lowering costs and easing cash management, while also building a digital trail to further demonstrate creditworthiness.[4]

Financial service providers can also gain from financial inclusion, which offers them an opportunity to expand their customer base. Particularly when aided by the tools of digital finance, financial institutions can broaden their pool of customers and assess the creditworthiness of potential new borrowers, cost-efficiently.

Finally, governments and broader society profit from financial inclusion. When taxpayers and beneficiaries have bank accounts, governments are better able to digitize their transactions with these individuals, thereby lowering cost, reducing leakage, and improving delivery.

All of these factors together add up to greater formalization, higher productivity, and deeper financial systems across economies. Overall, MGI estimated that widespread use of digital finance could boost the annual GDP of all emerging economies by $3.7 trillion by 2025, a 6 percent increase over the status quo.[5] Digital identification could be a critical tool in unlocking this value.

[1] *Digital finance for all: Powering inclusive growth in emerging economies*, McKinsey Global Institute, September 2016.
[2] *MSME finance gap: Assessment of the shortfalls and opportunities in financing micro, small and medium enterprises in emerging markets*, International Finance Corporation, 2017.
[3] Ibid.
[4] Financial inclusion also aids SMEs, though these are not considered within the scope of this report on digital ID. The estimated credit gap for such enterprises totals $4.5 billion in emerging economies.
[5] *Digital finance for all: Powering inclusive growth in emerging economies,* McKinsey Global Institute, September 2016.

digital ID could help resolve other documentation gaps by authenticating employment, tax, or other financial data.

Digital ID–enabled mobile banking can help address the problem of branch distance by allowing remote registration and enabling banking agents as well as technologies such as micro-ATMs that can bring financial services closer to people. In Estonia, the government has partnered with the Finnish fintech firm Holbi to enable people who hold their e-Residency digital ID to create a bank account without having to step foot in a branch.[105] Although the program is primarily for foreign business owners operating in Estonia, the e-Residency program shows the potential of digital ID in removing distance as a major barrier to opening a bank account. Digital ID can also reduce the importance of distance in long-term account usage by enabling mobile banking solutions, banking agents, and distributed micro-ATMs. Micro-ATMs are portable devices equipped to authenticate digital IDs and generally accessed through business correspondents such as local retail stores.[106] In India, Aadhaar-enabled micro-ATMs have significantly lowered barriers to financial access, with data from the National Payments Corporation of India showing a tenfold increase in Aadhaar-enabled transactions in 2017–18 compared with the previous fiscal year, with the average monthly transaction size increasing by 77 percent from $22 to $39 over the same period.[107]

Digital ID can reduce barriers to financial inclusion associated with account cost by dramatically cutting onboarding and verification costs associated with satisfying KYC requirements. In India, the use of Aadhaar for KYC verification reportedly reduced costs for financial institutions from approximately $5 to approximately $0.70 per customer.[108] Banks could reduce their KYC costs by eliminating manual processing of paper documentation and the need for in-person verification of the account holder's identity, reducing the costs of bank accounts and expanding opportunities for financial access.

Our analysis of emerging economies shows that the increased deposit base resulting from financial inclusion of unbanked individuals could greatly increase access to loans and capital that would directly and indirectly benefit individuals throughout the economy. We find that India, Brazil, Nigeria, and Ethiopia could gain $617 billion, $190 billion, $21 billion, and $2 billion, respectively, in new physical capital from an expanded deposit base by 2030.[109] This capital would take the form of loans extended directly to individuals and microenterprises, as well as broader investment that would spur economic development and activity that benefit workers and institutions. Therefore, digital ID would allow individuals to gain access to credit and benefit from broader investment in the economy. However, as shown by the large potential that we believe remains in India, the introduction of digital ID is not by itself enough to capture the entirety of the value of financial inclusion. Although the introduction of Aadhaar drove an increase in financial accounts from 48 million in 2016–17 to 138 million in 2017–18, 40 percent are still unseeded; individuals continue adapting and learning about the financial system, and banks have not yet transitioned their credit portfolios toward the newly banked population.[110]

Digital ID can improve the efficiency of labor markets in emerging and mature economies

More effective digital talent matching platforms for workers and digital contracting platforms for microenterprises could improve the efficiency of labor markets. Digital ID can play a key role in facilitating the growth of these digital platforms, which could streamline access to labor markets for inactive and unemployed workers and boost labor productivity throughout the economy.

Digital ID facilitates secure and high-assurance digitization of an individual's credentials and transaction history, enabling workers and microenterprises to effectively participate in

[105] Matt Burgess, "You can now set up borderless businesses and bank accounts online as e-residents of Estonia," *Wired,* May 25, 2017.
[106] Ronald Abraham et al., *State of Aadhaar report, 2017–18,* IDinsight, May 2018.
[107] Ibid.
[108] Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?,* Center for Global Development, October 2017.
[109] Figures given in 2018 real dollars.
[110] Ronald Abraham et al., *State of Aadhaar report, 2017–18,* IDinsight, May 2018.

digital talent matching programs. Digital ID–enabled talent matching could improve hiring efficiency by allowing employers to quickly find workers or microenterprises with a high degree of confidence that they have the requisite skills or background for an open position. Microenterprises could leverage digital contracting platforms to build out transaction histories and gain access to formal contracts with governments or larger companies. For individuals, high-assurance talent matching would mean faster hiring, additional employment opportunities, and the chance to find jobs that better fit their skills and qualifications.

Talent matching and contracting programs can enable people in the informal sector to enter the formal economy, providing benefits for both them and the broader society. The informal economy represents all economic activities that are hidden from official authorities for monetary, regulatory, or institutional reasons.[111] Individuals working in the informal sector are often excluded from formal legal protections and have limited access to formal employment, and governments are unable to tap their income for taxation. Large informal economies also reduce overall productivity and have a negative effect on a country's standard of living, with some economists estimating that the informal sector is up to 80 percent less productive than the formal sector, particularly in developing countries.[112]

Online talent platforms also increase labor market efficiencies by speeding the hiring process and cutting the time individuals spend searching between jobs. Previous MGI research has also found that online talent platforms could increase hiring. For example, startups can turn to contingent marketplaces to hire specialized help and lower their business costs; large companies may find it feasible to hire a fractional worker when they would not have hired a full-time worker; and demand may grow for services that people used to perform themselves, from household chores to driving to child care. Additionally, when more people find work and increase their income, their additional spending creates aggregate demand that enables job creation for others.[113]

Although forms of digital talent matching and contracting can be developed without digital ID, as demonstrated by existing platforms including LinkedIn and Freelancer.com, high-assurance authentication of credentials and identity can greatly increase the feasibility of large-scale programs. This would affect the labor force by allowing people who are unemployed, working part time, currently not participating in the labor market, or working in the informal sector to easily gain exposure to a wide variety of employers and effectively communicate their credentials. In addition, digital talent matching with high assurance and authentication would allow employed workers to find work that they are better suited for, increasing overall productivity, and would reduce frictional unemployment as companies use talent matching platforms to shorten their hiring timelines.

70%

The share of the working-age population that is employed in the informal sector in emerging economies

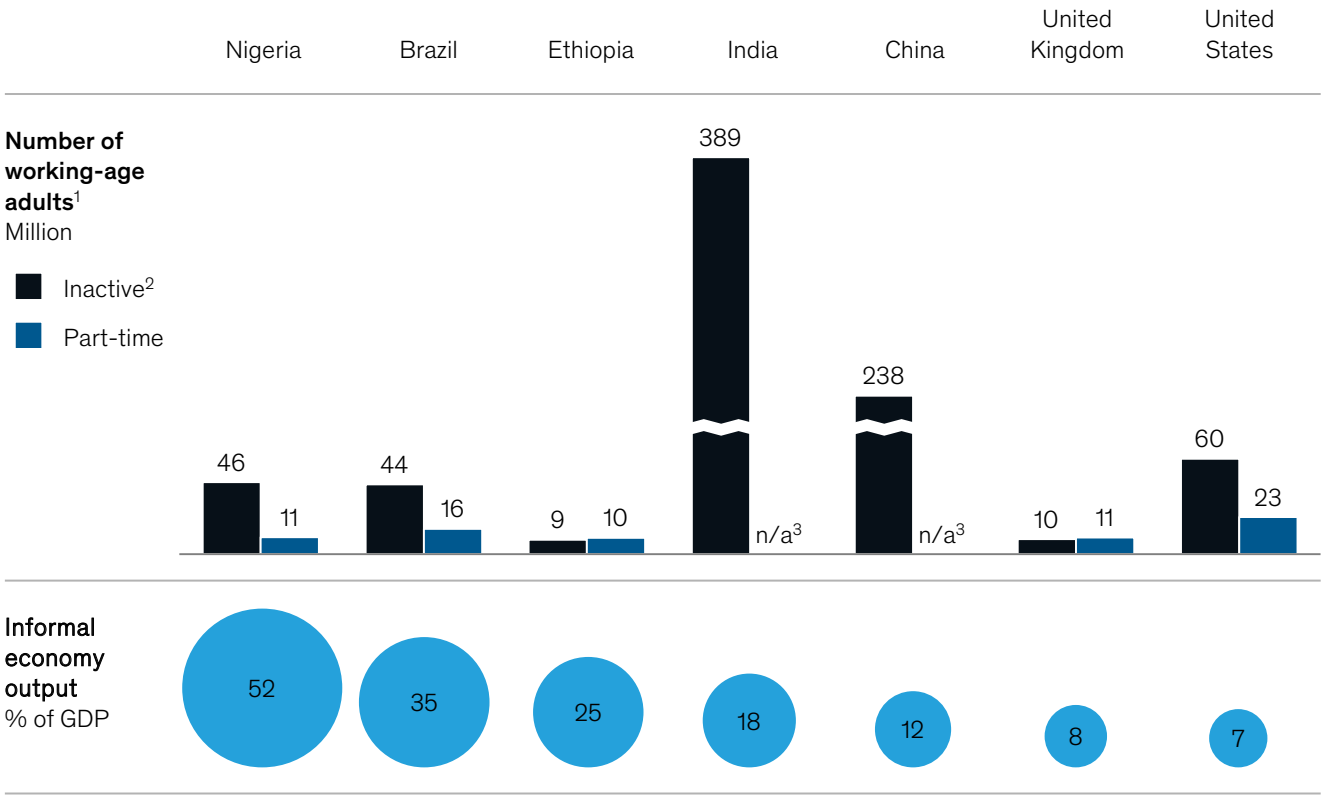
The population of inactive and part-time workers varies across our focus countries, as does the share of the economy driven by the informal sector (Exhibit 9). The size of affected populations will determine the potential impact of digital ID–enabled talent matching platforms. India's large inactive population—about 389 million adults—suggests the large opportunity to be gained from increased labor force participation, particularly from inclusion of women newly able to access the formal economy and employment opportunities across the country. In emerging economies, an average of 70 percent of the working-age population is employed in the informal sector and could benefit from access to the formal economy and broader employment opportunities.[114]

Overall, we estimate that digital ID could increase the reliability of information on talent matching platforms, reduce the friction of registering and creating a profile, and unlock automated work authorization and background checks for workers, enabling increases in employment in our focus countries ranging from 1 percent in China to 2.2 percent in Ethiopia.

[111] Leandro Medina and Friedrich Schneider, *Shadow economies around the world: What did we learn over the last 20 years?,* IMF working paper number 18/17, January 2018.
[112] Matías Busso, María Victoria Fazio, and Santiago Levy, *(In)formal and (Un)productive: The productivity costs of excessive informality in Mexico*, Inter-American Development Bank, August 2012.
[113] *A labor market that works: Connecting talent with opportunity in the digital age,* McKinsey Global Institute, June 2015.
[114] Based on an analysis of 70 emerging economies performed by the International Labour Organization; *Women and men in the informal economy: A statistical picture,* International Labour Organization, 2018.

Exhibit 9

Digital ID can facilitate digital talent matching and contracting platforms that can increase opportunities for inactive, part-time, and informal workers.



1. Working-age adults defined as individuals between the ages of 15 and 64.
2. Population not in the labor force.
3. Part-time employment data not available for China and India.

Source: International Labour Organization; International Monetary Fund; Nigerian National Bureau of Statistics; McKinsey Global Institute analysis

Such programs could also lead to substantive increases in labor force participation, as people currently excluded from the workforce take advantage of reduced hiring frictions to find a job that fits their background. According to our estimates, this increase translates to 900,000 full-time-equivalent workers joining the labor force in Nigeria, 6.7 million in India, and 1.5 million in the United States by 2030.

Digital ID can boost the productivity of land and agriculture through formalized landownership in emerging economies

Digital ID could enable digital land titles that would help farmers to sell or lease land and apply for new lines of credit that could increase investment and output on currently unregistered land. ID-enabled digital land titling could make formal ownership of assets accessible to a wider range of farmers in emerging countries who currently own land without evidence or registered legal claims.

With a digital land titling platform, similar to Estonia's successful e-Land Register, individuals could use their ID to verify land claims and make real-time updates to land transfers and purchases without the need for the potentially extensive travel, time loss, or fees currently necessary in many places. This could help stimulate more efficient land use from incentives to invest in longer-term management, increase supply and reduce prices by enabling a formal market, and allow landowners to use their digital title as collateral with banks. For example, Thailand, Indonesia, and Brazil experienced 30 to 80 percent increases in land values following the rollout of programs that introduced formal land titling. Such programs led to

increases in investment levels ranging from 40 to 105 percent in Brazil and Thailand, and increases in credit access from 200 to 350 percent in Brazil and Thailand.[115]

Furthermore, formalization of landownership would also allow farmers to access financial services and sources of credit. In Malawi, farmers whose income from crop sales was deposited directly into accounts spent 13 percent more on inputs for their future crops and achieved a 21 percent average increase in yields from the following year's harvest in comparison to farmers who received payment in cash.[116] Formalization of agricultural transactions enabled by digital ID could further contribute to increased investment in emerging economies.

As a result, we find digital ID could increase the productivity of the land and the agricultural output in emerging countries. We estimate that output could increase by up to 10 percent from more efficient land use, increased incentives to invest in longer-term management, and increased investment in future crops to increase yield that are enabled by digital ID. Countries such as Ethiopia, India, and Nigeria, where agriculture represents approximately 34 percent of national GDP (about $29 billion), 15 percent of national GDP (about $439 billion), and 21 percent of GDP (about $85 billion), respectively, stand to benefit the most.[117]

Digital ID can unlock time savings for individuals across many different uses

Digital ID can impact a wide range of interactions in our lives that result in time savings. Examples include shortening registration time for services by using a digital ID for transportation by bus or train, and using a digital ID as a reloadable cash wallet, a key service offered through Malaysia's MyKad ID.[118] Additionally, time savings can come from better account management. Individuals forget an average of 11 passwords per year, and 30 percent of calls to banks' call centers are requests for account access due to misplaced or forgotten passwords.[119] A digital ID would simplify the authentication process across all linked accounts and allow individuals to remember and recover countless passwords across a wide range of accounts.

Digitization of sensitive identity-related interactions also enables process streamlining and automation while reducing the need for travel, a particular benefit for people who live in rural areas. We estimate that individuals could save an average of 20 hours from e-government services per year, which would vary depending on the efficiency of government service provision in a given country. For example, in the United States alone, the Internal Revenue Service estimates that the average taxpayer spends 13 hours preparing and filing taxes, while Estonia's digital ID–enabled e-tax filing has reduced total tax filing time to three minutes.[120] However, time savings may not necessarily materialize into economic value if individuals spend their saved time for leisure instead of working additional hours.

Significant time savings are evident in current digital ID systems. In Estonia, for example, 67 percent of individuals regularly use their e-ID, and they save the equivalent of five days per year by using digital signatures for services such as submitting tax claims, voting online, paying parking tickets, and travel.[121] Over 99 percent of government services are online, allowing citizens round-the-clock access to the government (the only e-services not available at all times are for marriages, divorces, and real estate transactions).[122]

[115] Camilla Toulmin, "Securing land and property rights in sub-Saharan Africa: The role of local institutions," *Land Use Policy,* January 2009, Volume 26, Issue 1; Gershon Feder, *The intricacies of land markets: Why the World Bank succeeds in economic reform through land registration and tenure security,* Queensland Government, Natural Resources and Mines, 2002.

[116] Lasse Brune et al., *Facilitating savings for agriculture: Field experimental evidence from Malawi*, NBER working paper number 20946, February 2015.

[117] "Agriculture, Forestry, and Fishing value added (% of GDP)," World Bank.

[118] "MyKad: Is Malaysia ahead of the game?," PPC ID Card Solutions, October 8, 2015.

[119] *The future of identity in banking,* Accenture, 2013.

[120] Glenn Kessler, "Claims about the cost and time it takes to file taxes," *Washington Post*, April 15, 2013; "e-Tax," e-Estonia, e-estonia.com/solutions/business-and-finance/e-tax/.

[121] "e-Identity: ID card," e-Estonia, e-estonia.com/solutions/e-identity/id-card/.

[122] "e-Governance: Government cloud," e-Estonia, e-estonia.com/solutions/e-governance.

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. Although these uses of digital ID would primarily directly benefit institutions, individuals would also likely see some benefits from improved service delivery and lower prices due to competitive dynamics in affected private-sector industries and redirected government revenue arising from public-sector savings.

Institutions could benefit from significant time and cost savings

Digital ID can lead to significant reductions in direct costs and improved efficiency for both private and public institutions. These benefits could come from a variety of uses, including streamlined employee onboarding and hiring, efficient government and private service provisioning, simple digital land titling, seamless sharing of medical or financial information, and reduced administrative costs.

90%

The potential reduction in customer onboarding costs

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. For example, Indian payments application Paytm was able to use Aadhaar to register more than six million offline merchants, with the onboarding process taking less than three minutes on average.[123] 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 providing physical branches.[124]

Another channel for cost savings from digital ID is efficient land title issuance through digital land registries. In addition to the benefits to farmers, such programs could reduce the maintenance and administration costs of existing land registries. In many countries, issuing land titles is very slow because of the challenges of complex and overlapping rights. A study by the Instituto Libertad y Democracia found that 76 percent of rural properties and 65 percent of dwellings in the 12 Latin American countries it examined were in the informal sector and were not properly registered. The study further found that the process to buy, register, title, and obtain building permits for a plot of land took 101 days in El Salvador and up to 4,307 days (almost 12 years) in Guatemala.[125] Use of digital ID could eliminate paperwork and shorten processes associated with land management and could reduce inaccuracies and fraud in land registries.

Cost savings can also derive from seamless, secure sharing of information, for example in the case of electronic health records, which can be used as a tool for improving the overall quality and reducing the cost of healthcare. Cost savings can be captured through reduced duplicate testing and paperwork, better quality care from reduction of medical errors and adverse drug events, and better coordination of care.[126] A study of 550 hospitals in the United States found that costs associated with patients treated in hospitals with access to advanced electronic health records were on average 9.66 percent lower than for similar patients admitted to hospitals without such records.[127] We estimate that seamless sharing of medical information has the potential to deliver significant cost savings in countries around the world, including $130 billion in the United States, $6 billion in Brazil, and $8 billion in India.

Additionally, public and private institutions can leverage digital ID to slash administrative costs by reducing paper-based systems that require labor-intensive and manual administration for identification-related processes. Many governments currently maintain a range of identification systems that are managed by separate agencies for activities such as voting, issuing and checking passports, granting and renewing driver's or occupational licenses,

[123] *India's trillion-dollar digital opportunity*, Ministry of Electronics and Information Technology, Government of India, 2019.
[124] *Digital finance for all: Powering inclusive growth in emerging economies*, McKinsey Global Institute, September 2016.
[125] "Dead capital in 12 Latin American countries worth $1.2 billion, according to report," IBD News, June 12, 2006.
[126] Abby Swanson Kazley et al., "Association of electronic health records with cost savings in a national sample," *American Journal of Managed Care,* June 2014.
[127] Ibid.

registering vehicles, and filing taxes. Those systems could be integrated to reduce duplicative processes. For example, Nigeria has at least 13 government agencies operating separate identity systems. Many of these, such as the voter registry, driver's license registry, and SIM card registry, collect separate biometric data. These parallel identity systems create challenges for users, who must enroll multiple times and carry different ID cards to access services, and generate significant inefficiencies for the government.[128] In the case of Aadhaar in India, a paper-intensive, two-day process of verifying a new customer's identity became a 30-second fingerprint scan, increasing productivity and efficiency at private companies such as banks and cellphone providers.[129] The scale of these cost savings could be very large, and would depend on the existing processes for managing authentication and identification across industries and governments.

17m

The number of Americans who were victims of identity fraud in 2017

A wide range of savings from reduced fraud can benefit private and public institutions

Digital ID can help reduce fraud in a wide range of transactions across the public and private sectors, from decreased payroll fraud in worker interactions to reduced identity fraud in consumer and taxpayer and beneficiary interactions. We find that public and private institutions would receive the benefits of digital ID–enabled reduction of fraud differently.

Public providers of goods and services can reduce fraud by removing ghost recipients, deduplicating beneficiary rolls, and removing ineligible beneficiaries. Some studies indicate that the potential of digital ID to reduce fraud could be large. In Zambia, for example, World Bank studies have suggested that leakage in social transfer programs may be between 25 and 35 percent.[130] However, a recent cost-benefit analysis by the World Bank estimates that using the national ID to clean beneficiary lists and facilitate secure direct benefits transfers in four programs—the Public Service Pension Fund, the food security program, social cash transfers to households, and the Farmer Income Support Program—could save between $604 million and $2.04 billion. This calculation conservatively assumes that the identification program could reduce only a fraction of leakage, or around 5 percent.

Private providers could reduce fraud by preventing synthetic fraud, reducing ID theft, and addressing payroll fraud associated with ghost employees. Financial institutions, for example, can reduce theft and fraud through more robust onboarding and customer verification to assess customer risk. In the United States, approximately 16.7 million Americans were victims of identity fraud in 2017, an increase of 8 percent from 2016, and the cost of the data theft was nearly $17 billion.[131] Criminals also use fictitious IDs to secure credit in a practice known as synthetic identity fraud, which McKinsey estimates to be the fastest-growing type of financial crime in the United States.[132] In 2016, synthetic identity fraud was responsible for up to 20 percent of defaulted credit card debt, costing lenders worldwide an estimated $6 billion.[133]

Digital ID could increase the sales of goods and services by enhancing customer and user experience and loyalty

Institutions can use the capabilities of digital ID to improve customer experience and increase uptake of goods and services. Companies and other institutions can use digital onboarding to streamline uptake of their services. For example, the Indian telecom provider Jio onboarded some 160 million new customers in less than 18 months using e-KYC, enabled

[128] *The state of identification systems in Africa: A synthesis of country assessments,* World Bank, 2017.
[129] Vindu Goel, "India's top court limits sweep of biometric ID program," *New York Times,* September 25, 2018.
[130] This calculation conservatively assumes that digital ID would reduce only a fraction of this leakage. In Zambia, some studies have suggested that leakage in social transfer programs may be between 25 and 30 percent. See *Public Sector savings and revenue from identification systems: Opportunities and constraints*, World Bank, 2018; *Identity management cost-benefit analysis for Zambia, draft report,* World Bank, 2018.
[131] Sam Cook, "Identity theft stats & facts: 2017–2019," Comparitech, August 25, 2018; "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.
[132] Bryan Richardson and Derek Waldron, "Fighting back against synthetic identity fraud," McKinsey & Company, January 2019.
[133] Ibid.

by India's national digital ID system, Aadhaar.[134] Digital ID could also reduce opportunity costs by removing frictions within customer journeys. In the United Kingdom, for example, nearly 25 percent of financial applications are abandoned due to difficulties in the registration process.[135] For some microenterprises, formalized digital contracting records and contracting platforms could allow them to access international contracts and more fully participate in the global economy.

$118b

The amount online retailers in the United States lose a year from unwarranted transaction rejections

Institutions that already rely on some form of high-assurance identification, such as banks and digital gig-economy platforms like Uber, have the most to gain from digital onboarding and other digital ID–enabled improvements to authentication. Institutions that interact with individuals without the use of any identities, for example online merchants and informal employers, could also gain smaller benefits. Those institutions could integrate authentication into processes where it is currently not viable due to high costs and a lack of digital authentication options. This could be significant in industries such as online retail and payments, in which high-assurance authentication can be used to significantly improve the customer experience and prevent erroneous rejection of transactions. In the United States, for example, online retailers lose approximately $118 billion in revenue annually due to unwarranted transaction rejections, representing a huge opportunity for successful sales.[136] In Norway, online retailers address this problem by using the BankID system to verify payments or facilitate secure login and account management for customer pages.[137] The BankID has also been integrated into a wide variety of other services, including telecommunications, electricity provision, and real estate. For example, Norwegian landlords have been able to improve customer experience by using the digital ID for quick and simple signing of tenancy agreements, and Norwegian real estate agents use the BankID as a secure tool for bidding on properties.

In addition to increased uptake of goods, digital ID can enable improved applications of data analytics to increase productivity and unlock innovative solutions in business and government service delivery. Companies and governments could use transaction and authentication data to improve targeting of services and optimize their supply chains. For example, sharing of health data can be used to improve healthcare delivery and provide access to uncovered populations. Indian Prime Minister Narendra Modi announced the National Health Protection Scheme, which is intended to provide healthcare to 100 million poor families, in the government's 2018–19 budget. The goal of extending health insurance to poorer Indian citizens could be brought closer to reality by using the Aadhaar digital ID. Applications of digital ID to marketing could also significantly improve return on investment across marketing channels. McKinsey research has found that data-activated marketing based on a person's real-time behaviors could boost companies' total sales by 15 to 20 percent.[138]

Applications of digital ID to analytics, however, will require careful consideration of user privacy rights and mechanisms for ensuring that user consent is received and data are being used appropriately. The area of analytics applications has some of the greatest potential for dual use of digital ID to the detriment of individuals as consumers or citizens. Therefore, it will be critical for analytics-related applications to be created within a broader legal and governance structure that will ensure "good" use of digital ID by protecting user privacy, establishing user control over personal data, and preventing systemic misuse.

Institutions can benefit from greater employment and labor productivity

Digital ID can create significant benefits to institutions by fostering labor force productivity, increasing employment, and reducing payroll fraud through expanded and improved

[134] "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.

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

[136] Ibid.

[137] "366 things you can use BankID for," BankID, www.bankid.no/en/private/areas-of-use/.

[138] Julien Boudet, Brian Gregg, Jason Heller, and Caroline Tufft, "The heartbeat of modern marketing: Data activation and personalization," McKinsey & Company, March 2017, McKinsey.com.

talent matching, streamlined employee verification, and formalization that enables secure contracting with nontraditional workers, including contract and gig workers.

Just as digital talent matching can help individuals find new or better jobs, businesses and governments can leverage the platforms to more rapidly fill open positions and find the right employee for a given position, increasing workforce productivity. Beyond finding the right workers for open positions in the first place, digital talent matching can greatly reduce hiring costs. Previous MGI research has found that online talent matching programs can lower costs related to talent and human resources by up to 7 percent.[139]

The benefits of digital ID do not end when institutions find the right employee. It can help significantly cut the time necessary for employee verification and background checks and get hires working much faster. The need for streamlined employee verification 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.[140] A digital ID, especially one connected to a potential employee's background information and work history, can allow institutions to slash the costs and timeline of their employee onboarding process.

In addition to improving the hiring and employee verification process, digital ID can allow companies to contract with newly formalized nontraditional workers. This could include individuals currently working in the informal sector or microenterprises who are unable to secure contracts with established companies due to a lack of identification or an inability to demonstrate a contracting history. Such workers could leverage digital ID to keep a high-assurance record of their contract history, allowing institutions to quickly and accurately perform due diligence and authenticate their experience and identity.

Digital ID could increase formalization and expand the tax base, particularly in emerging economies

Greater revenue facilitated by digital ID could expand the tax base, helping promote formalization of the economy and more effective tax collection.[141] Emerging economies 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 India, the Ministry of Finance estimates that only 35 million people, or less than 3 percent of the total population, are in the taxpayer base.[142] In Tanzania, the National Identification Authority estimates that of 14 million people capable of paying taxes, only 1.5 million, or around 10 percent, do so.[143] Across Latin American countries, approximately half of potential tax revenues are lost to tax evasion.[144]

Some countries have been experimenting with identification systems to reduce tax fraud. In 2012, Pakistan began using the National Database and Registration Authority's capabilities to identify tax fraud through links between various databases. Out of a population of around 190 million, the country had fewer than 800,000 taxpayers. Under an agreement with the Federal Bank of Pakistan, NADRA was able to query a variety of databases to determine frequent travelers, individuals with multiple bank accounts, residents of wealthy neighborhoods, owners of expensive cars, high utility users, arms owners, and white-collar employees. This data mining allowed NADRA to identify some 2.4 million wealthy individuals who did not yet have national tax numbers, as well as 1.2 million who had tax numbers but were not filing. At the time, NADRA estimated that an additional 100 billion rupees (about $1 billion or 0.5 percent of GDP) in revenue could be generated within three months if a fraction of these 3.6 million were to begin paying some of the taxes they owed. Simply adding

[139] *A labor market that works: Connecting talent with opportunity in the digital age,* McKinsey Global Institute, June 2015.
[140] *Why is hiring taking longer? New insights from Glassdoor data*, Glassdoor, June 2015.
[141] *Digital revolutions in public finance*, IMF, November 2017.
[142] Ibid.
[143] Joseph J. Atick, *Digital identity: The essential guide,* ID4Africa Identity Forum, 2014.
[144] 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 2.4 million previously unidentified taxpayers into the system would have increased the potential tax base by 300 percent.[145]

In this chapter, we analyzed the economic benefits to individuals and institutions using a framework for understanding the interactions in which individuals could use digital ID. We find that digital ID could save individuals time and money, and improve the efficiency of labor markets and promote greater financial inclusion, which can lead to expanding credit and reducing the cost of credit. Institutions could also benefit from cost and time savings as well as fraud reduction, increased sales of goods and services, increased labor productivity, and expanding the tax base. In the next chapter, we quantify the benefits for individuals and institutions in each of our seven focus economies and then extrapolate our findings to calculate the global economic opportunity from digital ID.

[145] Tariq Malik, "Technology in the service of development: The NADRA story," Center for Global Development, November 7, 2014.

3 Quantifying the global opportunity

Our framework of how individuals and institutions use digital ID in multiple roles across the economy reveals many different benefits for both parties, suggesting that the overall economic impact could be significant. To understand how significant, we begin with a detailed microlevel analysis, examining nearly 100 ways of using digital ID in each of our seven focus countries: Brazil, China, Ethiopia, India, Nigeria, the United Kingdom, and the United States. We estimate the impact for each use in 2030 as a product of two factors: the addressable share of the economy and the potential for value creation. We then extrapolate our results from our focus countries to calculate the global opportunity from digital ID.

Across our focus countries, we find that digital ID could unlock economic value equivalent to between 3 and 13 percent of GDP in 2030 if the digital ID program enables multiple high-value use cases and attains high levels of usage. Extrapolating globally, in the case of emerging economies, we find that while the share of the economy that digital ID can address tends to be modest, scope for improvement can be sizable, leading to an average potential per-country benefit of roughly 6 percent of GDP in 2030, based on our modeling. 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. In this case, we find that an average per-country benefit of 3 percent could be possible, assuming high usage rates.

6%

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

This global economic estimate, however, captures only a fraction of the total potential benefits of digital ID. Digital ID can unlock significant noneconomic value by promoting political and social inclusion, facilitating the protection of rights, and increasing transparency. In some instances, the intrinsic value of social and cultural benefits enabled by use cases of digital ID may equal or even dwarf the economic benefits sized. In addition to the economic value we sized, we also anticipate that digital ID would enable new goods, services, and business models not yet conceived, but we do not attempt to capture them within our estimates. Our analysis should be viewed not as a forecast of what will happen, but rather as a sizing of the opportunity available if steps are taken to implement digital ID and develop the necessary digital infrastructure.

Potential varies by country based on the addressable share of the economy digital ID can affect and the opportunity for value creation

Both the magnitude and the nature of economic potential from digital ID differ significantly across our focus countries (Exhibit 10). While we undertake our estimation of the potential economic impact for each country in a bottom-up way for a set of relevant use cases, the differences in potential between countries can be understood by assessing where they stand on two factors: the addressable share of the economy that can be impacted by digital ID, and the potential for value creation in a country (see Box 3, “Our methodology”).

The first factor, the addressable share, represents the share of the economy consisting of interactions that digital ID could improve—in other words, the bottlenecks that digital ID can address. The factors we consider in determining a country’s addressable share are wage base, level of healthcare spending, expenditure on government benefits, and capital investment efficiency. The wage base is the total wages of a country as a proportion of its GDP and represents the amount of money going directly to workers through private and public payrolls. Countries where the wage base is higher would have greater exposure to

Exhibit 10

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

the benefits that digital ID can provide through mechanisms such as tax and payroll fraud reduction. The level of healthcare spending is also considered as a percentage of GDP and represents the share of the economy that can benefit from healthcare-related uses of digital ID, such as seamless sharing of medical information. A country's level of spending on government benefits for individuals, such as social welfare payments or subsidies, would determine whether digital ID–enabled efficiencies for disbursement would have a significant economic impact. The capital investment efficiency represents the ratio of a country's GDP to its fixed capital investment and determines the economic impact from new sources of capital resulting from increased financial inclusion that could be enabled by digital ID.

The second factor, the potential for value creation, represents the aggregate potential for greater formalization, inclusion, and digitization. It measures the degree to which digital ID can directly improve economic interactions. The factors that we consider in determining a country's potential for value creation include current levels of coverage of digital and conventional ID, offline population size, level of unmet financial needs, portion of the population that is unemployed or inactive, size of the informal economy and workforce, and fraud rate. Low current levels of ID coverage imply that populations without an ID today would be able to capture significant benefits even from a basic digital ID that enables uses such as financial inclusion and formalization. Similarly, a high share of offline population, or proportion of the population without internet access, suggests that considerable value could be generated from raising digital access and digitization of services enabled by digital ID.[146] The level of unmet financial needs represents the potential for financial inclusion of individuals who are currently unbanked, and the potential for new deposits and loans as these individuals enter the financial system. The unemployed and inactive population represents those who are not employed but actively looking for work and those who are not participating in the labor force, respectively. The informal economy and workforce represent the population not employed by a registered employer (as a composite of the value produced by such individuals as a share of GDP) and their representation as a share of the total workforce. High levels of informality would suggest that more value can be generated by economic formalization. Lastly, the fraud rate represents the level of corruption and fraud in an economy and indicates which countries have the most to gain from reductions in fraud occurring in disbursements, tax filings, and payroll.

The economic potential of digital ID also depends on whether the system is basic, which enables verification and authentication, or has advanced applications. A basic digital ID is similar to a digital version of a conventional physical ID. Advanced digital ID enables storing or linking additional information about individual ID owners and thus can facilitate advanced data sharing, with informed user consent, privacy protections, and control over personal data. 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. Estonia's e-Tax electronic tax filing system uses advanced data-sharing capabilities to prefill tax data directly from employer-provided information and has reduced the average time to file taxes online to three minutes for Estonian citizens.[147] In many cases, the lines between basic and advanced digital ID may blur because digital ecosystems with additional data can be built on top of basic digital IDs that enable initial authentication to access or interact with the systems.

[146] In areas where digital ID is used to authenticate individuals from internet-connected central locations, as is done for benefits disbursement in parts of India, individuals without personal internet connectivity could still capture value.
[147] "e-Tax," e-Estonia, e-estonia.com/solutions/business-and-finance/e-tax/.

Box 3

Our methodology

This research seeks to analyze and quantify the potential economic benefits of digital ID for an illustrative set of countries and to derive broader directional estimates for additional countries in both emerging and mature economies. A country-by-country approach is essential, because each country or situation is unique, with different drivers of potential value.

We begin with detailed microlevel analysis, looking at nearly 100 ways of using digital ID in each of our seven focus countries. We estimate the microlevel impact for each use case in 2030 as a product of two factors: the addressable share of the economy that would be impacted and the potential for value creation. Within the addressable share of the economy, we estimate the incremental share of interactions that may adopt and use digital ID. For example, payroll fraud prevention is estimated based on the product of total wages, the percent of workers who may receive payroll tied to digital ID, and the potential payroll fraud prevented per worker. We do not perform a comprehensive cost-benefit analysis of digital ID but focus on sizing incremental value possible from levers such as time and cost savings and greater supply of labor and capital resulting from digital ID–based applications.

To understand how the use of digital ID could affect the overall economies of our seven focus countries, we use McKinsey's proprietary general equilibrium macroeconomic model. We then extrapolate from the focus countries based on metrics for the share of the economy addressable by digital ID and the potential for value creation in a global set of countries. Our estimates presume that the components of good ID are in place, including that it is established with individual consent, protects user privacy, and ensures control over personal data. Our approach is particularly sensitive to three sets of assumptions:

- **Usage and adoption by 2030**. We assume high levels of digital ID adoption and usage by 2030, based on current levels in the most successful existing digital ID programs. We consider both basic and advanced ID programs as well as country income levels in setting our assumptions. In this sense, our estimates are of potential value, not predictions or forecasts of the value that could be created by digital ID by 2030.
- **Accompanying general infrastructure.** We assume that countries develop the digital infrastructure and ecosystems required to enable digital ID and gain the value it helps unlock. We believe that digital ID is a foundational set of technologies, pivotal to unlocking the value we quantify but not sufficient—each area of use will require digital infrastructure, applications, and interfaces built by institutions that interact with digital ID users. These include sufficient levels of telecom and electrical coverage, e-government services, digital financial services, digital talent matching and contracting platforms, digital health records, and digital asset registries. Our estimates of potential value from digital ID include the full value that comes from the use cases it could enable. We do not attempt to isolate the incremental value from digital ID alone, since we believe that in most cases this is not possible. For example, we estimate the benefit from expanded credit to borrowers that digital ID can enable, on the understanding that applications for digitally enabled credit scoring and approval would also be a part of that value.
- **Time savings for individuals.** To quantify the economic value of individuals' time, we model hours saved as increased labor hours. We note that while time may be valued at or above potential earnings in labor markets, not all time saved is likely to materialize as additional labor hours. As a result, not all of these potential sources of economic value may translate into GDP, but we use GDP as a comparable base to give a sense of the order of magnitude of the opportunity.

Our analysis does not account for several potential additional sources of value, including digital ID for businesses, the potential for individual institutions to gain market share, increased cross-border flows enabled by interoperable digital ID, innovation and the creation of new markets, products, and services, and future uses not yet developed.

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

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 (Exhibit 11). The estimated ranges are 8 to 13 percent for Brazil; 4 to 7 percent for Ethiopia, India, and Nigeria; and 0.5 to 4 percent for China, the United Kingdom, and the United States, with the low end of each range representing the potential value from basic digital ID and the high end representing the potential value from digital ID with advanced characteristics.

Brazil has the greatest potential for value creation from digital ID in our sample, ranging from 8 percent of GDP in 2030 for basic ID to 13 percent for advanced ID

Brazil stands out with the greatest potential for value creation out of our seven-country focus group, with benefits potentially accruing about equally to individuals and institutions. Furthermore, the three highest-value use cases in Brazil center on the consumer, worker, and taxpayer and beneficiary.

For Brazil, consumer interactions are responsible for 40 percent of the economic potential sized, and almost three-fourths of these benefits could come from financial inclusion. Approximately 49 million Brazilians, or 30 percent of the adult population, are excluded from access to credit and financial services, and 57 percent of unbanked individuals in Brazil cite account fees and other expenses as the primary barrier to opening a bank account.[148] Digital ID–enabled digital customer registration could help make financial services more affordable and widely accessible by allowing banks to meet regulatory Know Your Customer and anti–money laundering requirements. We estimate that an advanced digital ID could reduce KYC costs for Brazilian banks by up to $14 per new account or 95 percent, and this, along with remote registration capability, could make banking a reality for the 32 percent of unbanked Brazilians who cite distance from branches as the main barrier to access. Increased lending to individuals and businesses resulting from an expanded deposit base could generate up to $190 billion in increased investment.[149]

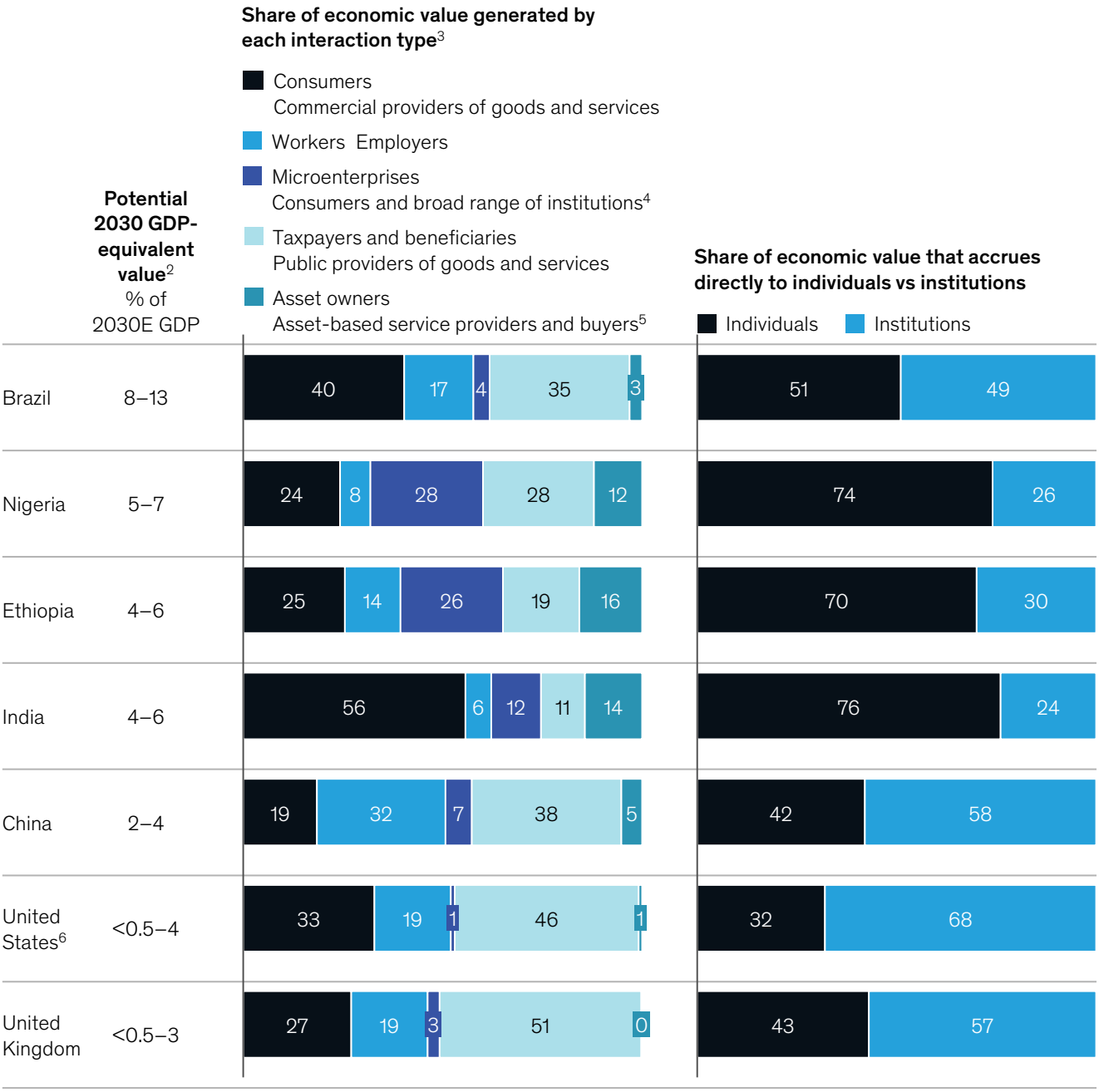
Interactions by taxpayers and beneficiaries account for an additional 35 percent of potential economic value, largely a result of taxation of newly formalized income and reduction in tax fraud and time savings from e-government. A recent assessment by the Union of Prosecutors of the National Treasury estimated that Brazil's tax gap represented 23.6 percent of aggregate tax revenue in 2014, or 8.6 percent of GDP.[150] The informal sector constitutes 35 percent of total GDP, and the associated loss of tax revenue is exacerbated by evasion, error, and carelessness in tax filing in the formal sector, estimated to impact about 40 percent of Brazilian tax revenues.[151] We estimate that integration of tax filing with digital ID has the potential to raise revenues and reduce fraud, enabling Brazil to generate up to $122 billion in economic value in 2030. Brazil could leverage digital ID to enable the creation of e-government services that could save Brazilians up to 2.8 billion hours annually in time they would have spent on activities such as voting, renewing licenses, and filing taxes. The potential for e-government in Brazil is demonstrated by the success of the e-government program in the city of Limeira, where a digital transformation to the government hotline greatly decreased resolution times for citizen complaints and helped citizens regain trust in local government.[152]

[148] Global Findex Database.
[149] All figures in the country analysis converted to 2018 real dollars.
[150] Flavio Rubinstein and Gustavo G. Vettori, "Closing the Brazilian tax gap: Public shaming, transparency and mandatory disclosure as means of dealing with tax delinquencies, tax evasion and tax planning," *Derivatives & Financial Instruments,* 2016, Volume 18, Number 1.
[151] Leandro Medina and Friedrich Schneider, *Shadow economies around the world: What did we learn over the last 20 years?*, IMF working paper number 18/17, January 2018; Kenneth Rapoza, "Tax evasion a way of life in Brazil," *Washington Times*, July 13, 2004.
[152] Matheus Pantaroto Conejo and Gustavo Hermínio Salati Marcondes de Moraes, *Electronic government in Brazil: The case of the restructuring of Channel 156 in the city of Limeira*, 2016.

Exhibit 11

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

38%

of the adult population are excluded from access to credit and financial services

In addition to increasing tax revenue, interactions involving taxpayers and beneficiaries also yield value through reduced leakage and fraud from ghost recipients of government benefits. Brazil's spending on benefits in 2017 was 38 percent of GDP; a large addressable share of the economy could be impacted by digital ID–enabled leakage reduction. Government benefits have been a focus in Brazil since the introduction in 2003 of the Programa Bolsa Familia, which among other goals aims to "improve the efficiency and coherence of the social safety net" through measures including conditional cash transfers.[153] The program has been very successful in preventing extreme hunger and poverty in the country and has contributed to a sharp reduction in income inequality. The introduction of digital ID could help further streamline benefit disbursements in Brazil. We estimate that removal of ghost beneficiaries and reduction of leakage in the public benefits system could save Brazilian taxpayers up to $90 billion, providing value to both taxpayers and legitimate beneficiaries who could access funds that are currently diverted away from them.

We find that digital ID could also generate value through worker interactions, contributing 17 percent of total value, by enabling digital talent matching and contracting platforms and reducing private-sector payroll fraud; microenterprise contributes 4 percent.

Digital talent matching platforms for workers and digital contracting platforms for microenterprises could generate value equal to 1.3 percent of GDP through reduced frictional unemployment, formalization of some informal workers, entry of inactive workers into the labor force, and creation of digital contracting records for microenterprises. A 2015 LinkedIn survey found that Brazilian respondents used LinkedIn or similar platforms to reduce the time spent looking for a new job by 52 percent, and 56 percent of respondents said that talent matching platforms had helped to broaden or improve their job options—the highest percentages of the countries surveyed.[154] Digital ID can enable much more effective talent matching and contracting platforms, and Brazilians are well positioned to capture the benefits.

Brazil ranks 96th in the world on Transparency International's Corruption Perceptions Index, and it experiences high rates of fraud throughout the economy. As a result, Brazil has high potential for improvement through measures that affect fraud levels in the economy. We estimate that use of digital ID for high-authentication payroll and removal of ghost employees could save private-sector companies up to $69 billion in payroll fraud.

Nigeria could capture economic value equivalent to 5 to 7 percent of GDP in 2030 from greater formalization, fraud reduction, increased tax revenue, and financial inclusion

Three-quarters of the benefits of digital ID could accrue to individuals in Nigeria, and one-quarter to institutions due mainly to the benefits of greater formalization.

In Nigeria, 28 percent of the additional value created by digital ID could be generated by microenterprise interactions, largely from formalization of labor for self-employed individuals. The International Labour Organization estimates that 93 percent of Nigeria's workforce is informal and 81 percent is self-employed.[155] The largely informal and self-employed workforce skews the overall benefits of digital ID toward individuals, who could receive 74 percent of the total overall value. The formalization of labor for microenterprises from increased ID coverage could contribute an additional 1 percent to Nigeria's GDP by 2030, as self-employed individuals could use formal identification to enable more significant investment in their microenterprises and gain access to a broader range of services in the formal economy. In addition, self-employed individuals in Nigeria could use digital ID to formalize contract records and use digital contracting platforms to access opportunities while working with the government or large corporations in major sectors such as oil and mining. Self-employed individuals could document their microenterprise transaction histories to satisfy formal authentication requirements and use their proven work histories to unlock opportunities even without formal credentials. We estimate that the use of digital contracting and talent matching

[153] Bolsa Familia in Brazil, Centre for Public Impact.
[154] *Preparing Brazil for the future of work: Jobs, technology, and skills*, McKinsey Global Institute, March 2018.
[155] Leandro Medina and Friedrich Schneider, *Shadow economies around the world: What did we learn over the last 20 years?*, IMF working paper number 18/17, January 2018.

platforms by microenterprises in Nigeria could add approximately 0.5 percent to 2030 GDP in increased productivity.

81%

of the workforce in Nigeria is self-employed

Taxpayer and beneficiary interactions also generate 28 percent of the total value created by digital ID in Nigeria, driven primarily by reduced payroll fraud and benefits leakage and increased tax revenue plus time savings from e-government services. Although a relatively low addressable share of the economy is impacted by reductions in benefits leakage, with 12 percent of GDP spent on benefits in 2017, high fraud rates create significant potential for improvement. Ghost workers represent a large opportunity in Nigeria, where the government has found tens of thousands of fraudulent or nonexistent employees on payrolls throughout the federal civil service. The Nigerian Ministry of Finance discovered almost 24,000 ghost workers on the public payroll in 2016, two years after 60,000 ghost workers were discovered. A 2009 government review revealed that ghost workers made up approximately half of the 20,000-person workforce in the Customs Service.[156] We estimate that digital ID could create $350 million in savings from preventing such government payroll fraud, and a further $3 billion could accrue from the removal of ghost beneficiaries on public welfare programs. In addition, the shadow economy is estimated to be more than half of the total economy in Nigeria, at an average of 52 percent of GDP from 2004 to 2015 according to IMF calculations, and formalizing income generated in the shadow economy could provide significant additional revenue opportunities.[157] We estimate that Nigeria could use digital ID to expand the tax base to include informal income and reduce fraud and errors in tax filing to generate more than $13 billion in additional tax revenue. Nigerians could save 1.8 billion hours annually from efficient services that reduce the need for travel to and from government offices and filing of physical paperwork.

Consumer interactions are another major potential contributor to value in Nigeria; benefits could be realized primarily through increased financial inclusion. The country's unmet financial needs are significant: 60 percent of the adult population, or about 64.5 million individuals, does not have a bank account and therefore may be cut off from access to credit or the ability to deposit income.[158] The World Bank found that 18 percent of the unbanked population in Nigeria cited a lack of identification documentation as the primary reason for not opening an account, with an additional 13 percent citing cost and 19 percent citing distance. A digital ID that provides universal identification, reduces KYC costs, and enables remote registration could help significantly close this gap and vastly expand financial access in Nigeria. We estimate that increased lending to individuals and businesses resulting from an expanded deposit base could generate up to $21 billion in additional investment by 2030.

70%

of the benefits of digital ID in Ethiopia could accrue to individuals

Ethiopia could capture economic value equivalent to 4 to 6 percent of GDP in 2030 from greater use of contracting platforms, more financial inclusion, and reduced fraud

As in Nigeria, the economy in Ethiopia is heavily informal, and as a result, the majority of benefits from digital ID would flow through to individuals. We estimate 70 percent of the benefits could accrue to individuals in Ethiopia, and 30 percent to institutions. The International Labour Organization estimates that 89 percent of the workforce in Ethiopia is self-employed, and the informal sector is approximately the size of one-quarter of the country's GDP.[159]

Microenterprise interactions are the main driver of value in Ethiopia, generating 26 percent of the economic potential from digital ID. More than 80 percent of the benefits generated by microenterprise interactions are driven from digital contracting platforms, and the rest from formalizing labor. Digital contracting platforms in Ethiopia could provide benefits by increasing utilization of excess microenterprise capacity by accelerating matching between microenterprises already in the formal sector and private- and public-sector institutions requiring contractors. We estimate that this increased efficiency would generate an

[156] Leyira Christian Micah and Temple Moses, "IPPIS and the ghost workers' syndrome in Nigeria's public sector," *Scholars Journal of Economics, Business and Management,* August 2018, Volume 5, Issue 8.
[157] Leandro Medina and Friedrich Schneider, *Shadow economies around the world: What did we learn over the last 20 years?,* IMF working paper number 18/17, January 2018.
[158] The 2017 Global Findex survey, World Bank.
[159] Leandro Medina and Friedrich Schneider, *Shadow economies around the world: What did we learn over the last 20 years?,* IMF working paper number 18/17, January 2018.

employment impact equivalent to approximately 700,000 additional full-time employees by 2030. In addition, digital contracting platforms could bring individuals currently not in the labor force into the labor market, generating an employment impact equivalent to 533,000 additional full-time employees by 2030. Overall, digital contracting platforms could create productivity gains equivalent to a 1.5 percent increase in GDP by 2030. The formalization of contracting histories could allow microenterprises in Ethiopia to secure contracts with public- and private-sector institutions. We estimate that this would generate an employment impact equivalent to approximately 176,000 full-time employees by 2030.

41m

Potential individuals for financial inclusion in Ethiopia

Consumer interactions could generate a quarter of the value in Ethiopia, primarily through increased capital resulting from financial inclusion. Ethiopia has significant potential for financial inclusion, with 65 percent of the population, or approximately 41 million individuals, excluded from the financial system. A digital ID that allows banks to offer remote registration capabilities could have a particularly large impact, as 80 percent of the population lives on rural smallholdings that can be ten kilometers or more from the nearest bank branch or ATM.[160] However, Ethiopia has low capital investment efficiency, which means that additional investment has a relatively smaller impact on economic output than in the other countries we surveyed. Overall, bringing unbanked individuals into the financial system could generate up to $2.5 billion in additional physical capital investment from the resulting increase in the deposit base, an increase of up to 1 percent in GDP-equivalent value.

Taxpayer and beneficiary interactions are responsible for 19 percent of the value from digital ID, primarily through decreases in benefits leakage and the expansion of the tax base as well as time savings from e-government services. The addressable share of the economy that can be impacted by uses improving benefits disbursement is limited by Ethiopia's government spending on benefits, equivalent to 18 percent of GDP in 2017. This is low relative to the other focus countries we examined. Removal of ghost beneficiaries could save the Ethiopian government up to $2.2 billion, approximately 6.6 percent of projected 2030 expenditures. Creating a high-assurance ID that is integrated with employment and financial records could also allow the Ethiopian government to expand its tax base by accessing the hidden economy, resulting in up to $1.9 billion in additional revenue, equivalent to 11 percent of the projected 2030 tax base. Ethiopians could save up to 1.1 billion hours annually from more efficient e-government services that cut out paperwork and travel time when dealing with the government.

Asset owner interactions are responsible for 16 percent of the value from digital ID, and benefits are primarily generated through increased land productivity resulting from formalized landownership and cost savings from land registry maintenance. As Ethiopian farmers receive digital IDs, they would be able to use them to acquire legal titles to their land. Formalized landownership would help encourage long-term investment in their land and would give farmers access to a broader range of services, generating up to $1 billion in increased productivity. We estimate that this gain could contribute to an approximately 0.9 percent increase in GDP by 2030. In addition to increased productivity, digitization of land registries enabled by digital ID could remove administrative and other maintenance costs for existing physical local land registries. We estimate that this could create more than $200 million in additional savings for the Ethiopian economy.

India has already captured benefits from Aadhaar but has significant potential to create additional value, mostly from greater financial inclusion

We calculate that India could capture additional economic potential equivalent to 4 to 6 percent of GDP in 2030 from high adoption of digital ID, with about 76 percent of that potential value accruing to individuals and 24 percent to institutions. While this is in line with Ethiopia and Nigeria, the fact that about 1.2 billion people in India are already enrolled in Aadhaar puts the country on a different trajectory for realizing potential benefits. The extent of use case implementation and the potential value realized will, however, depend on the

[160] *Digital finance for all: Powering inclusive growth in emerging economies,* McKinsey Global Institute, September 2016.

76%

of the benefits of digital ID in India could accrue to individuals

policy environment and on how legal requirements and operating regulations on digital ID applications evolve.[161]

We find that India would benefit most from consumer interactions, generating 56 percent of potential value created, largely driven by greater financial inclusion. Despite the increase in account opening enabled by Aadhaar, nearly 40 percent of bank account owners had not made a deposit or withdrawal in the 12 months before March 2018.[162] It will take time for new account holders to begin adding deposits to their bank accounts and participate fully in the financial system, which is a major reason that the potential for value creation in satisfying unmet financial needs is significant. Digital ID can also encourage increased usage of financial services and access to credit for new account holders in India by enabling secure mobile banking and micro-ATMs in rural or less developed communities where branch access is limited. Furthermore, 20 percent of Indian adults, or approximately 195 million individuals, are still unbanked. Due to India's moderately high capital investment efficiency, we estimate that increasing financial inclusion could generate an additional $617 billion in new physical capital investment from an expanded deposit base, translating into a GDP increase of up to 3.5 percent by 2030.

Beyond increasing capital in the economy, digital ID could create additional value through consumer interactions by allowing retailers to reduce supply chain and operational costs through targeted service provisioning and dynamic labor and supplier management. Previous MGI research found that improved use of analytics could create a 0.5 percent annual increase in retail industry productivity through mechanisms including improved marketing operations and dynamic labor management, including accurate predictions of staffing needs based on consumer patterns.[163] Digital ID could be an important facilitator of those and further productivity improvements. It could allow retailers to accurately identify consumers, employees, and suppliers and perform advanced analytics on high-quality associated data to streamline and improve processes. Some of the benefits from these savings and productivity improvements would likely be distributed to individuals through price reductions and improved services due to industry competition. Such applications of digital ID to improved analytics are also major contributors to value from consumer interactions in the United Kingdom, the United States, and China. However, as we have noted previously, applications of digital ID to analytics will require careful consideration of user privacy rights and mechanisms for ensuring that users have given their consent and have appropriate control over how their data are being used.

Asset owner interactions generate 14 percent of the potential value created from digital ID in India. In particular, farmers in India could use a digital ID to receive a formal land title and enable long-term investment in their land. The resulting increased agricultural productivity could generate up to $55 billion in value and contribute approximately 0.7 percent to GDP.

Approximately 12 percent of the potential value created in India from digital ID could be generated through microenterprise transactions, and 6 percent through worker interactions. India has a high potential for value creation from use cases impacting the informal economy and workforce, with 78 percent of the nonagricultural workforce employed in the informal sector and the informal sector responsible for approximately 18 percent of GDP.[164] The use of digital contracting for microenterprises could generate productivity increases equivalent to approximately 0.7 percent of GDP. This would be driven by newly formalized microenterprises gaining access to the formal contracting market, as well as more efficient matching of microenterprises already in the market and increased labor force participation of some previously inactive workers entering the labor force. Overall, digital contracting platforms could create an increased employment impact equal to 6.3 million additional full-time-

[161] 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.

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

[163] *Big data: The next frontier for innovation, competition, and productivity*, McKinsey Global Institute, May 2011.

[164] *Women and men in the informal economy: A statistical picture*, International Labour Organization, 2018; Leandro Medina and Friedrich Schneider, *Shadow economies around the world: What did we learn over the last 20 years?*, IMF working paper number 18/17, January 2018.

equivalent workers by 2030. Women could benefit the most from employment opportunities presented by digital contracting platforms; a 2014 study showed that only 22.5 percent of Indian woman participated in the formal labor force.[165] The use of digital talent matching for workers in the formal sector could also create benefits from worker interactions both through labor force participation and reduction of frictional unemployment in the formal sector. We estimate that reduced frictional and long-term unemployment and increased labor force participation resulting from digital talent matching platforms in the formal sector could create a net employment impact equivalent to adding more than 1.2 million FTEs.

We estimate that taxpayer and beneficiary interactions could generate 11 percent of the remaining potential value, primarily through reductions in benefits leakage and increased tax revenue from reduced tax evasion and errors as well as decreased tax fraud. Aadhaar has been used to improve the efficiency of benefits disbursements and to reduce leakage for government subsidies to individuals for resources such as natural gas.[166] Yet a significant addressable share of the economy could be impacted by further improvements in disbursement efficiency due to the size of total government benefits—about 28 percent of GDP in 2017. We estimate that further integration of digital ID into the benefits system in India could generate up to $26 billion in value from removing remaining ghost beneficiaries and leakage. India could also generate significant value if digital ID could be integrated comprehensively into the tax filing process. We estimate that digital ID could be used to increase the tax base and reduce fraud to generate an additional $23.5 billion of revenue.

The economic potential of digital ID in China is more in line with mature economies, with total potential value equivalent to 2 to 4 percent of GDP in 2030

The economic value of digital ID in China is driven primarily by transactions generated by taxpayers and beneficiaries and those involving workers, with 42 percent of total potential value accruing to individuals and 58 percent to institutions. China's relatively high existing level of ID coverage—98 percent of the population, according to World Bank analysis—means that it has a low potential for value creation from uses that boost ID coverage alone. Unlike India, which also has high levels of ID coverage through Aadhaar, China has a higher share of the population online, lower unemployment, and a larger formal workforce, all of which reduces the economic value potential of digital ID relative to that of India. The potential gains generated by microenterprises and asset owners in China are also lower relative to other emerging economies like Nigeria and Ethiopia. Overall, the benefits to institutions would be largely from more efficient hiring and reduced fraud and tax leakage.

Taxpayer and beneficiary interactions could generate 38 percent of the total value in China and would be driven primarily by increased tax revenue and reduced fraud, healthcare data sharing, and time savings. We estimate that increases to the tax base and reduced tax fraud from digital ID–enabled efficiencies could contribute almost $350 billion to the Chinese treasury by 2030, or approximately 6 percent of projected government revenues. China has a high potential for value creation from fraud-related uses, in line with other emerging countries, and ranks 77th in Transparency International's Corruption Perceptions Index.[167] In addition, a high addressable share of the economy can be affected by uses that create efficiencies in benefits disbursements. Therefore, digital ID could enable large savings in benefits expenditure by facilitating the removal of ghost and illegitimate recipients from government disbursements. We estimate that China could save up to $805 billion by 2030 through reduced fraud in benefit transfers.

China could also use digital ID to enable sharing healthcare data to unlock up to $22 billion in savings by 2020. Effective digital ID could allow the healthcare system to expand on recent efforts to support data sharing and analysis in a way that protects user privacy and reduces the cost of healthcare.[168] Individuals in China could also save almost 19 billion hours a year through broader e-government services. Secure and high-assurance digital ID could allow

[165] Sher Verick, *Women's labour force participation in India: Why is it so low?,* International Labour Organization, 2014.
[166] Neeraj Mittal, Anit Mukherjee, and Alan Gelb, *Fuel Subsidy Reform in Developing Countries: Direct Benefit Transfer of LPG Cooking Gas Subsidy in India,* Center for Global Development, 2017.
[167] Corruption Perceptions Index 2017, Transparency International, February 2018.
[168] Liu Zhihua, "Health sector gets 'big data' boost," *China Daily,* August 14, 2018.

both the local and national governments to expand their e-government offerings and provide more efficient and responsive services.[169]

Worker interactions could generate 32 percent of the total value in China, primarily through increased labor productivity from digital talent matching and reduced payroll fraud in both government and the private sector. We estimate that improved labor productivity spurred by digital talent matching could create up to $26 billion in value from increased productivity as workers use their digital ID on digital talent matching platforms to shift from informal to formal employment and find more productive employment within the labor market. Recent college graduates could particularly benefit from talent matching programs that allow them to find jobs best suited to their credentials, as a glut of graduates has caused higher unemployment and competition for employment even in a relatively tight economy.[170] In addition to talent matching, digital ID could help reduce public- and private-sector payroll fraud, generating up to $445 billion in savings for both Chinese companies and government employers.

Consumer interactions generate 19 percent of the value in China, primarily driven by productivity improvements enabled by analysis on high-quality data across sectors. We estimate that analytics could add up to about 0.8 percent to China's GDP by 2030, as digital ID could allow Chinese companies to build on existing initiatives to integrate high-quality data analytics into fields such as medical research and marketing.

High adoption of advanced digital ID in the United States could result in total economic value equivalent to 4 percent of GDP in 2030

In the United States, we estimate that the economic potential of digital ID is equivalent to less than 0.5 to 4 percent of GDP, with 32 percent of that value accruing to individuals and 68 percent to institutions. The benefits profile for digital ID in the United States is similar to that of the United Kingdom, except that it could capture an additional 1 percent of value relative to GDP, an opportunity driven in part by higher levels of healthcare expenditure. Due to the prevalence of private healthcare insurance and delivery in the United States, we allocate the potential value generated through digital ID applications in healthcare to both the taxpayer and beneficiary and the consumer interaction channels.[171]

68%

The potential benefits of digital ID that could accrue to institutions in the United States

According to the World Bank, 2015 healthcare expenditure in the United States was 16.8 percent of GDP, compared with the developed economy average of 12.5 percent, and greater than all other countries except the Marshall Islands and Sierra Leone.[172] As a result, the United States is the focus country with the largest addressable share of the economy that could be impacted by uses that reduce healthcare costs. Digital ID could create significant efficiencies in healthcare expenditures through facilitated sharing of records, which can streamline hospital operations and reduce unnecessary pharmaceutical expenses. We estimate that digital ID could generate up to $130 billion in healthcare savings in the United States by 2030 and contribute up to 0.9 percent to GDP by 2030.

The savings from healthcare data sharing would be largely captured by healthcare providers and the government, which is why institutions account for 68 percent of the economic value in the United States, or approximately 11 percent more than in the United Kingdom. Some of these savings are likely to be distributed to individuals through price reductions fostered by competitive dynamics in the private sector and insurance market, as well as by increases in available government funds from decreased healthcare expenditure.

In addition to healthcare savings, taxpayers and beneficiaries have the potential to generate more than $360 billion in additional tax revenue through reductions in tax evasion, errors

[169] Yao Yang, "Towards a new digital era: Observing local e-government services adoption in a Chinese municipality," *Future Internet*, August 2017, Volume 9, Issue 3.

[170] *Asia Blog*, "How the Asian financial crisis led to China's massive graduate unemployment," blog entry by Eric Fish, June 8, 2017, asiasociety.org/blog/asia/how-asian-financial-crisis-led-china%E2%80%99s-massive-graduate-unemployment.

[171] 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.

[172] Healthcare expenditure in Sierra Leone climbed in 2015 from an average of 9.7% of GDP from 2000 to 2013 due to continued response to an outbreak of the Ebola virus in 2014.

during tax filing, and tax fraud. This increased revenue represents 7.2 percent of projected 2030 tax revenue and could contribute 0.7 percent to 2030 GDP. At the same time, benefits would come from accessing e-government services. Individuals in the United States stand to save 4.4 billion hours from the provision of e-government services at the federal, state, and local levels.

33%

The total potential of digital ID generated from consumer interactions in the United States

Consumer interactions generate 33 percent of the total value potential in the United States, and in addition to the previously discussed healthcare-related benefits, the value is driven primarily by reduced identity-related fraud, retail sector operational savings, and improved productivity across sectors from analytics on high-quality data. We estimate that digital ID could create $27 billion in reduced identity-related fraud, and project that retailers could save $6 billion from more efficient operations and supply chain management enabled by digital ID. The use of digital ID for analytics on high-quality data could create economic value equivalent to 0.91 percent of GDP by 2030, as companies across a variety of sectors could improve the productivity of services including insurance risk scoring and marketing. However, applications of digital ID to analytics will require careful consideration of user privacy rights and mechanisms for ensuring that users who have given their consent have appropriate control over how their data are being used.

High adoption of digital ID in the United Kingdom could generate total economic value equivalent of less than 0.5 to 3 percent of GDP in 2030, nearly all from advanced ID

In the United Kingdom, the gains from digital ID are mostly derived from interactions involving taxpayers and beneficiaries—which generate more than 50 percent of the potential value—and secondarily from interactions involving consumers and workers. Overall, individuals could receive 43 percent of the benefit from digital ID in the United Kingdom and institutions 57 percent through reduced costs and fraud as well as additional tax revenue.

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. A high addressable share of the UK economy can be impacted by uses that enable more efficient healthcare spending, as healthcare expenditure is 9.8 percent of GDP.[173] We estimate that the use of digital ID for seamless sharing of medical records in the United Kingdom could create savings of up to $9.3 billion, or approximately 9 percent of projected 2030 expenditures.

An area where digitization of services could provide significant benefits to the United Kingdom is e-government services and efficient digital tax filing, which could create significant time savings and reduce errors and evasion associated with tax filing. The Gov. UK Verify program, launched in 2016, enables authentication with a set of public-sector departments through online login, but the program has seen slower than expected adoption and a relatively small set of available use cases. We estimate that a comprehensive suite of e-government services across government agencies could save individuals up to 450 million hours annually. Connection of a digital ID with an individual's employment records would allow for tax filing services to auto-populate required financial information, both reducing the potential for tax evasion and minimizing errors throughout the filing process. We estimate that the United Kingdom could generate $35 billion in additional tax revenue by 2030 through expansion of the tax base and reductions in errors and evasion in tax filing.

Consumer interactions in the United Kingdom could generate 27 percent of the total potential economic value. These gains would be driven by reductions in identity theft fraud, reduced retail supply chain and operational costs, and increased productivity for service providers from analytics on high-quality data. Although the United Kingdom has lower fraud rates than emerging economies, identity theft is still a major and growing issue. The UK antifraud organization Cifas reported that there were almost 175,000 cases of identity fraud reported in 2017, a 125 percent increase compared with a decade prior.[174] We estimate that digital ID could prevent up to 40 percent of consumer identity-related fraud, by making it harder to impersonate individuals in financial transactions and introducing high-assurance

[173] World Development Indicators, World Bank 2018.
[174] "Fraudulent conduct decreases overall—but worrying rises in some areas," *The Fraudscape*, 2018.

authentication into online marketplaces and digital ecosystems. In the United Kingdom, digital ID could generate up to $5.7 billion in ID-related fraud savings through 2030.

Digital ID could create additional value through consumer interactions by allowing retailers to reduce supply chain and operational costs through targeted service provisioning and dynamic labor and supplier management, as mentioned in the discussion of India, China, and the United States. Some of the benefits from these savings and productivity improvements would likely be distributed to individuals through price reductions and improved services due to industry competition. However, applications of digital ID to analytics will require careful consideration of user privacy rights and mechanisms for ensuring that users have given their consent and have appropriate control over how their data are being used.

Worker interactions could generate 19 percent of the total value from digital ID, primarily through reduced payroll fraud. Because of its large wage base—53 percent of GDP—the UK economy has a large addressable share that can be impacted by uses reducing payroll fraud, but low potential for value creation stemming from relatively low fraud levels limits the possible impact. The Crowe Clark Whitehill Annual Fraud Indicator 2017 report found that 1.7 percent of all payroll expenditures in the United Kingdom were fraudulent, costing employers £12.7 billion.[175] We estimate that integration of digital ID into payroll could create $11 billion of savings by 2030.

65%

of the total benefits of digital ID could accrue to individuals in emerging economies

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

to gain an understanding of the economic impact of digital ID globally, we examine a broader set of 23 countries using the same factors we outlined for our focus countries—the addressable share of the economy and the potential for improvement in ID coverage, digitization, financial inclusion, employment, formalization, and fraud reduction (Exhibit 12). 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.

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 these countries are able to generate high levels of adoption.

In emerging economies, much of the value could be captured even through basic digital ID with essential functionalities. Among other uses, basic digital ID can enable formalization of labor for workers and microenterprises and can be a critical tool in letting rural farmers formalize and claim their property rights. A basic digital ID can also be the first step toward a more advanced system, as has been seen in India. Although Aadhaar is a basic ID system, it has been used to seed other databases, such as beneficiary bank accounts, that in turn may have data-sharing capabilities.

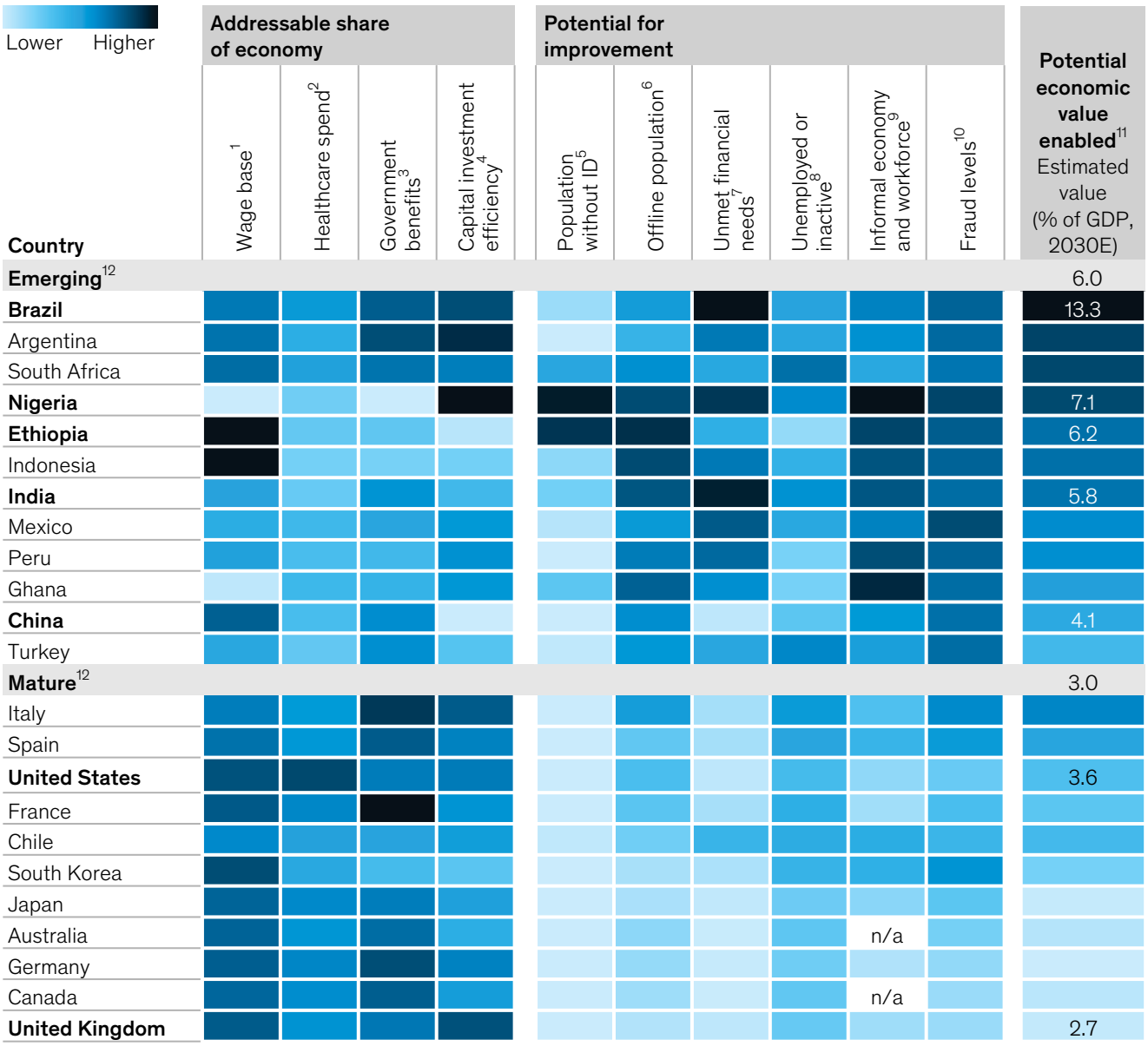
For mature economies, many processes are already digital, and the potential for improvement is more limited. This necessitates advanced digital ID programs that enable storing or linking additional information about individual ID owners that can facilitate advanced data sharing, with informed user consent, privacy protections, and control over personal data. 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.

[175] Jim Gee, *Annual fraud indicator: Identifying the cost of fraud to the UK economy*, UK Fraud Costs Measurement Committee, 2017.

Exhibit 12

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

Generating adoption will be a critical barrier to capturing the economic value from digital ID

Achieving high rates of adoption in multiple use cases is neither automatic nor certain. India's Aadhaar system has achieved over 90 percent coverage, while Nigeria's National eID, launched in 2014, has adoption rates below 10 percent.[176] Yet even in India, digital ID addresses a relatively small portion of the potential use cases, and recent policies and legal judgments have impacted Aadhaar usage and implementation outside the government sector.

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.[177] In the United Kingdom, the Gov.UK Verify digital ID offers authentication for more than 15 government services, including checking one's state pension and applying for a vehicle operator license.[178] By design, the program did not include more advanced data-sharing features that may encourage wider or faster adoption. Since the benefits could be significant, digital ID programs seem to be worth the effort, and continued research is essential to understand what drives adoption.

Beyond economic value, digital ID can be an important tool to empower individuals and foster greater inclusion

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.

A digital ID can be a critical element in ensuring that every child has access to an education. Birth certificates or national ID cards are required to enroll a child in primary school in Algeria, Cambodia, Kenya, Nepal, Peru, and Turkey, among many other countries.[179] A report by Plan International investigating the impact of birth registration on children's rights in India, Kenya, and Sierra Leone found a correlation between child identification and access to formal education. For example, the report found that children in Kenya with birth registration were 50 percent more likely to be enrolled in formal education and 20 percent more likely to be attending age-appropriate education.[180] Digital ID can provide convenient ID for the unidentified population and can unlock educational opportunities for many children who lack an ID or birth registration today.

A digital ID could also be an important enabler of access to healthcare. For example, the provision of unique identity to healthcare users has been a key factor in providing more than 100 million of India's poor with health insurance.[181] In Botswana, integration of the Omang national ID with a digital patient management system has improved administration efficiency and treatment outcomes for the country's flagship antiretroviral therapy HIV treatment program.[182] More advanced application of digital ID could have even larger effects, as demonstrated by uses of the Mobile Connect global digital ID system to provide medical practitioners with access to patient medical records. The San Diego Health Connect program used Mobile Connect to instantly alert doctors when patients were discharged from the hospital or admitted to the emergency room, allowing them significantly more time to consider optimal care strategies. The program also allowed doctors with the appropriate authorization

[176] "AADHAAR Dashboard," Unique Identification Authority of India, Uidai.gov; "About the e-ID Card," Nigeria National Identity Management Commission, Nimc.gov.ng, as of 2/1/2019.
[177] "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.
[178] "GOV.UK Verify Dashboard," Gov.UK.
[179] Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?,* Center for Global Development, October 2017.
[180] Kara Apland et al., *Birth registration and children's rights: A complex story,* Plan International Headquarters, 2014.
[181] Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?*, Center for Global Development, October 2017.
[182] *The role of digital identification for healthcare: The emerging use cases,* World Bank, 2018.

the ability to seamlessly examine medical information during visits, improving the speed, safety, coordination, and cost of medical care.[183]

Digital ID could 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, currently estimated to affect 160 million children, by providing proof of age. Several countries have recently strengthened identification for children in an attempt to fight child trafficking. In Peru, for example, the government launched the National Identification Document for Children in 2001. It requires that all children have identification documents in an explicit effort to reduce instances of and allow identification of victims of trafficking, sexual exploitation, and child labor.[184]

30%

The share of Estonians who vote online

Stronger identification could also help enforce laws against child marriage and thus contribute to its elimination and the empowerment of women and girls worldwide.[185] In Indonesia, for example, while 50 percent of all children had birth registration, 95 percent of the girls who married at 17 years of age or younger lacked a birth certificate.[186] Overall, a digital ID can increase official registration of marriages and provide undisputable proof of age for prospective spouses and allow appropriate officials to prevent registration of marriages that violate child marriage laws.[187]

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. For example, Pakistan updated its voter rolls with strong biometric controls that resulted in the inclusion of an additional 36 million new eligible voters as well as the elimination of 13 million entries with invalid identities, nine million duplicates, and 15 million entries without verifiable identities.[188] In Estonia, the use of e-ID allowed the transition of a multitude of government services online and has had the effect of increasing the transparency of government interactions. Under the Estonian system, individuals are able to determine what information about them is available through government agencies and who has access to it.[189] For example, more than 30 percent of Estonians vote online, of whom 20 percent say they would not vote at a physical polling place.[190]

In this chapter, we have outlined our calculations for the potential global economic value of high adoption of digital ID. It is significant—the GDP equivalent of 3 percent for a mature economy and 6 percent for an emerging economy. Overall, 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. 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. In the next chapter, we highlight these risks and explore how they can be overcome.

[183] GSMA, "Digital identity demonstrates its crucial role in transforming healthcare," blog entry, March 1, 2018, gsma.com/identity/digital-identity-demonstrates-crucial-role-transforming-healthcare.
[184] *ID4D country diagnostic: Peru,* World Bank, 2018.
[185] Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?*, Center for Global Development, October 2017.
[186] Cate Sumner, *Indonesia's missing millions: Erasing discrimination in birth certification in Indonesia*, Center for Global Development, June 2015.
[187] Lucia Hanmer and Marina Elefante, *The role of identification in ending child marriage*, World Bank, July 2016.
[188] Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?*, Center for Global Development, October 2017.
[189] Government Digital Service, "Government as a data model: What I learned in Estonia," blog entry by Peter Herlihy, October 31, 2013, gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/.
[190] *A comparative assessment of electronic voting*, Elections Canada, February 2010.

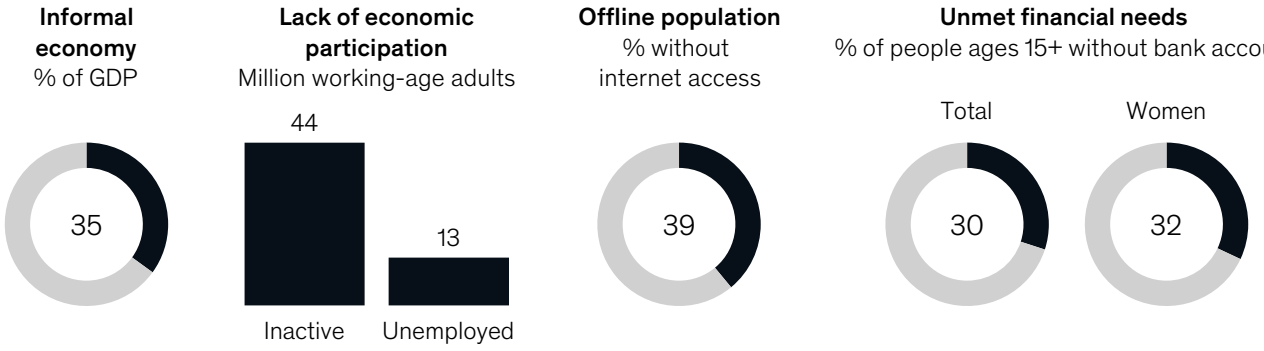
Country profiles

Brazil

Population 211M

Per capita GDP (2018 real $) $10K

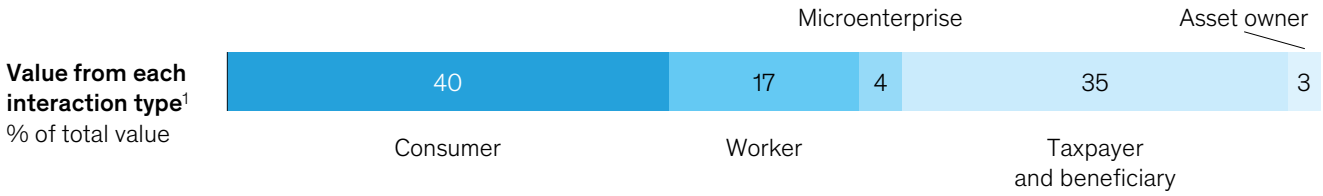
Areas for improvement through digital ID



Potential economic value enabled by digital ID

GDP equivalent value enabled by 2030

13% ($347B)



Selected examples of potential value generated[1]

$190B
increased investment from financial inclusion

$69B
reduced payroll fraud

3B
hours saved through streamlined e-government services

1. 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. Estimates of maximum 2030 potential value with advanced digital ID presented in 2018 real $.

Note: 2018 or latest available data for all statistics except GDP-equivalent economic value.

Source: World Bank ID4D; World Bank ID4D-Findex; We Are Social; International Labour Organization; McKinsey Global Institute analysis

Nigeria

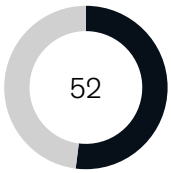
Population 196M

Per capita GDP (2018 real $) $2K

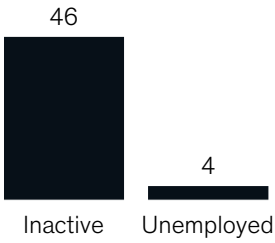
Areas for improvement through digital ID

ID coverage
Population, million people

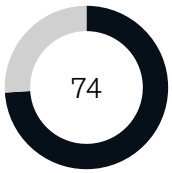
Informal economy
% of GDP



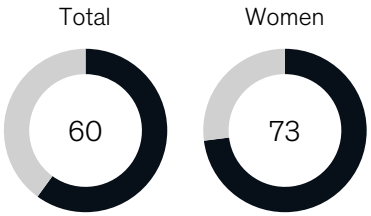
Lack of economic participation
Million working-age adults



Offline population
% without internet access



Unmet financial needs
% of people ages 15+ without bank account

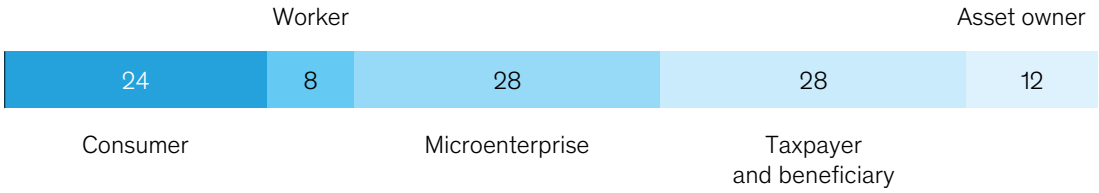


Potential economic value enabled by digital ID

GDP equivalent value enabled by 2030

7% ($59B)

Value from each interaction type[1]
% of total value



Selected examples of potential value generated[1]

$21B
increased investment from financial inclusion

1.1M
full-time equivalent employees added through increased employment from digital contracting

1.8B
hours saved through streamlined e-government services

Share of value[1]
% of total value

1. 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. Estimates of maximum 2030 potential value with advanced digital ID presented in 2018 real $.

Note: 2018 or latest available data for all statistics except GDP-equivalent economic value.

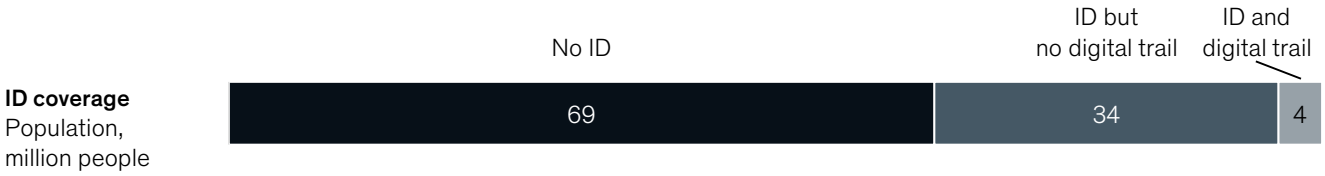
Source: World Bank ID4D; World Bank ID4D-Findex; We Are Social; International Labour Organization; McKinsey Global Institute analysis

Ethiopia

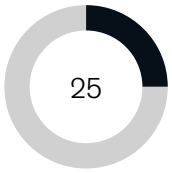
Population 107M

Per capita GDP (2018 real $) $768

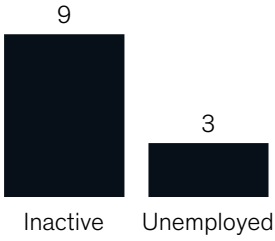
Areas for improvement through digital ID



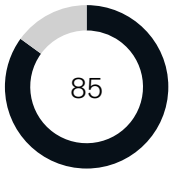
Informal economy
% of GDP



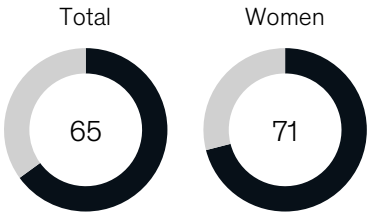
Lack of economic participation
Million working-age adults



Offline population
% without internet access



Unmet financial needs
% of people ages 15+ without bank account

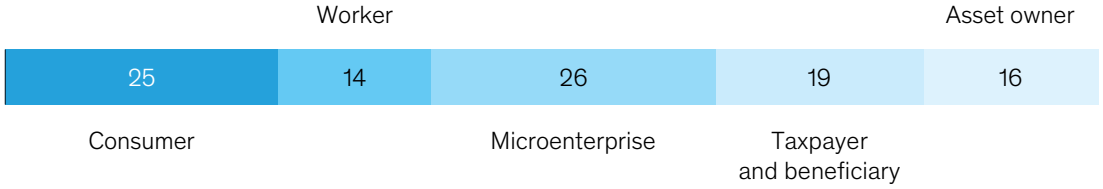


Potential economic value enabled by digital ID

GDP equivalent value enabled by 2030

6% ($12B)

Value from each interaction type[1]
% of total value



Selected examples of potential value generated[1]

$2B
increased investment from financial inclusion

1.4M
full-time equivalent employees added through increased employment from digital contracting

1.1B
hours saved through streamlined e-government services

Share of value[1]
% of total value

1. 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. Estimates of maximum 2030 potential value with advanced digital ID presented in 2018 real $.

Note: 2018 or latest available data for all statistics except GDP-equivalent economic value.

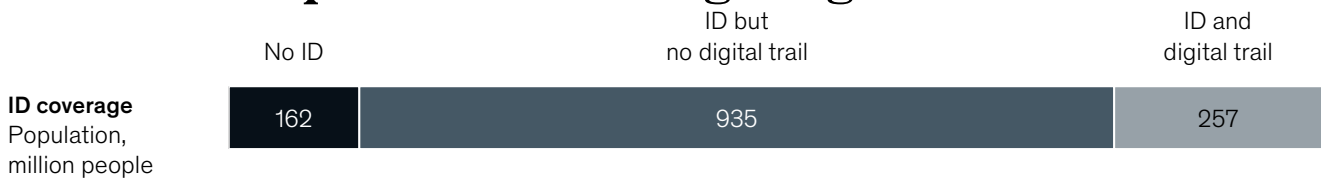
Source: World Bank ID4D; World Bank ID4D-Findex; We Are Social; International Labour Organization; McKinsey Global Institute analysis

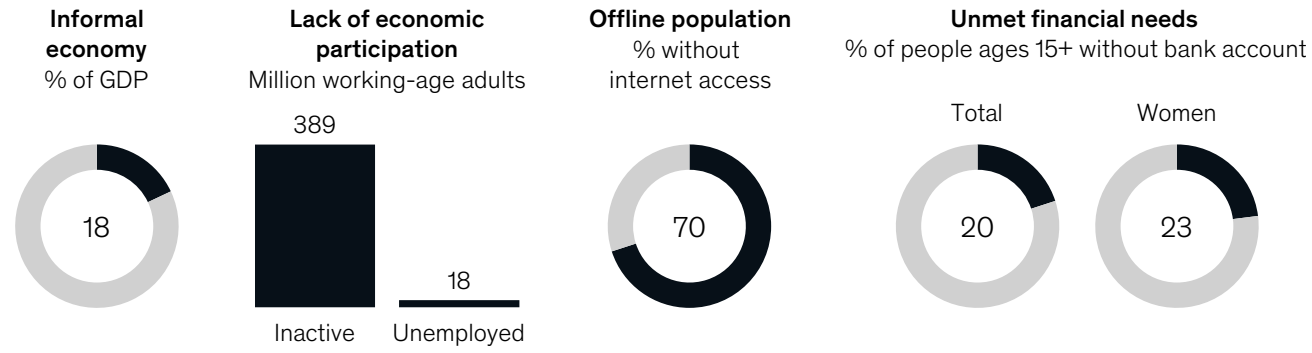
India

Population 1.3B

Per capita GDP (2018 real $) $2K

Areas for improvement through digital ID

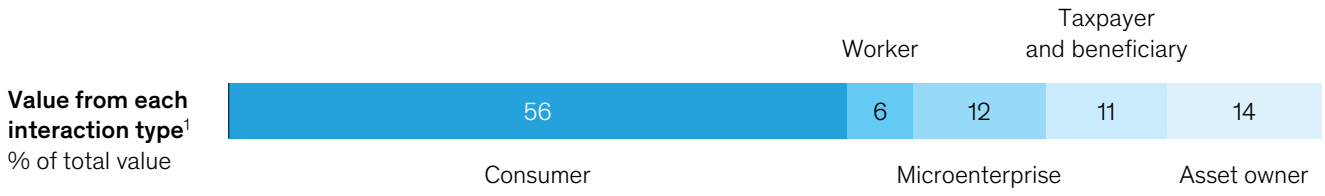




Potential economic value enabled by digital ID

GDP equivalent value enabled by 2030

6% ($409B)

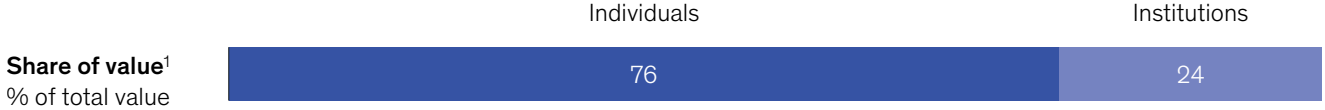


Selected examples of potential value generated[1]

$617B
increased investment from financial inclusion

6.3M
full-time equivalent employees added through increased employment from digital contracting

$55B
increased capital productivity from more formalized land ownership



1. 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. Estimates of maximum 2030 potential value with advanced digital ID presented in 2018 real $.

Note: 2018 or latest available data for all statistics except GDP-equivalent economic value.

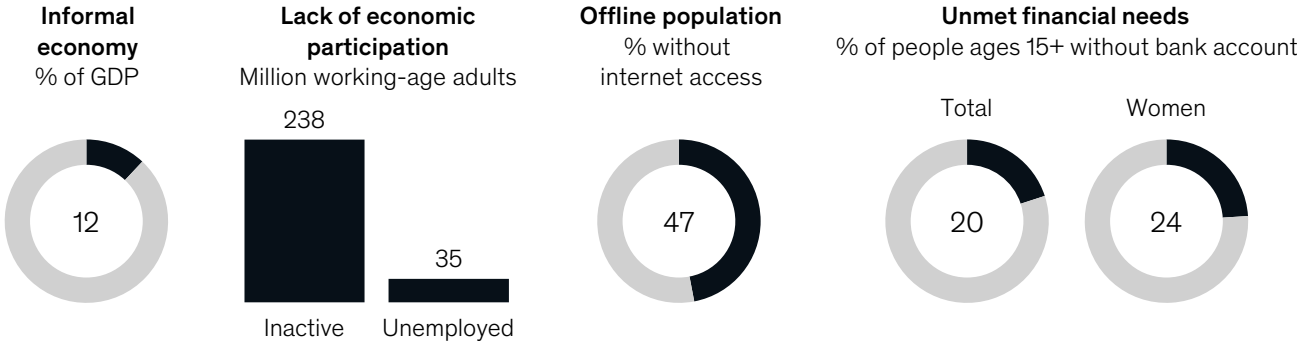
Source: World Bank ID4D; World Bank ID4D-Findex; We Are Social; International Labour Organization; McKinsey Global Institute analysis

China

Population 1.4B

Per capita GDP (2018 real $) $9K

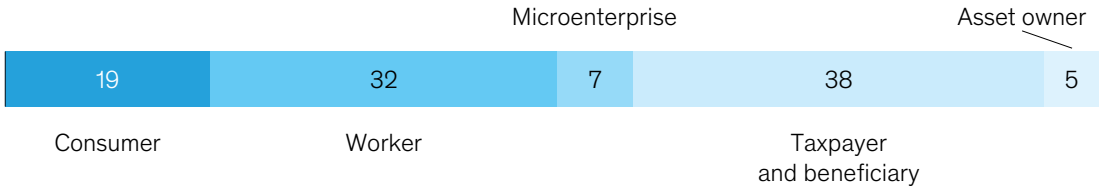
Areas for improvement through digital ID



Potential economic value enabled by digital ID

GDP equivalent value enabled by 2030

4% ($1.1T)



Selected examples of potential value generated[1]

$13B
reduced retail supply chain and operational costs

$445B
reduced payroll fraud

19B
hours saved through streamlined e-government services

1. "No ID" population figures are based on World Bank ID4D reporting of the latest registration levels for national ID. Where available registration data exceeds population or where data are limited, as in China, this number is set to zero.
2. 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. Estimates of maximum 2030 potential value with advanced digital ID presented in 2018 real $.

Note: 2018 or latest available data for all statistics except GDP-equivalent economic value.

Source: World Bank ID4D; World Bank ID4D-Findex; We Are Social; International Labour Organization; McKinsey Global Institute analysis

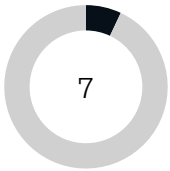
United States

Population 326M
Per capita GDP (2018 real $) $59K

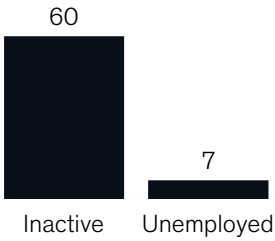
Areas for improvement through digital ID

ID coverage
Population, million people

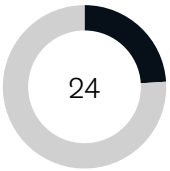
Informal economy
% of GDP



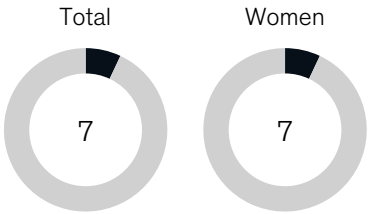
Lack of economic participation
Million working-age adults



Offline population
% without internet access



Unmet financial needs
% of people ages 15+ without bank account

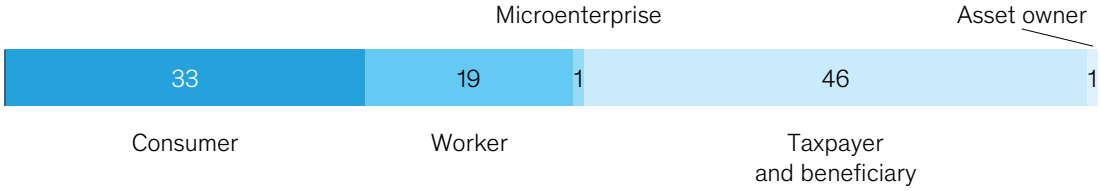


Potential economic value enabled by digital ID

GDP equivalent value enabled by 2030

4% ($995B)

Value from each interaction type[2]
% of total value



Selected examples of potential value generated[1]

$6B
reduced retail supply chain and operational costs

$287B
reduced payroll fraud

4.4B
hours saved through streamlined e-government services

Share of value[2]
% of total value

1. "No ID population" figures are based upon World Bank ID4D reporting of the latest registration levels for national ID. It is reported as zero in all high-income countries that have a birth registration rate of over 99.9%, such as the United States or United Kingdom.
2. 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. Estimates of maximum 2030 potential value with advanced digital ID presented in 2018 real $.

Note: 2018 or latest available data for all statistics except GDP-equivalent economic value.

Source: World Bank ID4D; World Bank ID4D-Findex; We Are Social; International Labour Organization; McKinsey Global Institute analysis

United Kingdom

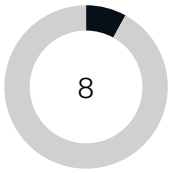
Population 66M

Per capita GDP (2018 real $) $40K

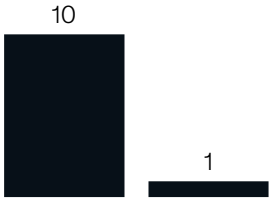
Areas for improvement through digital ID

ID coverage
Population, million people

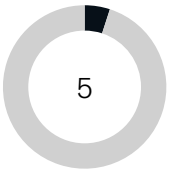
Informal economy
% of GDP



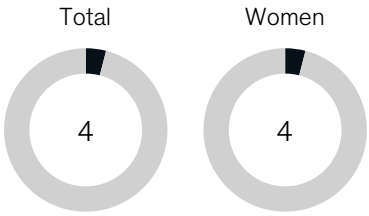
Lack of economic participation
Million working-age adults



Offline population
% without internet access



Unmet financial needs
% of people ages 15+ without bank account



Potential economic value enabled by digital ID

GDP equivalent value enabled by 2030

3% ($97B)

Value from each interaction type[1]
% of total value

Selected examples of potential value generated[1]

$5B
reduced retail supply chain and operational costs

$11B
reduced payroll fraud

450M
hours saved through streamlined e-government services

Share of value[1]
% of total value

1. "No ID population" figures are based upon World Bank ID4D reporting of the latest registration levels for national ID. It is reported as zero in all high-income countries that have a birth registration rate of over 99.9%, such as the United States or United Kingdom.
2. 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. Estimates of maximum 2030 potential value with advanced digital ID presented in 2018 real $.

Note: 2018 or latest available data for all statistics except GDP-equivalent economic value.

Source: World Bank ID4D; World Bank ID4D-Findex; We Are Social; International Labour Organization; McKinsey Global Institute analysis

4 Understanding the risks

Digital ID can form the foundation of a host of applications in many aspects of an individual's life, work, and social interactions, creating significant economic and social value. However, digital ID is not without potential for misuse, and it therefore requires proper controls and robust governance, together with established rule of law. Yet even when digital ID is used expressly for creating value and promoting inclusive growth, there are risks. Understanding and addressing those risks can help countries capture the significant economic value and other social and cultural benefits digital ID has to offer.

In this chapter, we identify and discuss two main sets of risks involved with "good" digital ID.[191] First, digital ID is inherently exposed to risks already present in other digital technologies with large-scale population-level usage. Second, some risks associated with conventional ID programs also pertain to digital ID and include human execution error, unauthorized credential use, and the exclusion of individuals. Digital ID could meaningfully reduce some of these risks by minimizing opportunity for manual error or breaches of conduct.

Stakeholders can use a common framework in prioritizing risks as they determine policy, governance, and system design (see Box 4: "Tailored assessment of risk severity and likelihood can guide policy and system design"). However, the specifics of risks differ for each digital ID program due to multiple varying underlying characteristics, including nature of the ID provider, other stakeholders involved, and the economic and geopolitical environment.

Digital ID is exposed to the risks already present in other digital technologies with large-scale population-level usage

Whether data breaches at credit agencies or on social media, failure of technical systems, or concerns over fraud or abuse, institutions and policy makers around the world today are grappling with a host of potential new dangers related to the digital ecosystem (Exhibit 14). The introduction of digital identification programs will be no exception to this broader trend. The risk of technological failure and cybersecurity threats are not present in conventional (or nondigital) ID systems, but they exist in any digital ecosystem, where data are typically concentrated and highly connected. Similarly, digital ID programs are exposed to risk of malfeasance by employees of the ID provider and requesting parties, particularly associated with the collection and exploitation of potential concentrated personal data.

Technological failure could generate significant costs, potentially slowing the pace of adoption and preventing economic value from being realized

Technological failure could occur because of hardware or software failure, or the failure of supporting infrastructure like electricity or the internet. Hardware failure could involve technical issues with the physical components of the digital ID system that cause loss or corruption of stored data, a reduction or collapse in processing power, or other limits on the functionality of the overall system. Software failure could involve issues with the programs or operating systems that enable the use and interoperability of the digital ID. These could include a wide variety of issues impacting either processing of user information on the back end or limiting front-end functionality for individuals or requesting parties. For example, a failure in the underlying digital ID hardware or software could limit the ability of users to

[191] "Good" digital ID can be verified and authenticated to a high degree of assurance, is unique, is established with individual consent, and protects user privacy and control over personal data. For more details see Box E1, "What is digital ID?"

Box 4

Tailored assessment of risk severity and likelihood can guide policy and system design

Country and system specific identification and assessment of risks helps prioritize areas for greatest attention, thereby informing policy and system design. Stakeholders considering or currently managing a digital ID program should perform a bespoke analysis to identify the highest priority risks for their system and the specific risk reduction mechanisms to invest in. The size of a risk event depends both upon its severity, if it were to occur, as well as the likelihood that it would happen (Exhibit 13).

The severity of a risk event, such as a cyber breach compromising personal data, encompasses both economic and non-economic impact. Economic impact reflects direct costs, remediation costs, and foregone opportunities. Non-economic impact reflects cost that may not be quantifiable, at least in the short term. In the cyber breach example, violation of user rights including privacy, control, or consent could be accounted for even if immediate financial cost was small or difficult to quantify.

The likelihood of a risk event represents the probability that it occurs. Likelihood will depend on the threat, actors and their capabilities, vulnerabilities in the technology environment, and the value of the underlying assets. In the cyber breach example, an ID provider such as an established banking consortium with preexisting, tested cyber protections might have a lower likelihood of cyber-breach.

Specifics of risk events matter for assessing both severity and likelihood. For example, a limited cyber intrusion attempt that does not gain access will have lower severity than a large-scale breach of hundreds of millions of customer records. For any provider, more limited intrusions are more likely than extensive ones.

Risk events with both high severity and high likelihood (top right of Exhibit 13) are highest priority. Policy, governance, and controls should all be designed to minimize, if not eliminate, such risks.

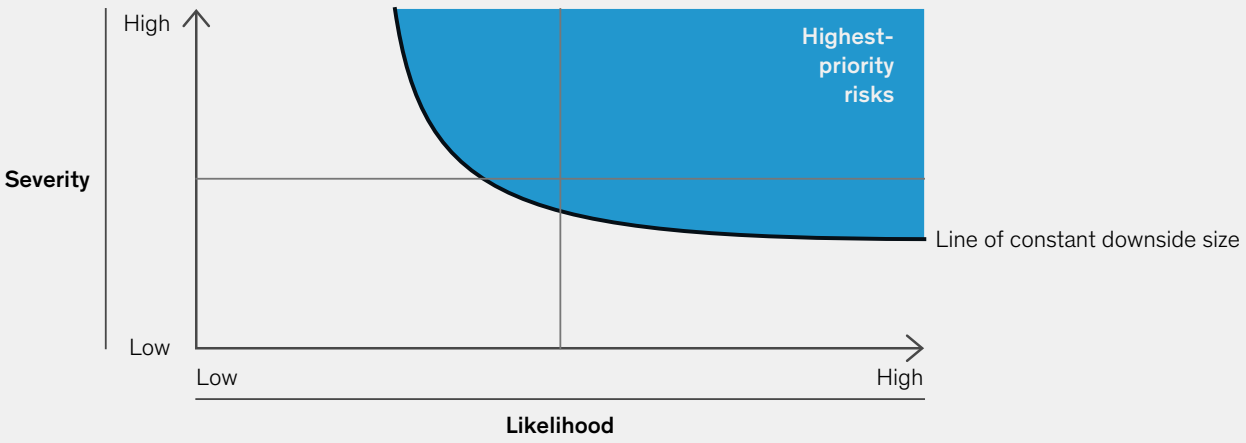
Risk events that are unlikely to happen but could be crippling if they do (top left of Exhibit 13) also require significant focus. A full system failure, destroying all data records, during a back-end migration provides a potential example. Guarding against such risks requires regularly pressure testing whether the risk really is highly unlikely, remaining vigilant to detect early signs of anything going wrong, and maintaining a water-tight back-up plan in case something does happen.

Total size also can be big for risk events with relatively low severity but that occur frequently (bottom right of Exhibit 13) if the small consequence of many occurrences adds up to something meaningful. For example, short base station power interruptions might delay interactions relying on mobile phone–based digital ID authentication. Associated costs and forgone opportunities for individuals, requesting parties, and the ID provider might add up in an area with spotty cellphone reception. Guarding against such risks requires continually improving controls to reduce their frequency, while also using robust system design—for example, by having a back-up method of authentication in regions with inconsistent reception.

Exhibit 13

Stakeholders may consider prioritizing risks based on severity and likelihood as an effective risk mitigation strategy.

Generalized risk profile

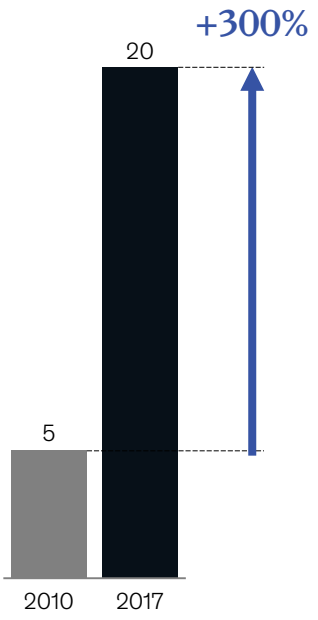


Source: McKinsey Global Institute analysis

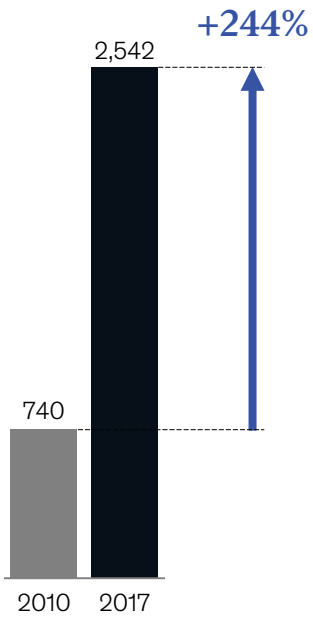
Exhibit 14

Risks and concerns associated with digitization are growing as the digital ecosystem expands.

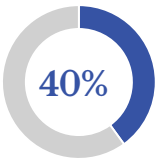
Global reliance on data is growing rapidly
Data usage (zettabytes[1])



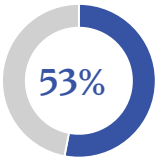
Cyberattacks are also on the rise
Number of cyberattacks in the United States



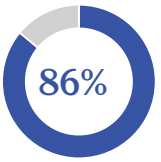
Individuals around the world have significant concerns about the use of their data
Survey of 6,500 individuals across 10 European countries, 2017



cite trust issue as most common barrier to using new technology applications



don't feel that they are in control of their data



took action, such as warning family and friends not to use a service, as a result of trust issues

1. One zettabyte is equal to one trillion gigabytes.

Source: Seagate; Identity Theft Resource Center; Privacy Rights Clearing House; Risk-Based Security; Mobile Ecosystem Forum; McKinsey Global Institute analysis

access, control, or share their digital ID, or impact the ability of requesting parties to request, receive, or authenticate a user's identification.

Even if the hardware and software do not fail for technical reasons, the technology itself could still fail due to issues with supporting infrastructure. Such infrastructure can include access to electricity, internet, or telecom that is necessary to enable remote access. This could be a particular problem in areas with existing infrastructure problems such as electricity outages that would prevent users or requesting parties from being able to employ the full functionality of the digital ID system for significant periods of time. In cases of digital ID use that require remote access for authentication, such as many e-government services and payment-related applications, events such as internet outages could cut off individuals from important services, potentially for extended periods of time.

A failure of the technology associated with digital ID would have both immediate remediation costs for the ID provider and potential economic losses associated with a reduced ability to access use cases. Additionally, large or consistent failures could create distrust in the ID system itself and cause both users and requesting parties to reduce or stop their usage. This would block the realization of many of the benefits of digital ID, which are generally dependent on widespread adoption and use of the system by both individuals and institutions.

Any large-scale digital system carries similar risks, but the nature of some digital ID uses makes the impact more severe in the case of digital ID systems. Such failures can cause significant damage for individuals, as was seen during a 2010 mobile network outage in New Zealand caused by a hardware failure at Telecom NZ that left some users without internet

access for days.[192] Even where adequate infrastructure and technical capabilities exist along with robust hardware and software to support consistent remote access, the magnitude of a technology failure's negative impact can be large if critical services are linked to authentication via digital ID. Preventing such impact will depend on investment in and controls built into digital infrastructure and system governance, such as contingency planning and provision of alternative authentication mechanisms, as we discuss in the following chapter. Without alternative authentication mechanisms, a large-scale failure in an advanced digital ID system could cut off a potentially significant amount of economic and social activity.

Cybersecurity threats are a growing risk across the digital ecosystem, and digital ID programs are no exception

$16.8b

The amount lost in the United States in 2017 from identity fraud

Cybersecurity risks are increasing around the world. The rapid expansion of digital ecosystems means that individuals are increasingly interacting digitally without high-assurance identities. At the same time, the existing inefficiencies, security challenges, and lack of control continue to multiply as more and more interactions shift into the digital realm. The number of accounts online and 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 16.1 zettabytes of data generated in 2016.[193] The security of accounts and increased digitization pose increasing downside risk for the digital economy. For example, $16.8 billion was lost in the United States due to identity fraud in 2017.[194] All of this data from new sources opens up vulnerabilities to private and sensitive information. There is a significant gap between the amount of data being produced today that requires security and the amount of data that is actually being secured, and this gap will widen—a reality of our data-driven world. By 2025, almost 90 percent of all data created in the global datasphere will require some level of security, but less than half will be secured.[195]

Cyberthreats impact individuals through unauthorized access to their personal data, institutions through unauthorized leaks of private and confidential transaction information, and ID providers through direct costs, decreased trust in the system reducing usage, and the potential for intrusion to make the system inoperable, for example, in the case of a hostile foreign military attack intended to introduce dysfunction in the enemy. Costs associated with adverse cyberevents across the existing digital ecosystem can be found in three categories: investment in cybersecurity and risk mitigation; the direct and indirect costs associated with an adverse cyberevent; and the opportunity costs of forgoing use of cyberservices or infrastructure in the wake of an attack or the threat of attacks.[196] Digital ID stakeholders will face the same costs as they deal with cybersecurity threats, and they must consider how to protect their systems against the very real threat of attacks.

The costs and disruptions can be significant. For example, Equifax, a massive credit rating agency based in the United States, was breached from an external party that gained access to 150 million individuals' personal records, such as addresses, financial documents, and Social Security numbers. To date, this violation has cost roughly $600 million in legal fees, free identity theft services, and required system upgrades.[197] In February 2016, a cyberintrusion into the central bank of Bangladesh allowed hackers to request the transfer of $951 million into bank accounts in Sri Lanka and the Philippines, of which they were able to steal $81 million despite a coordinated international response.[198] Cyberattacks have also targeted the basic infrastructure of states around the world, such as in a 2015 attack in Ukraine that shut down the electrical grid serving around 250,000 people.[199]

Any large-scale digital system runs similar risks, and while high-assurance digital ID systems can mitigate these risks, it could also exacerbate them because of aggregation effects. But by tying high-value use cases to a secure digital ID and replacing the insecure

[192] Vaimoana Tapaleao, "Telecom: 'Serious hardware failure' to blame for XT outage," *New Zealand Herald,* February 19, 2010.
[193] *Data age 2025: The evolution of data to life critical*, Seagate, March 2017.
[194] *Better identity in America: A blueprint for policymakers,* Better Identity Coalition, July 2018.
[195] *Data age 2025: The evolution of data to life-critical,* Seagate, March 2017.
[196] Barry B. Hughes et al., *Cyber benefits and risks: Quantitatively understanding and forecasting the balance,* Pardee Center for International Futures, 2015.
[197] John McCrank and Jim Finkle, "Equifax breach could be most costly in corporate history," Reuters, March 2, 2018.
[198] Michael Corkery, "Hacker's $81 million sneak attack on world banking," *New York Times*, April 30, 2016.
[199] Lorenzo Franceschi-Bicchierai, "Who hacked the lights in Ukraine?," Motherboard, December 1, 2016.|

authentication methods used today, digital ID has the potential to reduce the likelihood of intrusions through channels such as stolen passwords and phishing attacks. However, unless systems are designed with appropriate security controls, the aggregation of information that allows digital ID to unlock large portions of its economic value could also create a treasure trove of data to be accessed and generate a greater motivation to carry out cyberattacks to access more sensitive information. For example, for non-biometric systems, one ID code leaking could compromise the security of multiple systems that use the ID for authentication. The potential consolidation of information could also increase the magnitude of attacks, as breaches could reveal critical user information for large groups in the event of a large-scale breach of data tied to a digital ID. This risk emphasizes the need for measures such as distributed data storage and high standards for data storage in any digital ID system, as well as checks built into credentials and rigorous system governance, which we cover in more detail in the following chapter.

Digital ID will be exposed to the risk of malfeasance by employees of the ID provider and requesting parties

We discussed the threat of systemic misuse of a digital ID by governments or private institutions earlier in this report. Digital ID is also exposed to malfeasance by rogue individuals or groups both within the ID provider and at requesting parties. An institution may employ individuals or grant them administrative access to digital ID–related personal data, creating a risk that these individuals may access, disclose, or collect data without user consent.

28%

of global data breaches are perpetuated by internal actors

Internal misuse of data is a significant risk of digital systems; a 2018 Verizon report found that 28 percent of reported global data breaches were perpetrated by internal actors.[200] The internal actors responsible for these breaches included system administrators as well as employees in HR, finance, and customer service. Healthcare is particularly susceptible to malfeasance, with internal misuse of data responsible for 56 percent of all data breaches in the sector. Most misuse took the form of abuse of data privileges, and it often involved violations of patient privacy by doctors or other medical personnel who inappropriately looked at the personal details and medical history of people they know or interact with.[201] Misuse could become a particular threat in advanced digital ID systems with data-sharing capabilities because people with access to data could compromise the security of potentially highly sensitive medical, financial, or other information.

Internal misuse is a growing threat in the broader digital ecosystem, and a recent study of cybersecurity professionals found that 55 percent believed that the increasing number of devices with access to sensitive data was the main cause.[202] If a digital ID is integrated into a host of critical applications across a wide variety of sectors, an insider threat could further increase. Potential break points could include employees, IT users or technicians, and contractors at both ID providers and requesting parties, who could take advantage of their access to sensitive and potentially highly valuable personal information.[203] Whether used for illicit profit, espionage, criminal activities such as blackmail or extortion, or more minor privacy violations, malfeasance could pose a significant risk and undermine trust in the ID system. Effective management of access rights and rigorous governance within both ID programs and requesting parties will be critical to minimize the likelihood and magnitude of individual malfeasance and protect the integrity of user data.

In addition, shifting regulations and consumer preferences are placing increasing emphasis on data privacy and control for all digital systems. These privacy measures are in part a response to the plethora of cybersecurity threats and incidents of misuse in the digital world today and reflect rising consumer awareness of privacy concerns. 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. As we discuss in the following chapter, these regulations will impact the internal governance, security, and data management

[200] *2018 data breach investigations report,* Verizon, 2018.
[201] Ibid.
[202] *Threat monitoring, detection and response report,* Crowd Research Partners, 2017.
[203] Ibid.

standards that digital ID will have to meet and will be an important factor in how the systems are designed and implemented. Beyond policy, preventing misuse will require careful consideration of governance measures such as independent oversight and management of access rights.

Digital ID reduces risks associated with conventional ID, but some risks may take on a different character

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 these risks by minimizing opportunity for manual error or breaches of conduct, but these risks will also manifest themselves in new ways when users utilize and interact with their ID through a digital interface.

While digital ID reduces the likelihood of human error, this risk remains present
Poor data entry, inadvertent data release, and unsecured communication with vendors are all examples of human execution risks that currently plague many conventional ID programs and could also reduce the validity and usability of a digital ID. Poor data entry includes incorrect transcribing of personal information from documents or testimony provided during registration or in updates to ID-related data. Inadvertent data release can include accidental disclosure of personal data or accidental data sharing, including situations where administrators leave printouts or storage devices containing personal data in a public space. Unsecure communication with vendors includes accidental sharing of data with third parties without appropriate controls or authorization.

While conventional IDs carry a high likelihood of human error due to the inability to reconcile data across different databases or sources of information, digital ID could reduce the likelihood of execution error by integrating data sources and implementing data quality checks and controls. However, the types of error than can occur will change as digital technology is introduced into the identification process. Human error is a generally unavoidable issue when interacting with digital systems, and digital ID is unlikely to be an exception. In particular, the input of data is exposed to data entry errors, and individuals associated with the ID provider and requesting parties could potentially inadvertently release data.

The magnitude of impact resulting from errors made at the human-digital interface could be greater than that of errors made with conventional IDs. For digital IDs that are integrated with a wide variety of economic and noneconomic use cases, such as payments and voting, respectively, mistakes could have widespread implications and flow through to an individual's ability to authenticate themself or an institution's ability to trust in authentication. Therefore, it will be critical that ID providers design their system with checks and controls against human error, including measures such as systemic cross-checks of data entered in databases, and ensure effective oversight and governance of ID programs and their employees or contractors.

Unauthorized use or manipulation of credentials is a risk with digital ID
The risk of unauthorized use or manipulation of credentials can include measures such as counterfeit credentials used by individuals or institutions to commit identity theft or obscure an identity. This risk is already prevalent with conventional IDs, with fake or stolen identification documents used for identity theft, and illegal activity such as tax avoidance and noncompliance with legal requirements such as the drinking age. Even the most advanced credentials face the risk of unauthorized use or manipulation, and bad actors will have a large incentive to develop new and advanced methods of doing so.

Digital ID, however, can address some elements of this risk by enabling the credential to be cross-referenced with the relevant databases and, in some situations, leveraging biometrics to verify identity. Such features would significantly increase the difficulties associated with creating false credentials or stealing the credentials of others and would reduce the likelihood of unauthorized use occurring. However, instances where this risk does occur with digital IDs in the absence of proper risk reduction mechanisms could have an outsize

magnitude of impact relative to conventional IDs. A significant example is the fabrication or theft of biometrics, which are, by definition, irreversible. In the event of a biometric being stolen or fabricated and a mechanism being developed to enable its use, remediation may be very difficult if not impossible. The difficulty extends to nonbiometric credentials associated with digital ID systems, such as smart cards. Such credentials can be expensive and difficult to replace relative to conventional IDs, increasing the costs associated with their fabrication or unauthorized use. Preventing significant harm to users will require careful consideration of credential risks when building out the digital infrastructure of a program, and measures such as affordable and easy replacement of compromised credentials to make it possible for people who have been affected to safely and effectively authenticate themselves.

Digital ID, like conventional IDs before it, faces the risk of excluding individuals from critical services and the ability to authenticate their identity

Although digital ID can be used as a tool to include many people without an identity, if a digital ID becomes mandatory to access public services, such as food aid, or private services, such as opening a bank account, individuals who cannot or do not want to acquire a digital ID could be adversely affected. Individuals without sufficient technological access or savvy or who do not trust a digital ID system could be completely excluded. In addition, infrastructure limitations such as limited internet or telecom access could prevent individuals in rural or poor communities from participating in digital ID systems.

While exclusion is an existing risk for conventional ID programs, the likelihood of exclusion would decrease with the spread of digital IDs across the population, especially in areas with low existing ID coverage and many developing countries. However, digital ID may have the effect of increasing the likelihood of exclusion if it encourages widespread requirements for use of the digital ID as a barrier to access to services without recourse to alternative authentication methods. This could become a significant problem if institutions respond to the introduction of a digital ID by making it a mandatory requirement for a host of services that do not currently require conventional ID. A motivation for this could be a desire to leverage data-sharing capabilities or changed incentives due to reduced authentication costs with digital ID relative to conventional ID. Such an outcome could not only increase the likelihood of exclusion but increase the magnitude of the risk that people without IDs could be cut off from critical social or economic services that they used to be able to access. ID providers will have to make inclusion a goal and adapt their digital infrastructure and policies to prevent negative impacts on individuals without an ID. These measures could include provision of alternative authentication mechanisms for service provision, and efforts to adapt the ID to areas with limited infrastructure, as we discuss further in the following chapter.

For example, in India, the mandatory integration of Aadhaar into social programs may have inadvertently resulted in some instances of food deprivation and restrictions on social security, particularly for the poor and elderly when distribution shops for food rations had trouble reading fingerprints or could not connect to the central server through the cellphone network. Additionally, some individuals may have been denied social security pensions despite suffering from disabilities that prevented them from using Aadhaar.[204] In response to concerns about such incidents, several local governments, including New Delhi's, stopped using Aadhaar for food programs.[205] These instances were referenced in decisions by the Indian Supreme Court, which ruled in 2018 that no person can be denied benefits under a social welfare program because of failure of authentication through Aadhaar.[206] The Aadhaar Act of 2016, and its related regulations, already had a provision for exception management in case Aadhaar-based identification was not possible. Furthermore, government agencies such as UIDAI, the Direct Benefit Transfer mission, and related ministries had issued directions reiterating this and highlighting various exception management processes to avoid such situations. This serves to highlight that even with policies in place, implementation failures can materialize that could result in possible exclusion. The court also ruled that Aadhaar

[204] Soutik Biswas, "Aadhaar: Is India's biometric ID scheme hurting the poor?," BBC News, March 27, 2018.
[205] Gaurav Vivek Bhatnagar, "Testimonies reveal how Aadhaar has brought pain, exclusion to the poor," The Wire, March 15, 2018.
[206] "Aadhaar needed for PAN, not for bank a/c: Key points of SC," *Times of India*, September 26, 2018.

authentication cannot be made mandatory for private-sector applications such as bank account opening or registration for mobile connections. Recent amendments proposed in parliament would make it permissible for companies to leverage Aadhaar on a voluntary basis if they also offer and make consumers aware of alternative identification options.[207]

Any discussion of the value of digital ID must also include a discussion of the potential risks involved. In this chapter, we have provided an overview of key risks associated with digital ID. They fall into two groups: risks associated with digitization broadly, and risks that are also associated with conventional IDs. The discussion of risks in this chapter provides a first step in understanding how to mitigate risk in designing, implementing, and governing a good digital ID system. We turn to that topic in the next chapter.

[207] "Cabinet nod to amendment of laws for Aadhaar seeding with mobile numbers, bank accounts," *Times of India,* December 17, 2018.

5 Toward implementation

Good digital ID systems will be adopted and used on a sustainable basis if they provide value for all stakeholders, including individuals, businesses, and governments, and engender trust. Therefore, a focus on promoting value and trust is critical to governance throughout the life cycle of a digital ID system, from design to implementation. To inform critical design and implementation decisions, the state of digital infrastructure, trust in institutions, and the policy landscape need to be fully assessed. Additionally, digital ID programs should prioritize use cases that generate meaningful value for both individuals and institutions. At the same time, a focus on ongoing excellence in customer and user experience, including easy registration, also matters. Finally, to unlock value while addressing risk, digital ID systems require careful design, appropriate identification infrastructure, and well-controlled governance. In this chapter, we outline areas that matter for capturing the value of digital ID and outline concrete steps that all stakeholders can take to participate in and promote a successful digital ID program.

Assessment of digital infrastructure, level of trust in institutions, and policy landscape is a key first step in implementation

A minimal level of digital infrastructure, sufficient trust in the digital ID provider, and a policy landscape that provides some safeguards to individuals are preconditions for the implementation of a digital ID system. Beyond these minimal levels, the specific characteristics and state of these essential factors will help shape choices about the design, implementation, and governance of the ID system. In this section, we discuss these key factors that must be assessed from the outset to help stakeholders build a sustainable digital ID system.

60%

of people in sub-Saharan Africa are covered by a 3G or 4G network

Internet access, degree of smartphone penetration, and reliability of electricity make up the foundation of digital infrastructure necessary for a digital ID program

A digital ID system relies on some basic level of digital infrastructure, including the level of internet access, degree of smartphone penetration, and reliability of electricity supply. Programs requiring remote access by users, such as e-government services, depend on widespread internet access that at a minimum must cover internet-enabled hotspots to allow for authentication. Countries' levels of internet access vary significantly, with 99 percent of people in North America living in areas covered by a 3G or 4G network compared with only 60 percent in sub-Saharan Africa (Exhibit 15).

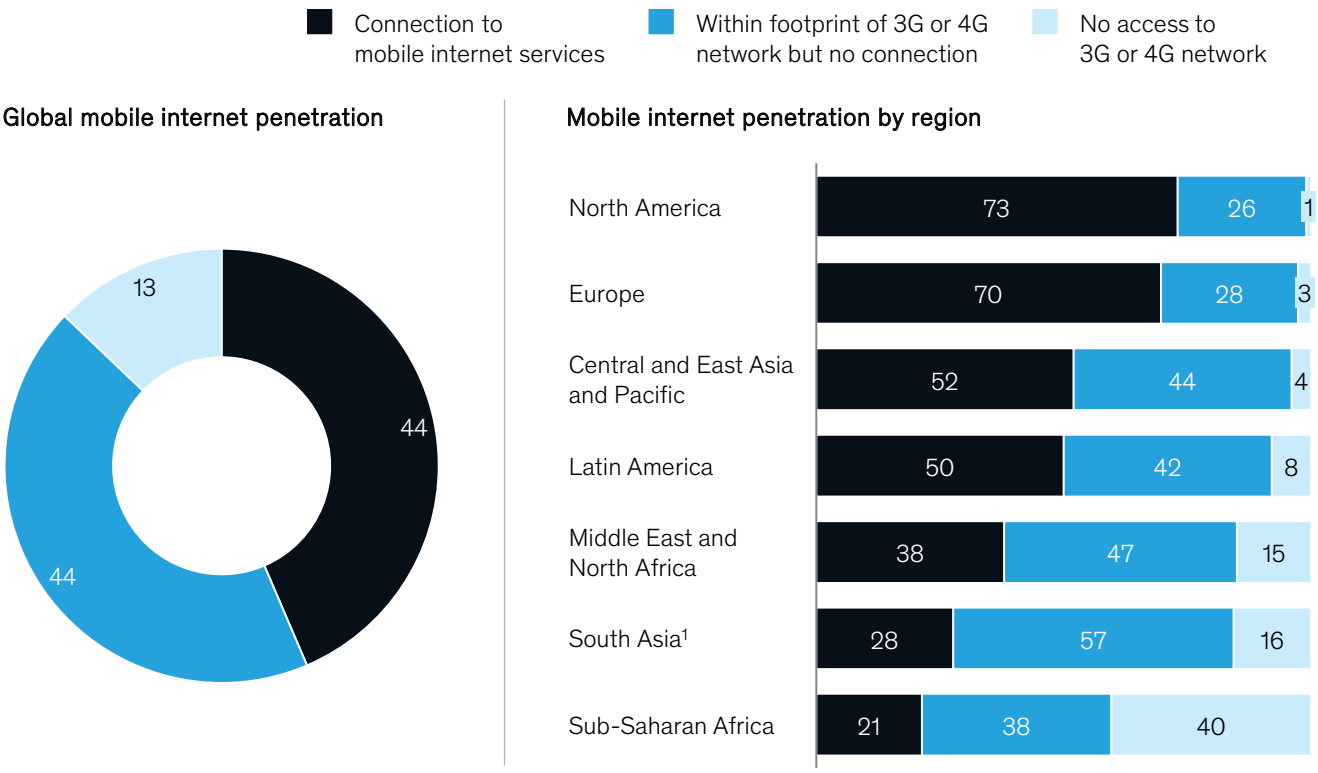
Internet access is not enough. Digital ID systems require penetration of devices necessary for adoption by both users and requesting parties. The World Bank found that 54 percent of individuals globally do not use the internet, which greatly limits their ability to participate in programs even in areas that are covered by a network.[208] Digital ID programs need to access devices such as smartphones to improve feasibility and promote ease of adoption. Across emerging economies, phone subscriptions and smartphone ownership are either already high or growing fast. However, smartphones still remain unaffordable for many people. Lastly, a reliable electrical grid ensures the consistent system functionality necessary for providing predictable services and maintaining trust in the system. This is a particularly big problem

[208] World Telecommunication/ICT Development Report and database, International Telecommunication Union, June 2018.

Exhibit 15

Global mobile technology penetration varies across regions.

% of population



1. Connection to mobile internet services and network access has been growing rapidly in South Asia. Telecom Regulatory Authority of India reported that there are 1.17 billion wireless phone subscribers and 560 million internet subscribers in India alone as of October 2018.

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

Source: GSMA, *State of Mobile Internet Connectivity 2018*; McKinsey Global Institute analysis

in low-income countries, where the World Bank estimated in 2016 that 61 percent of the population—72 percent in rural areas—did not have electrical access.[209]

For programs in areas where infrastructure is limited, digital ID might first be extended to parts of the country with more robust infrastructure. Digital ID programs rolled out in areas with limited digital infrastructure access may fail to work. This could affect the trust necessary for requesting parties and users to enable high-value applications, possibly making both requesting parties and users less willing to invest in a system that offers access to authentication only intermittently. In particular, ID providers in countries without consistent internet access would likely be able to support only uses that could be accessed at central locations (which would themselves, at a minimum, need consistent internet access). Those uses could include disbursement of government benefits or subsidies, which can be made out of internet-connected disbursement centers.

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. Most emerging economies lag behind advanced economies in their payment systems infrastructure, although some are taking the lead. For example, Jordan and Peru are building payments architecture that is faster and less costly than many payment systems in advanced economies.[210] As a second example, 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,

[209] Sustainable Energy for All (SE4ALL) database, International Energy Agency and World Bank, updated on June 29, 2018; SE4ALL Global Tracking Framework World Bank, International Energy Agency, and the Energy Sector Management Assistance Program.

[210] *The Level One Project guide: Designing a new system for financial inclusion,* Bill & Melinda Gates Foundation, April 2015.

and digital asset registries are all infrastructure preconditions for important ways of using digital ID involving government service provision, medical care, and landownership. For example, Estonia developed an e-Land Register web application that contains information on all ownership relations and limited real rights for more than one million properties and land parcels. This register is integrated with Estonia's digital ID through the X-Road data-sharing system and has become an integral part of the country's real estate market.[211]

While some underlying level of digital infrastructure is necessary, even for basic digital ID, a lack of infrastructure to support more advanced digital ID applications is not an impediment to successful implementation of basic ID. Over time, higher functionality can be developed.

Users must trust the institutions handling their data as ID providers or requesting parties to enable program adoption and promote ongoing usage

Individuals and institutions will only use a digital ID program that they trust. In good digital ID programs, users and requesting parties must trust that the data they share with the ID provider will be secure and remain in their control. Studies have found that the institutions people in different countries trust to handle their data vary significantly, as do the types of data that individuals feel require elevated levels of privacy. These factors will significantly impact the types of institutions that succeed in providing and adopting a digital ID program.

A study of European attitudes toward data sharing by YouGov on behalf of the Open Data Institute found significant differences among both institutions and countries in levels of user trust (Exhibit 16). Healthcare providers, financial institutions, and local governments were generally trusted the most, but the degree of trust varied by up to ten percentage points across the five countries surveyed.[212] Research commissioned by Omidyar Network further revealed the large geographic divide associated with user trust. The study found that relative levels of trust differed significantly across the world, with individuals in Eastern and Central Europe much more likely to trust governments relative to private companies, while individuals in Latin America were more than twice as likely to trust private companies over government.[213] These differences imply that the institutions most likely to gain user trust for data management will differ across geographies and cultures, with implications for the optimal implementation approach and the ability of a digital ID to garner adequate adoption.

The value individuals place on data privacy and security also depends on the type of data shared through a program. The relative value individuals place on the privacy of their data varies across the world and is rapidly changing. A recent review of public attitudes toward the importance of privacy found significant differences in how much individuals in different countries, even those at similar levels of economic development, value data privacy.[214] For example, respondents in Germany placed significantly more value on data privacy than those in the United States or Britain, who in turn valued privacy significantly more than respondents in China or India. The authors also found that individuals across countries differ in the types of data they consider most important, with German respondents valuing the privacy of their health history ten times more than respondents in the United States.

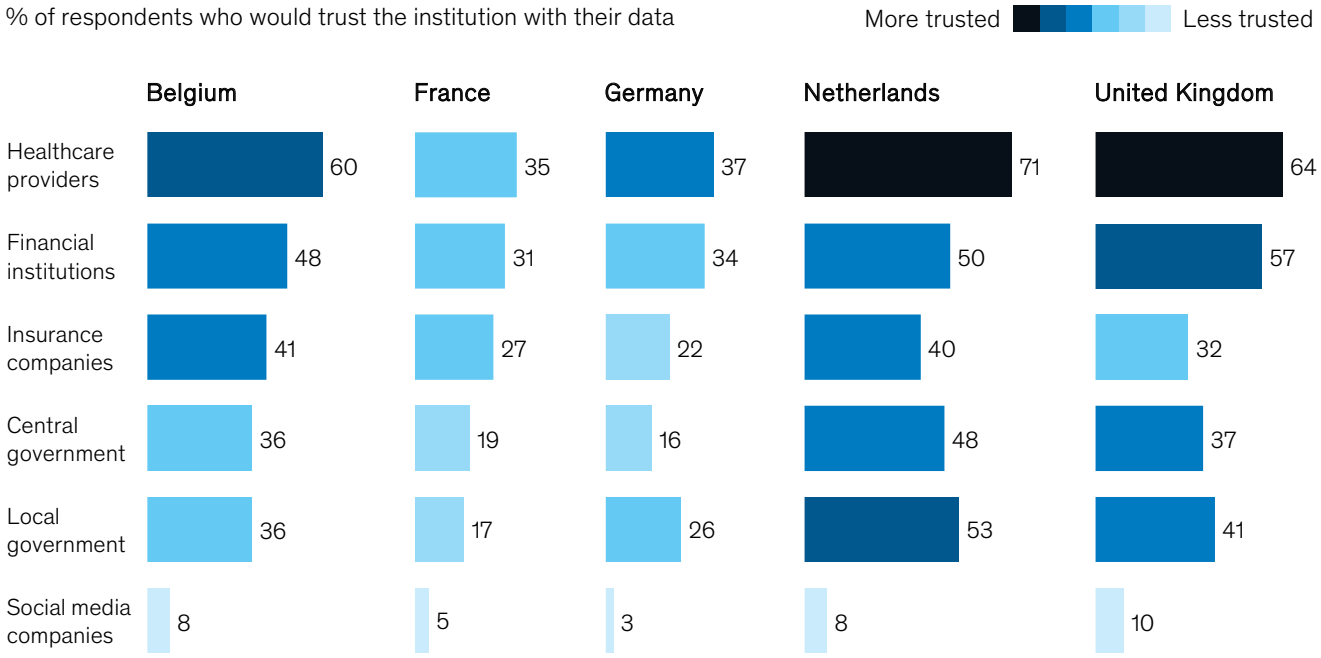
Levels of trust and attitudes about privacy vary by country and are evolving over time. An Accenture personal data survey in 2014 found that 69 percent of surveyed businesses said their customers were becoming more aware and concerned about privacy concerns, and 67 percent of businesses surveyed said customers were taking actions to protect their privacy more proactively, such as changing passwords more often and opting out of services.[215] As institutions consider involvement with digital ID, whether as ID providers or requesting parties, they will need to strongly consider preconceived user perceptions of their sector and the value users place on the data that will be involved in a digital ID system.

[211] "e-Land Register," e-Estonia, e-estonia.com/solutions/interoperability-services/e-land-register/.
[212] "Attitudes towards data sharing," YouGov on behalf of the Open Data Institute, July 4, 2018.
[213] "Trust and privacy," Omidyar Network, October 2, 2017.
[214] Ibid.
[215] Tim Cooper and Ryan LaSalle, *Guarding and growing personal data value*, Accenture, 2016.

Exhibit 16

Individuals in Europe trust healthcare providers, financial institutions, and local government with access to their data—but trust varies across countries.

% of respondents who would trust the institution with their data



Source: "Attitudes towards data sharing," conducted by YouGov on behalf of the Open Data Institute; McKinsey Global Institute analysis

A policy and regulatory landscape that protects privacy, addresses systemic risk, and establishes a legal framework for digital ID is a necessary foundation for a program

The policy and regulatory landscape in any country sets the framework for the ID system and lays the groundwork for addressing systemic risk. Legal protections and recognition for use of digital identification 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 digital ID use cases.

The legal foundation of an ID will include policy that determines access and the processes that must be followed to consider an identity legally authenticated. This will be particularly crucial to unlock use cases tied to sensitive personal information or requiring high levels of assurance such as access to health records or financial transactions. In particular, governments will have to define under what conditions use of a digital ID would be considered acceptable in judicial proceedings or legally binding. With more advanced data-sharing activities, institutions that are sharing and requesting data will need policy guidelines to reduce their risk and encourage adoption of digital ID. For example, these might include guidelines for dispute resolution in cases resulting from digital ID usage, and guidelines on legal requirements and liability in the event of cybersecurity breaches.

Privacy is another key consideration for policy makers. An appropriate level of user privacy protection is necessary to build the trust required for broad-based adoption. Digital systems that are transparent about the information they gather and give customers control of their personal data will earn user trust and ongoing as well as expanded access.[216] However, policy makers should be aware that poorly designed privacy protections can inadvertently

[216] Timothy Morey, Theodore "Theo" Forbath, and Allison Schoop, "Customer data: Designing for transparency and trust," *Harvard Business Review*, May 2015.

Box 5

Europe's GDPR defines data rights and has led to significant challenges for institutional compliance

The European Union's General Data Protection Regulation (GDPR) takes a rights-based approach to data privacy that is intended to provide a common framework for data interchange and data privacy across the EU by shifting the burden of privacy risk from individuals to the institutions that process their data. It is the most comprehensive data privacy law globally to date. Under the law, EU residents have the right to access, erase, or object to use of their personal data. Facing fines of up to 4 percent of global annual revenues for violations of the law, companies have had to prioritize implementation of controls that protect these rights of European residents.

GDPR leaves significant room for legal interpretation of its principles, which has forced institutions to make hard choices regarding what constitutes an unacceptable risk from a compliance perspective. In particular, organizations have had to define the scope of individuals covered, the set of necessary processes and controls, and the time frames for GDPR-related services.

Several of the challenges that institutions in the EU have experienced can provide insight for countries hoping to pursue a similar approach and illustrate the potential for digital ID systems to enable data privacy regulation in addition to benefiting from it. These difficulties include developing the ability to identify personal data and data processing activities, implementing individual data rights, managing third parties, and deploying technology and organizational controls. Beyond the capacity to localize relevant personal data, organizations have faced broader difficulties in implementing processes to ensure that the provision of individual data rights defined by the regulation and the reporting of breaches to regulators are executed within mandated time frames. Implementation of rights such as data access and erasure can have huge implications for existing data management systems, and uncertainty about the expected volume of user requests has made companies unsure of the level of investment necessary to enable full compliance.

Institutions that have successfully implemented GDPR programs have generally defined a detailed IT target state and organization to ensure sustainable compliance and have pursued a consent-driven data approach and a clear tiering of automation levels. Overall, GDPR has transformed the European privacy landscape. The lessons learned from its implementation show the challenges, and potential, of such an approach to data regulation.

introduce frictions and reduce the use cases and economic value that can be unlocked by an ID program.

Policy makers can ensure privacy protection and address systemic risks through a rigorous regulatory framework. In particular, regulation can realign incentives for businesses and governments to behave in a way consistent with the collective interests of individuals and the broader society. 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. Countries around the world have made considerable progress in recent years in developing privacy regulations, with the furthest-reaching regulations developed by the European Union through the 2016 General Data Protection Regulation (see Box 5, "Europe's GDPR defines data rights and has led to significant challenges for institutional compliance").

When crafting policy to address privacy concerns and other systemic risks, policy makers should account for the potential trade-offs associated with regulation. In particular, measures that impose significant regulatory burdens on requesting parties or ID providers could generate direct costs of compliance and impose constraints on ID adoption and innovation. For example, a study by the Information Technology & Innovation Foundation found that stringent privacy regulations do not have a measurable impact on user trust or adoption of digital applications or systems and can reduce the willingness of institutions to invest in innovative digital use cases.[217] Meeting the challenge of protecting citizens' privacy without

[217] Alan McQuinn and Daniel Castro, *Why stronger privacy regulations do not spur increased internet use*, Information Technology & Innovation Foundation, July 2018.

unduly suppressing digital innovation will only become more important as the global digital ecosystem continues to expand.

In addition to privacy considerations, digital ID uses will be dependent on the rules and regulations requiring individuals to show identification in order to receive products or services. Such rules include KYC requirements, mandated by nearly every country in the world for financial institutions, in conformance with the recommendations of the Financial Action Task Force.[218] KYC rules also are typically in place for subscriber verification for purchasers of mobile devices. To foster financial inclusion, many countries have put in place the potential for e-KYC, enabling providers to capture user identification details electronically, as would occur using digital ID. For example, banks in India can use the Aadhaar digital ID to perform electronic authentication of an individual's biometric information and demographic details. If a customer consents to the process, the bank can send a fingerprint to the Unique Identification Authority of India and can instantly open an account for the customer if the authentication is successful.[219]

If digital ID is used to satisfy rules and regulations, it becomes all the more important to actively minimize the risks of excluding anyone who does not have, or does not want to use, a digital ID. Policy measures to address the risk of exclusion could include additional funding for infrastructure and remote access to ID registration as well as requirements for alternative authentication methods for individuals who cannot use or opt out of using a digital ID. The dynamics of mandatory adoption can also apply to policies made by private institutions, such as industry-wide digital ID requirements. Responding to concerns about exclusion resulting from mandated ID use by private companies, the Indian Supreme Court ruled that banks and telecommunication companies were not allowed to require digital ID as a precondition of providing services.[220]

70%

or higher:

The adoption rates of digital ID in Denmark and India

To achieve adoption and usage, digital ID programs must provide value and reduce friction for both individuals and institutions

To unlock the potential value described in this report, widespread adoption and usage of digital ID programs by individuals and institutions are essential. While the path to achieve this varies by country, both successful programs and costly scrapped failed systems provide important lessons. The most successful cases, such as Denmark and India, indicate that adoption rates can surpass 70 percent in less than five years; in other cases, such as the United Kingdom and Nigeria, adoption has been slower, with rates so far under 10 percent.[221] Willing and widespread adoption and usage will occur only if the digital ID provides more value than the status quo, if the user experience is positive, and if initial registration is easy.

Use cases in financial services and government provide the greatest value relative to existing alternatives for both individuals and institutions

Digital ID programs should prioritize use cases that generate meaningful value for both individuals and institutions, to quickly generate a critical mass of users. Both users and institutions will need to be able to capture value from use cases introduced in a digital ID system to encourage adoption. This value should be greater than the value of existing alternatives to digital ID.

A use case generates value relative to the status quo in different ways for individuals and institutions. For individuals, this means generating cost or time savings or making access to products or services easier or newly possible. This value must be sufficiently greater than alternative methods of accessing similar services and outweigh an individual's perceived risks of using the ID. Meanwhile, institutions will be drawn to use cases that reduce costs, increase revenue, or, in the case of public institutions like government, improve economic or social

[218] *FATF 40 recommendations,* Financial Action Task Force, October 2003.
[219] *FATF guidance: Anti-money laundering and terrorist financing measures and financial inclusion*, Financial Action Task Force, November 2017.
[220] Vindu Goel, "India's top court limits sweep of biometric ID program," *New York Times*, September 26, 2018.
[221] *The next generation of national electronic identity and signing in Denmark*, Denmark Ministry of Finance Agency for Digitisation, April 2016; "AADHAAR Dashboard," Unique Identification Authority of India; "About the e-ID Card," Nigeria National Identity Management Commission; "GOV.UK Verify Dashboard, Gov.UK; as of 1/2/2019.

welfare. Individuals who use a digital ID gain when more institutions accept that ID. All else being equal, institutions will prefer ID-based solutions that improve customer experience, thereby increasing usage.

We find that digital ID has the greatest potential to provide value to both institutions and individuals simultaneously through high-frequency use cases in government and financial services. Both of these sectors are used by large numbers of individuals who stand to benefit significantly from relevant digital ID uses and by institutions that are well positioned to capture direct and indirect value as requesting parties.

Governments around the world have the potential to tap digital ID for uses such as e-government services and the provision of benefits to capture value while improving the experience of citizens. The use of e-government services could save both citizens and government workers valuable time and enable governments to become more responsive to citizen needs. In Estonia, the adoption of digital ID for government services has saved the equivalent of more than 820 years of working time annually for state employees and citizens—time they can spend on work, with their families, or engaging in leisure activities.[222] We estimate that e-government services could save citizens around the world an average of 20 hours per year, providing an incentive for them to adopt digital ID.[223] Governments around the world stand to reap significant cost benefits from streamlined service provision as well as broader value from the economic and social welfare benefits of increased citizen productivity. The use of digital ID for tracking and accountability in the provision of benefits can similarly improve the efficiency of critical citizen touchpoints with the government while driving significant cost savings.

As discussed in Chapter 3, a major use case of digital ID in the financial sector is satisfying KYC rules that require banks to verify the identity of individuals opening an account. This use demonstrates the financial sector's unique potential to generate significant immediate value for users and institutions as a tool to spur broad-based usage. Banks stand to benefit significantly from the use of e-KYC, which can significantly cut costs for authenticating customer identity. For example, the use of Aadhaar for e-KYC is estimated to have reduced the cost of consumer onboarding for financial institutions from approximately $5 to approximately $0.70.[224] At the same time, users would benefit from shortened account processing times and more streamlined processes, which allow them access to financial services without weeks of waiting and piles of documentation. Users may also benefit indirectly from passed-on cost savings from financial institutions in the form of lower fees or improved services that make financial services even easier to use.

Initial digital ID registration should be as easy as possible for both individuals and institutions

Digital ID registration should offer the appropriate level of authentication that can meet most users' needs and apply to the widest range of use cases from the outset. The process for individuals should be intuitive, straightforward, convenient, and fast. For example, India successfully onboarded nearly one billion people by rapidly creating about 50,000 enrollment points in locations 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.[225] New Zealand's Realme digital ID program was able to help spur high adoption by offering users a choice between two levels of authentication offered by different ID providers. Users of the program are able to choose the level of authentication that meets their needs, reducing unnecessary friction for individuals who do not need immediate access to high-security use cases.

75%

The adoption rate of BankID among adults in Sweden

Starting at enrollment, some consumers, particularly in emerging economies, may need education both to navigate the online world more broadly and to use their digital IDs in specific

[222] Heiko Vainsalu, "How do Estonians save annually 820 years of work without much effort?," e-Estonia, December 2017.
[223] See Chapter 3 for more detail.
[224] Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?,* Center for Global Development, October 2017.
[225] Ibid.

areas. Effective and inclusive education will be critical to make sure that users are aware of how they can use their ID properly and safely. This has been a concern in India, where the last State of Aadhaar report found that about 97 percent of Aadhaar users in the states of Andhra Pradesh, West Bengal, and Rajasthan were not aware of the biometric locking and unlocking security features of their IDs, and 93 percent were not aware of the authentication options available beyond fingerprint scans.[226]

Investing in improving user experience will be essential to achieve a critical mass of usage

User experience for both individuals and institutions must be positive. Users will only use products and services that meet their standards for customer experience, while providers will integrate digital ID only if it fits the customer journey they want to offer. At the same time, institutional users also demand sufficiently high experience, including in technical support, integratability, and value-added services.

Digital ID providers should prioritize continuous improvement of individual user experience and program accessibility. The sustained usage that is necessary to unlock long-term value will require digital ID providers to make using the ID intuitive and easy. For example, Sweden's BankID program, which has a roughly 75 percent adoption rate among adults, invested in an intuitive interface and encouraged long-term usage through a mobile application that removed the need for a security token or card reader as part of the login and authentication process. Accessibility was also a key factor in driving the successful adoption of Denmark's NemID program, which made a number of improvements, including integration of a computerized phone system, to its user journey to make the program accessible to partially sighted and elderly users.

Privacy is also a growing contributor to individual user experience, though detailed preferences vary by country. For example, in a Pew survey following the 2016 Cambridge Analytica data breach, 26 percent of respondents reported having deleted the Facebook app from their mobile device in the previous year.[227]

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 to encouraging long-term integration of digital ID with requesting party services. Companies may want to adopt digital IDs that are flexible enough to be used with their services and adaptable to their business model. This has been an important factor in Estonia's successful Mobile ID program, which has allowed banks and other companies to build bespoke services on top of the digital ID's basic authentication feature. This has led to innovative practices, such as Swedbank's integration of the Mobile ID with interactive voice recognition software to allow callers into its call center to "log in" to the call center before they are connected.[228]

At the same time, institutions need to be able to seamlessly integrate digital ID into their services at a minimal expense. Although the requirements for integration of digital ID into legacy systems and processes will vary across requesting parties, ID providers can reduce friction by developing clear standards that enable digital IDs to be interoperable across use cases and institutions and to reduce upfront development requirements and expenses for potential requesting parties. The EU took a step in this direction through the creation of eIDAS, which established clear standards for electronic signatures, qualified digital certificates, electronic seals, time stamps, and other authentication mechanisms. These standards have allowed EU-based requesting parties to recognize digital IDs from multiple sectors across all EU member states and have spurred the development of a commoditized market for authentication components.[229]

[226] Ronald Abraham et al., *State of Aadhaar report, 2017–18,* IDinsight, May 2018.
[227] Andrew Perrin, *Americans are changing their relationship with Facebook*, Pew Research Center, 2018.
[228] Alix Murphy, *Estonia's mobile ID: Driving today's e-services economy*, GSMA Mobile Identity, June 2013.
[229] *Identity in a digital world: A new chapter in the social contract*, World Economic Forum, September 2018.

An ID system that unlocks value while addressing risk requires appropriate design, infrastructure, and 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, with facilitated data sharing, 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. Additional considerations will include distributed storage of data in a way that avoids concentration of high-value information and integration of privacy by design principles into both system design and standards for all parties leveraging data tied to the digital ID. Such measures will be particularly critical to protecting the privacy and maintaining the trust of users in an advanced digital ID system with large-scale data sharing.

Digital ID system ownership structure will have a significant impact on the nature, capabilities, and risks of a program

Digital ID system ownership takes one of three forms: centralized, federated, or decentralized. 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.

In a centralized system, a single provider, typically a government agency, is integrated into all use cases, must generate adoption and use, and bears all costs. Examples include the national advanced digital ID programs in Estonia and India. Benefits include streamlined service delivery and high data aggregation capabilities, with tools like distributed storage helping avoid data consolidation. In a centralized system, the ID provider can have significant control over how authentication is performed and can ensure completely consistent ID services and a unified experience for users and requesting parties. This could be particularly important for governments or private ID providers that want to fully determine the level of due diligence carried out for identity proofing based on regulation and risk appetite, potentially increasing ID assurance.[230] Such a setup does, however, concentrate risk and liability, placing a significant burden of trust on the single provider.

In a federated system, ownership is shared among multiple stand-alone systems that share common standards. Examples include SecureKey Concierge in Canada, which is led by financial institutions, and GOV.UK Verify, a basic digital ID launched by the public sector and administered by private companies such as Barclays and Experian. A federated structure distributes cost, dilutes potential for abuse, and potentially offers users a wider range of institutions to which users entrust their ID.[231] However, a federated model also requires coordinated decision making and introduces complexity such as the need for legal agreements and for technology and data management standards that may disincentivize institutions from participating as ID providers. In an alternative form of federated ID system, governments play a pure standard-setting role and many separate ID providers choose to provide services. This more unconstrained approach allows the highest flexibility for the market to build IDs to meet individual uses while providing options for different levels of data sharing and allowing citizens the most control over ID use.

Decentralized models operate with no institutional owners and so hinge on distributed ledgers—for example, through blockchain and other technologies—to establish and manage identities, and on collective user demand. Such models remain in the early stages of development. Although it is not an ID system, Solid, launched by Tim Berners-Lee in September 2018, provides an example. As a project to decentralize the web by developing a

[230] Ibid.
[231] Ibid.

platform for linked data applications, Solid provides structural benefits that include strong user control over data, decentralized data storage, and the absence of any central authority that might manipulate or misuse the system. However, development of standards and technologies that provide the requisite security while enabling positive user experience may pose significant challenges, as would the lack of a central authority to address problems or grievances.

Digital ID infrastructure and processes 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 about how people register, for example whether through physical or remote digital channels. In the case of physical channels, ID providers will need to leverage a physical network for activities requiring physical touchpoints with users to more easily generate adoption and enable use cases.

In addition, the identification infrastructure will influence what credentials users can use, such as smart cards, innate biometrics, or passwords and personal identification numbers. Given the rapid changes to credential technology happening today, programs will have to evaluate the maturity, performance, scalability, ease of use, security, and affordability of the credential systems they implement.[232] Credentials can include what people have, such as smart physical cards; what people are, such as their innate biometrics; and what people know, such as passwords or PINs. The choice or combination of credentials used by an ID program will affect the costs of the program, which can range from $0.50 to $20 per user depending on the complexity of the necessary hardware or software and relevant authentication infrastructure (for example, biometric scanners).[233] Ease of use was a critical factor in the launch of the Estonian Mobile-ID service in 2007 that allowed users to authenticate themselves through high-security SIM cards in their phones instead of smart ID cards, which required specialized readers and were not compatible with mobile devices and tablets.[234] In Malawi, field tests of different biometric credentials found that both operators and participants clearly preferred iris scans to fingerprints. Over 80 percent of participants rated the iris scan "easy to use," compared with only 15 percent for fingerprint scans.[235] Credentials and their user interfaces will be critical to how ongoing user and requesting party interaction will occur and will require important decisions about software or applications used for authentication.

Additionally, careful process design can help reduce the risk of error at the human-digital interface and protect consumers, ensuring that their information remains safe at the point of enrollment. Examples include systemic rules that cross-check entered data against existing databases as well as measures that replace compromised credentials and provide alternative authentication methods where necessary.

Digital ID must 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. For decision rights, the organizational structure should be flexible enough to effectively handle dynamic problems, such as cyberbreaches, and should include individuals who are capable of making independent judgments about program risk without retaliation. This was achieved in Peru through the appointment of a nonpolitical independent oversight board for the government-run program, which has the authority to check excesses or inappropriate decisions made by the program administrators.[236]

[232] *Technology landscape for digital identification,* Identification for Development, World Bank, 2017.
[233] Thampy Koshy et al., *Understanding cost drivers of identification systems,* World Bank working paper number 132906, 2018.
[234] Alix Murphy, *Estonia's mobile ID: Driving today's e-services economy*, GSMA Mobile Identity, June 2013.
[235] Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?,* Center for Global Development, October 2017.
[236] Ibid.

Access rights establish who user data is available to and what they can do with it. Access rights will be a concern for both ID providers, which will be involved with all data flows, and requesting parties, which will be able to access the data related to their particular use case. Mechanisms to enforce access rights can include strict data-sharing and access policies as well as systemic measures that limit the amount of data that can be accessed by requesting parties or ID provider staff to what is absolutely necessary for their function and task. Policies to establish access rights are often closely related to a country's approach to privacy and must at a minimum conform to the regulatory environment.

4%

The amount of annual global revenue that companies violating the EU GDPR can be fined

Enforcement mechanisms establish responses to violations of policies or unethical behavior related to the digital ID. These can include fines or penalties as well as systematic audits of ID use to prevent misuse or system abuse. For example, in Estonia, health data are open, all access is logged, and unauthorized activity results in jail time. In Europe, companies violating the EU GDPR can be fined up to 4 percent of annual global revenue.

Finally, digital ID programs must be designed to be able to adapt to contingencies including technology failure or cyberattacks. This should include continuity planning and established processes for crisis response within the ID provider organization. Due to the importance of ID access to both individuals and institutions using the ID, it will be critical that organizations are prepared to handle both technical errors and external events such as storms or large-scale attacks.

Individuals, businesses, and governments can take action now as ID providers, requesting parties, users, and regulators

Governments, businesses, and civil society actors will have to think through several important questions as they shape the course of digital ID programs in their countries, sectors, and communities. These include how to address potential misuse of the digital ID system, approaches to safeguard user privacy and ensure control over personal data, how to optimize 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 are outlined in this section.

Governments, businesses, and civil society actors can play multiple roles in any digital ID system.

Governments can play the role of requesting party, for example by asking for information about or authentication of constituents; ID provider, for example as the direct provider of a state-run system; or manager of a federated multi-provider system. In addition, governments will play critical roles as regulators and policy makers. In those roles, they 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 the country-specific economics of digital ID and to explore public-private and consortium-led models of provision.

A business can be a requesting party, for example asking for information or authentication from a consumer or an employee; an ID provider, either as a stand-alone organization or as a member of a consortium; or both. Additionally, businesses can interact with digital ID regulation at the industry level by working on development of private-sector ID technology and implementation standards. Steps businesses can take include innovating processes that could leverage digital ID to boost efficiency and improve customer experience, working to facilitate development of global standards, and collaborating with governments to conduct bespoke cost-benefit analysis of digital identity and develop new digital ID programs.

Civil society institutions can influence the priorities of businesses and government in the development of policy or program design. Steps they can take to help ensure that individuals capture the value of digital ID while they retain control over personal data and are protected from misuse include petitioning politicians, regulators, and institutions to develop digital ID programs and the policies necessary to make them safe, accessible, and socially beneficial.

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 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.

The design, governance, and use of digital ID is a rapidly evolving area deserving additional research. Topics for further investigation include system design, incorporating features to protect user privacy and ensure fully informed consent both at sign-up and during ongoing usage; economic quantification of risks, encompassing design decisions and associated costs; relative benefits and downsides of different models for digital ID system governance and ownership—public or private as well as centralized, federated, or decentralized; and continued accumulation of an evidence base documenting benefits by use cases, including the link to specific design decisions and drivers of usage and adoption.

While solutions are not always clear, and more research will help clarify upsides and downsides, digital ID is undoubtedly an important opportunity for economies, governments, businesses, and individuals around the world.

Technical appendix

This appendix provides additional details on the key assumptions, calculations, methods, and data sources used in our research on digital identification. It comprises the following sections:

1. Key assumptions in our estimation of economic potential
2. Methodology for microanalysis based on use cases in focus countries
3. Methodology for macroeconomic analysis and extrapolation

1. Key assumptions in our estimation of economic potential

Our analysis of economic potential is not a forecast or predicted value for 2030, but rather a sizing of the potential given certain assumptions. Our estimates presume that the components of good ID are in place, including that it is established with individual consent, protects user privacy, and ensures control over personal data. These estimates are particularly sensitive to three sets of overarching assumptions: usage and adoption targets, expansion of digital infrastructure and ecosystems, and the value of time savings.

Our economic potential estimates are based on ambitious but achievable usage and assumption targets by 2030

We assume high levels of digital ID adoption and usage by 2030, based on current levels in the most successful existing digital ID programs. We consider both basic and advanced ID programs as well as country income levels in setting our assumptions. In this sense, our estimates are of potential value, not predictions or forecasts of the value that will be created by digital ID by 2030.

As we note in our report, achieving high rates of adoption in multiple use cases is neither automatic nor certain. The most successful cases, such as Denmark and India, indicate that adoption rates can surpass 70 percent in less than five years. In other cases, such as Nigeria and the United Kingdom, adoption has been slower, with rates so far under 10 percent.[237] In our analysis, we assume that a basic ID would be adopted by 20 percent of the population in mature economies and 70 percent of the population in emerging economies. For advanced ID, we assume 90 percent adoption across both emerging and mature economies.[238]

We assume countries can develop the digital infrastructure and ecosystem necessary to support digital ID programs

We assume in our estimates that countries can develop the digital infrastructure and ecosystems required to enable digital ID and gain the value it helps unlock. We believe that digital ID is a foundational set of technologies, pivotal to unlocking the value we quantify but not sufficient on its own—each area of use will require digital infrastructure, applications, and interfaces built by institutions that interact with digital ID users. These include sufficient levels of telecom and electrical coverage, e-government services, digital financial services, digital talent matching and contracting platforms, digital health records, and digital asset registries. Our estimates of potential value from digital ID include the full value that comes from the use cases it can enable. We do not attempt to isolate the incremental value from digital ID alone, since we believe that in most cases this is not possible. For example, we estimate the benefit

[237] *The next generation of national electronic identity and signing in Denmark,* Denmark Ministry of Finance Agency for Digitisation, April 2016; "AADHAAR Dashboard," Unique Identification Authority of India; "About the e-ID Card," Nigeria National Identity Management Commission; "GOV.UK Verify Dashboard," Gov.UK, as of 2/1/2019.

[238] We assume advanced digital ID adoption of 91 percent in India, to account for the rollout and widespread adoption of the Aadhaar digital ID.

from expanded credit to borrowers that digital ID can enable, on the understanding that applications for digitally enabled credit scoring and approval will also be a part of that value.

We recognize that economic value may not necessarily materialize into GDP
To quantify and analyze the economic benefits of digital ID, we used GDP as a comparable base to give a sense of the order of magnitude of the opportunity and compare across use cases and types of value. However, even in achieving the economic potential, a share of the benefits sized is unlikely to materialize into direct increases of GDP due to the dynamics of consumer surplus and fraud reduction.

A portion of the economic benefits from time savings and productivity improvements that we sized may lead to changes in consumer surplus without necessarily affecting total output. To quantify the economic value of individuals' time, we model hours saved as increased labor hours. We note that while time may be valued by individuals at or above the potential earnings in labor markets, not all time saved is likely to materialize as additional labor hours. Furthermore, some of the productivity benefits captured by institutions could translate into competitive dynamics that change market share composition and consumer surplus without necessarily increasing overall output at the country level.

Similarly, the benefits sized related to reductions in payroll, tax, and benefits fraud may not fully materialize into GDP, depending on expenditure patterns for fraudulent income. A portion of reduced fraud could represent transfer of income from the informal sector to the formal sectors and while this would likely lead to a net productivity increase, not all value would generate increases in total output.

2. Methodology for microanalysis based on use cases in focus countries

We begin with detailed microlevel analysis, looking at nearly 100 ways of using digital ID in each of our seven focus countries. We estimate the microlevel impact for each use case in 2030 as a product of three factors: the addressable share of the economy that would be impacted, the incremental share of interactions for which individuals may adopt and use digital ID, and the potential for value creation from each such interaction. We do not perform a comprehensive cost-benefit analysis of digital ID but focus on sizing incremental value possible from levers such as time and cost savings and greater supply of labor and capital resulting from digital ID–based applications.

Our focus economies represent 48 percent of the world's population and 49 percent of global GDP
A country-by-country approach is essential to understand the economic potential of digital ID because each country or situation is unique, with different drivers of potential value. In selecting focus countries for this research effort, we sought to optimize for geographic and economic diversity while covering a substantial share of global population and economic production. Ultimately, we selected Brazil, China, Ethiopia, India, Nigeria, the United Kingdom, and the United States, which cover roughly 48 percent of global population and 49 percent of global GDP today.

We sized the economic potential of digital ID after identifying nearly 100 ways digital ID could be used
We identify nearly 100 ways of using digital identification, feasible with today's technological capabilities, through a review of existing interactions in which individuals use identification across six core roles: as consumers, workers, microenterprises, taxpayers and beneficiaries, civically engaged individuals, and asset owners. Additionally, we include use cases already deployed by digital identification systems across the world. For each use case, we determine the primary economic drivers through which economic value could be enabled and the level of digital identification that would be needed to unlock value.

The economic drivers through which digital ID could create economic value were: increased investment and lending from financial inclusion, increased labor market efficiency and productivity, time and cost savings, reduced fraud, increased tax revenue, increased productivity of land and agriculture, and increased sales of goods and services.

Use cases were classified as those that can be enabled by basic digital authentication and those requiring more advanced digital ID with facilitated data sharing, based on the underlying role of digital ID in creating value. For example, time savings associated with digital voting may require only high-assurance authentication, and additional data sharing in these instances could have a negative impact on privacy. However, digital talent matching and streamlined work authorization with instant background checks may require additional data sharing to confirm education history, work history, and any criminal record. It is important to note that use cases requiring data sharing do not explicitly require the digital ID itself to store or share data; this functionality can exist separately in digital systems built on top of authentication-only digital ID systems.

Impact of use cases across our focus countries

In our analysis, we performed a bottoms-up economic sizing for nearly 50 of the use cases that we identified, selected based on initial estimates of the order of magnitude of economic impact. We chose to size use cases with the greatest estimated potential for economic value generation and largest potential for impact on the population and economy in impacted countries (Exhibit A1). For this reason, we did not perform economic sizing on use cases associated with interactions by civically engaged individuals (e.g., verification of online donations, school enrollment), and instead described relevant use cases qualitatively throughout the report (see Chapter 3).

Increased lending and investment from financial inclusion

To estimate the impact of new physical capital from access to financial services, we leverage research conducted in 2016 by the McKinsey Global Institute in *Digital finance for all: Powering inclusive growth in emerging economies* and refresh the component of the analysis pertaining to increased investment in physical capital due to increased access to bank accounts. Based on the ability of digital ID to address core barriers to bank account access—including not having the required identification documentation, services being too expensive, and branches being too far away—we see digital ID as a key enabler to digital financial services and assume this could unlock developed-world levels of financial inclusion within emerging economies. Noting that bank account penetration is in many instances a leading indicator for deposits and subsequent lending, we calculate growth in investments in physical capital since 2016 and subtract this from initial estimates to determine the remaining potential.

The underlying calculation considers three components: the additional deposits from individuals currently excluded from access to bank accounts, closed system slack generating new loans, and higher return loans to micro, small, and medium-size enterprises.

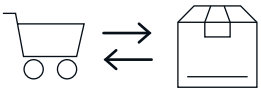
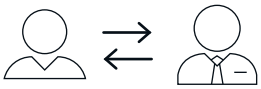
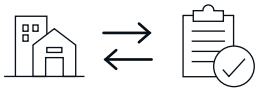
— **Individual deposits.** We considered existing retail deposits in each of our focus countries and used World Bank income data to estimate the average retail deposits per household in each wealth bracket.[239] Assuming that households will add deposits to the financial system at the same per household deposit levels currently observed in each wealth bracket, the total additional deposits that newly included households will add to banks' deposit bases was projected.

— **The closed system slack and new loans.** Financial institutions in many emerging economies do not lend as much as they could, and their loan-to-deposit ratios are below the regulatory limit. In countries where the loan-to-deposit ratio is lower than the worldwide average, we assumed that more loans can be made. Digital identification can enable digital finance applications that unlock new lending due to a lower cost of issuing loans and collecting payments for individuals and microenterprises. More important, digital ID–enabled digital finance expands the potential customer base by creating digital data records on household and microenterprise income streams. This enables new credit scoring methods to assess the creditworthiness of potential borrowers. To avoid projections of excessive lending that could stress system stability, we constrain the total increase in loans outstanding to stay below certain thresholds in four areas: loan-to-GDP

[239] We assumed there are two adults per household for model simplicity.

Exhibit A1

Top 10 use cases across all focus countries.

Rank	Overall top use cases	Interaction type	
1	Increased lending and investment from financial inclusion		Consumers Commercial providers of goods and services
2	Time savings from e-government services		Taxpayers and beneficiaries Public providers of goods and services
3	Increased business productivity from improved applications of data analytics		Consumers Commercial providers of goods and services
4	Seamless and secure sharing of healthcare records		Taxpayers and beneficiaries Public providers of goods and services
5	Reduced private-sector payroll fraud		Workers Employers
6	Improved agricultural land productivity fostered by increased formalization		Asset owners Asset-based service providers and buyers
7	Reduced business supply chain and operational costs from analytics		Consumers Commercial providers of goods and services
8	Reduced government benefits leakage and fraud		Taxpayers and beneficiaries Public providers of goods and services
9	Entry of some inactive workers into labor force due to digital contracting programs		Microenterprises Consumers and broad range of institutions
10	Inclusion of individuals in tax base		Taxpayers and beneficiaries Public providers of goods and services

Source: McKinsey Global Institute analysis

ratio, loan-to-bank-reserves ratio, total percentage change in loans, and percentage change in household loans. We assumed that loans would increase from new deposits and system slack until any of these constraints was reached.

— **Higher-return loans.** The returns to lending rise as the availability of borrowers increases. We calculated current returns as the weighted average return on invested capital of major corporations within each focus country, because the majority of lending today is to large corporations. We assumed new loans will be to MSMEs, whose return on invested capital is larger than that of corporations due to both higher lending rates and higher returns.

Increased labor market efficiency and productivity

To estimate the impact of digital ID on increasing participation in and efficiency of labor markets, we consider a multitude of use cases across access to formal employment, improved talent matching and contracting, and reduced payroll fraud from ghost workers. For the digital talent matching use cases, we leverage 2015 research by the McKinsey Global Institute in the report *A labor market that works: Connecting talent with opportunity in the digital age.* We assumed a portion of the value estimated in that report could be unlocked specifically by digital ID programs and refreshed relevant parts of the analysis.

We model the benefits of digital ID for the labor market by evaluating how digital talent matching programs could affect workers and how digital contracting platforms could impact microenterprises. Although forms of digital talent matching and contracting can be developed without digital ID, as demonstrated by existing platforms including Freelancer.com and LinkedIn, high-assurance authentication of credentials and identity can greatly increase the feasibility and applications of large-scale programs. The underlying calculations are based on the following factors:

— **Improved participation.** As we discuss in Chapter 2, many working-age people in countries around the world are not working or are economically underutilized. They include individuals who are unemployed, those who are working part time but would prefer to work full time, newly retired people, stay-at-home parents, discouraged workers, and others who are out of the labor force for other reasons. High-assurance digital talent and contracting platforms will increase the likelihood that those who are not participating in the labor force will find opportunities of interest to them, whether permanent full-time jobs, part-time jobs, or freelance work. This may mobilize some fraction of stay-at-home mothers; youth who are not in employment, education, or training; retired people; and working-age individuals who have been discouraged or are inactive for other reasons. We model this impact as increased labor force participation and hours worked. Our assumptions on the increased participation of inactive working-age adults and increased hours for part-time workers are informed by the results of surveys including the MGI European Aspirations Conjoint Survey (2014).

— **Faster matches.** High-assurance online talent and contracting platforms reduce the amount of time it takes for those who are unemployed (whether they are between jobs, are new entrants to the workforce, or have been inactive for a long period) to obtain new positions. This will reduce the number of unemployed people at any given time. We model the impact as a reduction in frictional unemployment. Our assumptions are informed by national statistics and data from organizations including the International Labour Organization and the OECD.

— **New matches.** High-assurance online talent and contracting platforms can synthesize detailed matching attributes to enable broader searches that help companies and workers find one another. They enable new matches that would not have been made otherwise. This may be due to the enhanced transparency of job openings and to the ability of the unemployed to look for work opportunities across geographies. We model these impacts as a reduction in the overall unemployment rate.

— **Better matches.** High-assurance online talent and contracting platforms make it possible to match individuals who are already employed with better jobs or more effective teams. They do this by providing more transparency into the skills and traits of individual workers as well as the requirements of specific jobs and tasks. When workers are matched to jobs that more appropriately fit their skills, they will be more productive (that is, those individuals can produce more output). We calculate the potential to raise productivity through better matches for the subset of the population in each country that changes jobs each year by taking advantage of online talent platforms.

— **Reduced informal employment.** Around the world, many people are engaged in informal employment, which typically involves low and variable wages and a lack of legal and social protections. Informal enterprises lack the economies of scale, technology tools, and management expertise to grow and become more productive. Previous MGI research has found that around the world, informal enterprises operate at just half the average productivity level of formal companies in the same sectors. A review of the literature on productivity differentials from formalization finds ranges that vary widely across countries and sectors, such as 15 percent among Brazilian retailers and 84 percent among legal firms in Mexico. However, since the variance is wider in emerging economies than in mature economies, we assume a 10 percent differential for mature economies and a 30 percent differential for emerging economies in our focus set.

Time and cost savings

We estimate benefits generated through significant reductions in direct costs and improved efficiency for both private and public institutions through sizing a variety of use cases, including reduced operational and supply chain costs and seamless sharing of medical or financial information.

— **Reduced operational and supply chain costs.** We estimate that certain industries (e.g., retail) can capture operational and supply chain cost savings from controlled and regulated application of digital ID in the workplace. Digital ID could be an important facilitator of those productivity improvements, by allowing retailers to accurately identify consumers, employees, and suppliers and perform advanced analytics on high-quality associated data to streamline and improve processes. We leverage research conducted in 2011 by the McKinsey Global Institute for the report *Big data: The next frontier for innovation, competition, and productivity* to estimate the potential impact on retailers. We assume that digital ID could enable at least half of the projected productivity growth in retail from applications of analytics to high-quality data to reduce operational and supply cost, and consequently estimate a cost reduction of up to 5 percent for businesses.

— **Seamless sharing of medical information.** We estimate that digital ID could generate a reduction of up to 10 percent in hospital spend per patient in our focus countries. This assumption was based on academic research examining spend on patients with available electronic health records.[240]

Reduced fraud

We estimate the impact of digital ID on fraud reduction across a wide variety of use cases in the public and private sectors. For example, we sized the use of digital ID for payroll fraud reduction in the public and private sectors and reduced government benefits leakage.

— **Reduced payroll fraud.** We estimate that digital ID can significantly reduce payroll fraud by removing fraudulent employees from government and private-sector payrolls. Our assumptions on existing rates of payroll fraud across our focus countries were linearly scaled based on the Transparency International Corruption Perceptions Index from studies that found rates of approximately 1 percent in the United Kingdom and approximately 20 percent in Nigeria.[241] We leveraged previous MGI research and expert interviews to estimate that digital ID could prevent 50 to 75 percent of addressable payroll fraud.

— **Reduced government benefits leakage.** We estimate that digital ID could enable governments to reduce benefits leakage by leveraging high-assurance identification to identify and remove ghost recipients. For the mature economies in our focus set, we assume that 1 percent of government benefits are affected by fraud, informed by findings on benefits fraud from the United Kingdom's Department for Work and Pensions, and estimate that up to 80 percent of fraudulent benefits transfers can be eliminated with advanced digital ID.[242] In the emerging economies in our focus set, we assume that use of advanced digital ID can reduce benefits expenditure by up to 21 percent. This assumption is based on the estimated leakage reductions in India for programs that have integrated Aadhaar into disbursement.[243]

Increased tax revenue

We estimate the increased tax revenue unlocked by digital ID through use cases that leverage high-assurance authentication and data sharing to increase the tax base. Digital ID can help increase the tax base through income formalization and by reducing the tax collection gap.[244]

[240] Abby Swanson Kazley et al., "Association of electronic health records with cost savings in a national sample," *American Journal of Managed Care*, June 2014.
[241] *Annual fraud indicator: Identifying the cost of fraud to the UK economy*, UK Fraud Costs Measurement Committee, 2017; Adongoi Toakodi and Victor Eyo Assi, "Corruption in the civil service: A study of payroll fraud in selected ministries, departments and agencies (MDAS) in Bayelsa State, Nigeria," *Research on Humanities and Social Sciences,* 2016, Volume 6, Number 3.
[242] *Fraud and error in the benefit system: Financial year 2016 to 2017 estimates*, UK Department for Work and Pensions, November 30, 2017; updated July 20, 2018.
[243] Ronald Abraham et al., *State of Aadhaar report, 2017–18,* IDinsight, May 2018.
[244] *Public sector savings and revenue from identification systems: Opportunities and constraints*, World Bank, 2018.

We estimate that digital ID could create an incremental per-unit benefit for tax collection ranging from 1.3 percent in India to 19 percent in Nigeria.

Increased productivity of land and agriculture

Digital ID could enable digital land titles that would help farmers to sell or lease land and apply for new lines of credit that could increase investment and output on currently unregistered land. ID-enabled digital land titling could make formal ownership of assets accessible to a wider range of farmers in emerging countries who currently own land without evidence or registered legal claims. We estimate that this could lead to an increase in land productivity ranging from 10 to 15 percent for currently unregistered land in our focus countries.

Increased sales of goods and services

To measure the benefits from the use of digital ID to enable improved application of data analytics and increase productivity, we leverage research conducted in 2011 by the McKinsey Global Institute and described in the report *Big data: The next frontier for innovation, competition, and productivity* as well as research conducted in 2016 for *The age of analytics: Competing in a data-driven world.* For each of our focus countries, we estimated the addressable share of the big data applications quantified in those reports in the retail, healthcare, education, finance, and manufacturing sectors that could be enabled by advanced digital ID. We weighted the productivity increases that digital ID could enable in each sector by the relative size of each sector in each of our focus countries to calculate the overall productivity growth by 2030.

3. Methodology for macroeconomic analysis and extrapolation

To understand how the use of digital ID will affect the overall economies of our seven focus countries and compare across various sources of value, we use McKinsey's proprietary general equilibrium macroeconomic model. We then extrapolate from the focus countries based on a composite of metrics for the share of the economy addressable by digital ID and the potential for value creation in a global set of countries.

McKinsey's Global Growth Model

The Global Growth Model (GGM) is a supply-side macroeconomic model that covers more than 100 countries, with data from 1960 through 2016. The structure of the model is anchored in the academic literature on economic growth models. In addition to the common growth drivers of capital and labor, our model incorporates unique features such as education, energy, R&D, openness to trade, and financial system depth as distinct drivers of growth. The model also incorporates the core features of a comprehensive macroeconomic model, including labor markets, monetary and fiscal policy expectations, and international trade and investment flows.

The model is estimated using dynamic panel "error correction" equations using simultaneous equation techniques to capture interactions among concurrent variables. Validity of the equations is further tested using instrumental variable techniques to control for biased correlations between simultaneously interacting independent variables.

The data underpinning the model are obtained from national governments, authoritative international sources, and data sets such as the Barro-Lee education database that are devised by researchers. These data sets are carefully merged to develop extended time series; where gaps remain, we impute missing data using standard econometric techniques.

The GGM uses an augmented Cobb-Douglas production function with fixed capital, energy consumption, and human capital as distinct factors of production. The production function incorporates a nested constant elasticity of substitution function to capture the imperfect substitution between capital and energy. The coefficients on the Cobb-Douglas are estimated using the dynamic error correction approach noted above.

The human capital index captures both labor supply and the quality of labor in a country. It is defined as the product of employment, average years of education, and an index of work. The fixed capital estimates are derived using a perpetual inventory method and the Harberger approach to calculating the initial stock.

Modeling macroeconomic value

Values associated with each of the economic drivers used in the bottoms-up use case analysis were aggregated at the country level and then used as inputs to the Global Growth Model to estimate macroeconomic potential. Through the GGM, we use GDP as a proxy for economic value in order to aggregate and compare across use cases, economic drivers, and economies, which would otherwise be hard to interpret across various units and contexts.

— Increased investment in physical capital from access to financial services is modeled as a direct increase in fixed capital.

— Participation in and efficiency of labor markets includes two components. First, additional participation in the labor markets is modeled as simultaneous increase in human capital or labor hours available, and then a reduction in overall productivity is applied based on the source of marginal labor with assumptions for relative productivity to the average worker. Second, we model productivity increases of the overall workforce driven by talent matching and formalization of labor markets.

— Productivity of land and agriculture is modeled as an increase in agricultural output.

— Time and cost savings are modeled in multiple components. First, time and cost savings for institutions are modeled using labor as a proxy for the efficiency gains, first measuring an increase in productivity to achieve the same outputs with reduced labor supply by the equivalent savings, then reintroducing the labor at the new productivity level. Time savings for individuals are modeled as increased labor hours.

— Reduced fraud and leakage are modeled separately for the public sector and private sector. The savings from reduced fraud and leakage for the public sector are closely tied to disbursements and are thus modeled as capital reintroduced as government investment. The savings from reduced fraud and leakage in the private sector are modeled as capital reintroduced as increased business investment.

— Increased sale of goods and services is modeled as increased efficiency and total productivity.

— Formalization and expansion of the tax base results in increased tax revenue modeled as increased government investment in infrastructure.

Feedback loops

Feedback loops include both positive and negative. Positive feedback loops include:

— Physical capital investment. An increase in physical capital investment increases overall capital stock and the productive capacity of the economy. It also raises expected future growth, increasing the value of equities and the availability of additional financing. This, in turn, results in further investment, innovation, and total factor productivity growth, thereby boosting overall GDP growth.

— Employment. Our model captures a dynamic in which a decline in the unemployment rate not only increases overall employment but also encourages individuals to reenter the workforce, raising the labor force participation rate. The combined increase in employment from the ability to absorb new technology is either through R&D or through imports of technology. This also increases total factor productivity and GDP growth.

— Public expenditure on benefits. An increase in public spending on benefits has a multiplicative impact on overall growth. As the level of human capital rises, the workforce becomes more productive, increasing total factor productivity and therefore driving further growth. In parallel, the rise in benefits translates into higher incomes and consumption, which translates to higher government revenue of which a portion is invested in benefits such as education and healthcare, further augmenting human capital.

Negative feedback loops include:

A rise in fixed capital investment boosts growth but also increases demand and inflation. Higher inflation can trigger higher interest rates, which ultimately dampen investment by raising investment cost and lowering the returns on that investment.

Classification of value across roles and individuals versus institutions

We classified use cases across six roles, informed by the types of interaction that would typically generate value through digital ID. The six roles considered in our report are interactions by:

- Consumers with commercial providers of goods and services
- Workers with employers
- Microenterprises with consumers and a broad range of institutions
- Taxpayers and beneficiaries with public providers of goods and services
- Civically minded individuals with governments and other individuals
- Asset owners with asset-based service providers and buyers
- We did not calculate economic value associated with use cases enabled by interactions generated by civically minded individuals. In cases where use cases could be generated by multiple types of interactions, we assigned value to the role(s) where the majority of interactions were likely to take place. For example, uses related to digital talent matching and contracting were calculated separately for worker and microenterprise interactions due to the different dynamics and populations affected by the talent matching and contracting platforms, respectively.
- We considered benefits generated through increased lending and investment resulting from financial inclusion as part of the consumer interaction type, due to the role of new depositors as consumers of financial products.
- In the case of benefits related to cost savings from seamless and secure sharing of medical information, we assigned generated value to taxpayer and beneficiary interactions for all of our focus countries except for the United States. This decision was driven by the large role played by public institutions in the healthcare market globally, making them generally the primary direct beneficiary of digital ID–related health savings. For 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. Although we did not include it in our benefits allocation, we also acknowledge the role played by private healthcare players in countries such as Brazil, which could also benefit from healthcare data-sharing savings.

In our breakdown of value across individuals and institutions, we categorized the macroeconomic benefits calculated through the GGM analysis into nine drivers and assigned their components of value to the parties that would primarily directly benefit. For value accruing primarily to institutions, including businesses and governments, we considered the following benefit drivers:

- Cost savings captured by businesses and government
- Reduced business and government fraud and expenditure leakage
- Increased government tax revenue
- Increased productivity from new and improved goods and service provision

Although these benefits primarily accrue to institutions, in many cases individuals could benefit from redistribution of these benefits through competitive dynamics or policies that lead to price reductions, improved service delivery, or increased wages or benefits.

For value accruing primarily to individuals, we considered the following benefit drivers:

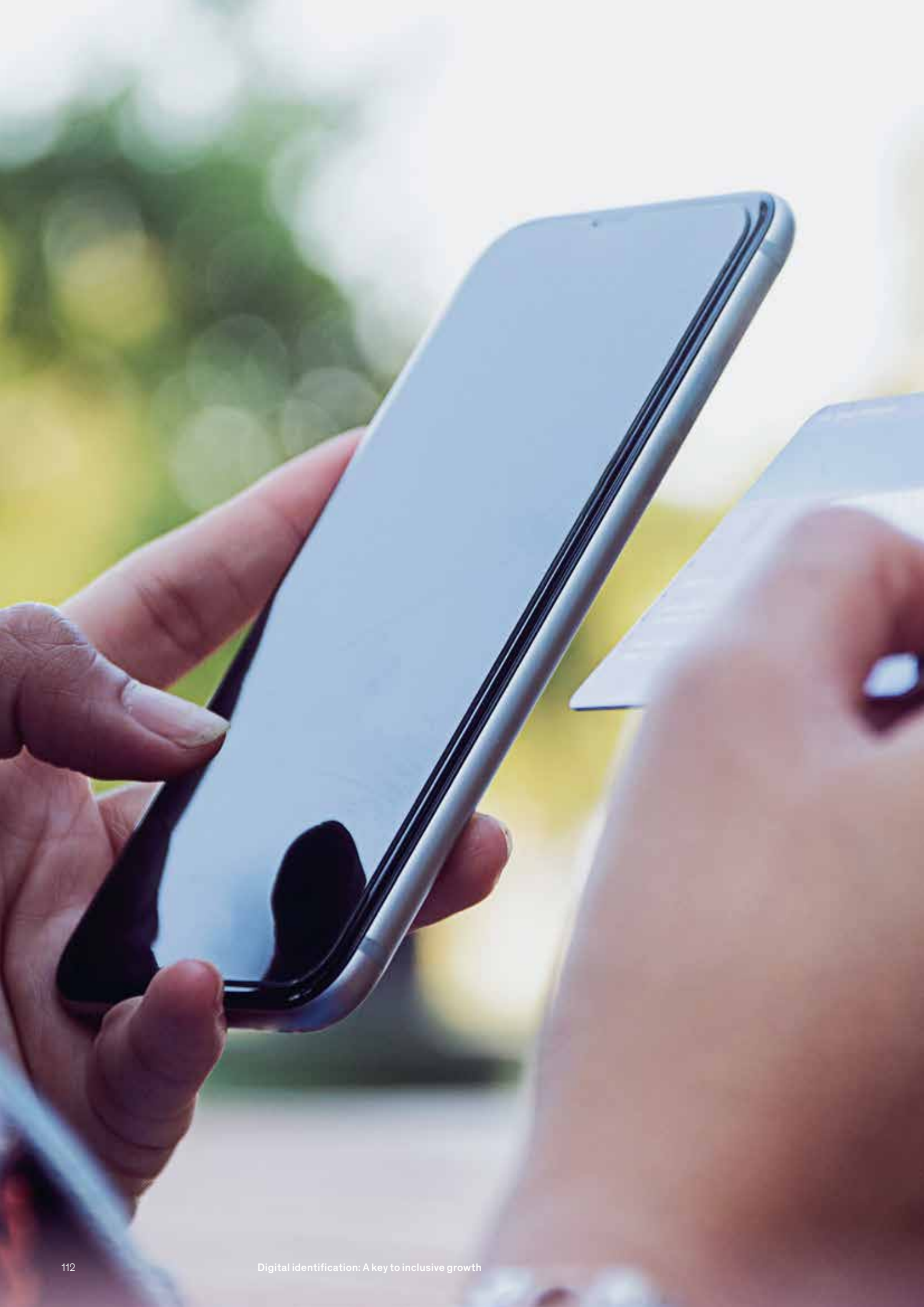
- Increases in lending and investment resulting from additional savings and credit
- Improved agricultural productivity from formalized landownership
- Increased labor productivity

Although these benefits primarily accrue to individuals, institutional actors such as governments and businesses could also capture value through mechanisms such as improved labor force productivity and improved access to credit from an increased deposit base.

Methodology for extrapolation

To understand the opportunity from digital ID on a global scale, we extrapolated the results from our focus countries to a broader set of 23 countries covering 63 percent of the global population and 78 percent of global GDP. This extrapolation was not for the purpose of making country-specific estimations but rather for sizing the overall range.

We analyzed the elements of addressable share of the economy and potential for value creation that drove variation in benefits across our focus countries to identify the subset of metrics that are most descriptive of value potential. We normalized these underlying factors for addressable share of the economy and potential for improvement across a set of 217 countries and created a composite indicator for potential economic value by multiplying the relevant normalized addressable share and potential for improvement factors. We then performed an exponential regression to extrapolate the potential economic impact under high-adoption scenarios from focus countries to the additional countries in our set.



Bibliography

A

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

Accenture, *The future of identity in banking,* 2013.

Alliance for Affordable Internet, *The 2015–16 affordability report*, 2016.

Apland, Kara et al., *Birth registration and children's rights: A complex story,* Plan International Headquarters, 2014.

Asia Blog, "How the Asian financial crisis led to China's massive graduate unemployment," blog entry by Eric Fish, June 8, 2017, asiasociety.org/blog/asia/how-asian-financial-crisis-led-china%E2%80%99s-massive-graduate-unemployment.

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

B

The Better Identity Coalition, *Better identity in America: A blueprint for policymakers*, July 2018.

Bill & Melinda Gates Foundation, *The Level One Project guide: Designing a new system for financial inclusion*, April 2015.

Birch, Dave, and Emma Lindley, *Self-sovereign identity and shared ledger technology*, Omidyar Network, September 2017.

Boudet, Julien, Brian Gregg, Jason Heller, and Caroline Tufft, "The heartbeat of modern marketing: Data activation and personalization," McKinsey & Company, March 2017, McKinsey.com.

Brito, Steve, Ana Corbacho, and Rene Osorio, "Does birth under-registration reduce childhood immunization? Evidence from the Dominican Republic," *Health Economics Review,* 2017, Volume 7, Number 14.

Brune, Lasse et al., *Facilitating savings for agriculture: Field experimental evidence from Malawi,* NBER working paper number 20946, February 2015.

Busso, Matías, María Victoria Fazio, and Santiago Levy, *(In)formal and (Un)productive: The productivity costs of excessive informality in Mexico*, Inter-American Development Bank, August 2012.

C

Caribou Digital, *Identities: New practices in a connected age,* Farnham, Surrey, UK: Caribou Digital Publishing, 2017.

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

Centre for Public Impact, Bolsa Familia in Brazil.

Cisco, *By the numbers: Projecting the future of digital transformation (2017–2022).*

Cisco, "Jio propels India to top in mobile broadband consumption by automating world's first all-IP network with Cisco," April 2018.

Cook, Sam, "Identity theft stats & facts: 2017–2019," Comparitech, August 25, 2018.

Cooper, Tim, and Ryan LaSalle, *Guarding and growing personal data value,* Accenture, 2016.

Crowd Research Partners, *Threat monitoring, detection and response report*, 2017.

D

Dahan, Mariana, and Lucia C. Hanmer, *The identification for development (ID4D) agenda: Its potential for empowering women and girls—background paper,* World Bank working paper number 99543, September 17, 2015.

de Chickera, Amal, "Statelessness and identity in the Rohingya refugee crisis," Humanitarian Practice Network, October 2018.

Denmark Ministry of Finance Agency for Digitisation, *The next generation of national electronic identity and signing in Denmark*, April 2016.

Doepke, Matthias, and Michele Tertilt, *Does female empowerment promote economic development?* Centre for Economic Policy Research discussion paper number 8441, June 2011.

Dunning, Casey, Alan Gelb, and Sneha Raghavan, *Birth registration, legal identity, and the post-2015 agenda,* Center for Global Development, September 2014.

E

European Parliamentary Technology Assessment, *ICT and privacy in Europe: Experiences from technology assessment of ICT and privacy in seven different European countries,* October 2006.

F

Feder, Gershon, *The intricacies of land markets: Why the World Bank succeeds in economic reform through land registration and tenure security,* Queensland Government, Natural Resources and Mines, 2002.

Financial Action Task Force, *FATF 40 recommendations,* October 2003.

Financial Action Task Force, *FATF guidance: Anti-money laundering and terrorist financing measures and financial inclusion*, November 2017.

FLACSO-Guatemala, *Barriers to electoral participation in Guatemala: Diagnostic of 4 municipalities*, 2007.

The Fraudscape, "Fraudulent conduct decreases overall—but worrying rises in some areas," 2018.

G

Gee, Jim, *Annual fraud indicator: Identifying the cost of fraud to the UK economy*, UK Fraud Costs Measurement Committee, 2017.

Gelb, Alan, and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?*, Center for Global Development, October 2017.

Gemalto, *Overview of the German identity card project and lessons learned (2017 update).*

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

Gov.UK, "GOV.UK Verify Dashboard."

Government Digital Service, "Government as a data model: What I learned in Estonia," blog entry by Peter Herlihy, October 31, 2013, gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/.

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

GSMA, "Digital identity demonstrates its crucial role in transforming healthcare," blog entry, March 1, 2018, gsma.com/identity/digital-identity-demonstrates-crucial-role-transforming-healthcare.

H

Hanmer, Lucia, and Marina Elefante, *The role of identification in ending child marriage*, World Bank, July 2016.

Hughes, Barry B. et al., *Cyber benefits and risks: Quantitatively understanding and forecasting the balance,* Pardee Center for International Futures, 2015.

I

Inside Out Security, "The world in data breaches," blog entry by Rob Sobers, July 16, 2018, varonis.com/blog/the-world-in-data-breaches.

International Labour Organization, *Women and men in the informal economy: A statistical picture*, 2018.

International Monetary Fund, *Digital revolutions in public finance,* November 2017.

International Telecommunication Union, *Review of national identity programs*, May 2016.

J

Javelin Strategy & Research, "Identity fraud hits all time high with 16.7 million U.S. victims in 2017, according to new Javelin Strategy & Research study," February 6, 2018.

K

Kazley, Abby Swanson et al., "Association of electronic health records with cost savings in a national sample," *American Journal of Managed Care*, June 2014.

Koshy, Thampy et al., *Understanding cost drivers of identification systems,* World Bank working paper number 132906, 2018.

L

Le Bras, Tom, "Online overload—it's worse than you thought," Dashlane, July 21, 2015.

M

Malik, Tariq, "Technology in the service of development: The NADRA story," Center for Global Development, November 7, 2014.

McKinsey Global Institute, *The age of analytics: Competing in a data-driven world,* December 2016.

McKinsey Global Institute, *Big data: The next frontier for innovation, competition, and productivity,* May 2011.

McKinsey Global Institute, *Digital finance for all: Powering inclusive growth in emerging economies*, September 2016.

McKinsey Global Institute, *A labor market that works: Connecting talent with opportunity in the digital age*, June 2015.

McKinsey Global Institute, *The power of parity: How advancing women's equality can add $12 trillion to global growth,* September 2015.

McKinsey Global Institute, *Preparing Brazil for the future of work: Jobs, technology, and skills*, March 2018.

McQuinn, Alan, and Daniel Castro, *Why stronger privacy regulations do not spur increased internet use*, Information Technology & Innovation Foundation, July 2018.

McWaters, R. Jesse, *A blueprint for digital identity: The role of financial institutions in building digital identity*, World Economic Forum, August 2016.

Medina, Leandro, and Friedrich Schneider, *Shadow economies around the world: What did we learn over the last 20 years?*, IMF working paper number 18/17, January 2018.

Micah, Leyira Christian, and Temple Moses, "IPPIS and the ghost workers' syndrome in Nigeria's public sector," *Scholars Journal of Economics, Business and Management*, August 2018, Volume 5, Issue 8.

Ministry of Electronics and Information Technology, Government of India, *India's trillion-dollar digital opportunity*, 2019.

Morey, Timothy, Theodore "Theo" Forbath, and Allison Schoop, "Customer data: Designing for transparency and trust," *Harvard Business Review*, May 2015.

Murphy, Alix, *Estonia's mobile ID: Driving today's e-services economy*, GSMA Mobile Identity, June 2013.

N

National Democratic Institute, "Burkina Faso campaign brings 16,000 women closer to voter registration," October 2012.

Nigeria National Identity Management Commission, "About the e-ID Card."

Nyster, Carly et al., *Digital identity: Issue analysis*, Omidyar Network, 2016.

O

Olanrele, Olusegun Olaopin, 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.

Omidyar Network, "Trust and privacy," October 2, 2017.

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.

P

Perrin, Andrew, *Americans are changing their relationship with Facebook*, Pew Research Center, September 5, 2018.

Ponemon Institute, *2018 cost of data breach study: Global overview,* June 2018.

PPC ID Card Solutions, "MyKad: Is Malaysia ahead of the game?," October 8, 2015.

R

Reuben, William, and Flávia Carbonari, *Identification as a national priority: The unique case of Peru,* Center for Global Development working paper number 454, May 2017.

Richardson, Bryan, and Derek Waldron, "Fighting back against synthetic identity fraud," McKinsey & Company, January 2019, McKinsey.com.

Rose, John, Olaf Rehse, and Björn Röber, *The value of our digital identity,* Boston Consulting Group, November 2012.

Rubinstein, Flavio, and Gustavo G. Vettori, "Closing the Brazilian tax gap: Public shaming, transparency and mandatory disclosure as means of dealing with tax delinquencies, tax evasion and tax planning," *Derivatives & Financial Instruments*, 2016, Volume 18, Number 1.

S

Salamone, Shawn, "Student, faculty researchers expose secret misuse of personal data by mobile apps," Baldwin Wallace University, September 21, 2017.

Seagate, *Data age 2025: The evolution of data to life-critical,* March 2017.

Sumner, Cate, *Indonesia's missing millions: Erasing discrimination in birth certification in Indonesia*, Center for Global Development, June 2015.

T

Telecom Regulatory Authority of India, *Indian telecom services performance indicators*, June 2016 and September 2018.

Thakkar, Danny, *Biometric devices: Cost, types, and comparative analysis,* Bayometric.

Theodorou, Yiannis, and Erdoo Yongo, *Access to mobile services and proof-of-identity: Global policy trends, dependencies and risks,* GSMA, 2018.

Tibbitts, Sabe, "The Aadhaar revolution—healthcare for all India," UK India Business Council, March 9, 2018.

Toakodi, Adongoi, and Victor Eyo Assi, "Corruption in the civil service: A study of payroll fraud in selected ministries, departments and agencies (MDAS) in Bayelsa State, Nigeria," *Research on Humanities and Social Sciences*, 2016, Volume 6, Number 3.

Toulmin, Camilla, "Security land and property rights in sub-Saharan Africa: The role of local institutions," *Land Use Policy*, January 2009, Volume 26, Issue 1.

Transparency International, Corruption Perceptions Index 2017, February 2018.

U

Unique Identification Authority of India, "AADHAAR Dashboard," Uidai.gov.

UK Department for Work and Pensions, *Fraud and error in the benefit system: Financial year 2016 to 2017 estimates*, November 30, 2017; updated July 20, 2018.

V

Vainsalu, Heiko, "How do Estonians save annually 820 years of work without much effort?," e-Estonia, December 2017.

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

Verick, Sher, *Women's labour force participation in India: Why is it so low?*, International Labour Organisation, 2014.

Verizon, *2018 data breach investigations report,* 2018.

Voices, "Demystifying technologies for digital identification," blog entry by Luda Bujoreanu, Anita Mittal, and Wameek Noor, February 27, 2018, https://blogs.worldbank.org/voices/demystifying-technologies-digital-identification.

W

We Are Social, *Global digital report 2018*, January 2018.

Wilson, Matthew, *Digital identity for smallholder farmers: Insights from Sri Lanka*, GSMA, 2018.

World Bank, *Global Findex Database 2017: Measuring financial inclusion and the fintech revolution*, 2018.

World Bank, "Global ID coverage by the numbers: Insights from the ID4D Findex survey," 2018.

World Bank, *Identity management cost-benefit analysis for Zambia, draft report*, 2018.

World Bank, *ID4D country diagnostic: Peru*, 2018.

World Bank, *ID4D-Findex survey data 2017.*

World Bank, *Principles on identification for sustainable development: Toward the digital age*, 2018.

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

World Bank, *Public sector savings and revenue from identification systems: Opportunities and constraints*, 2018.

World Bank, *The role of digital identification for healthcare: The emerging use cases*, 2018.

World Bank, *The state of identification systems in Africa: A synthesis of country assessments*, 2017.

World Bank, *Technology landscape for digital identification,* Identification for Development, 2018.

World Economic Forum, *Digital identity: On the threshold of a digital identity revolution,* January 2018.

World Economic Forum, *Identity in a digital world: A new chapter in the social contract*, September 2018.

Y

Yaga, Dylan et al., *Blockchain technology overview*, National Institute of Standards and Technology, US Department of Commerce, https://doi.org/10.6028/NIST.IR.8202.

Yang, Yao, "Towards a new digital era: Observing local e-government services adoption in a Chinese municipality," *Future Internet*, August 2017, Volume 9, Issue 3.

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