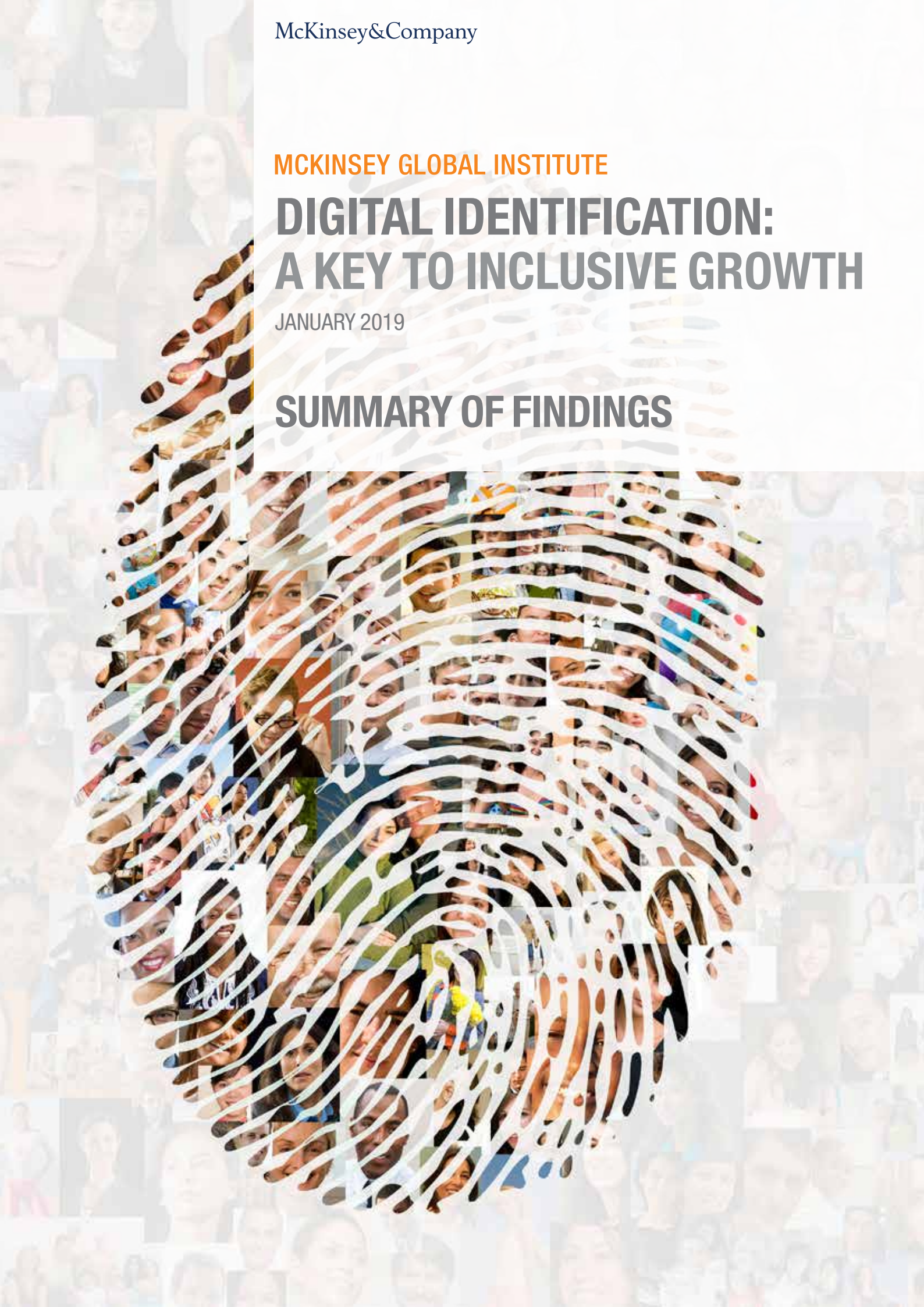


MCKINSEY GLOBAL INSTITUTE

DIGITAL IDENTIFICATION: A KEY TO INCLUSIVE GROWTH

JANUARY 2019

SUMMARY OF FINDINGS



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.

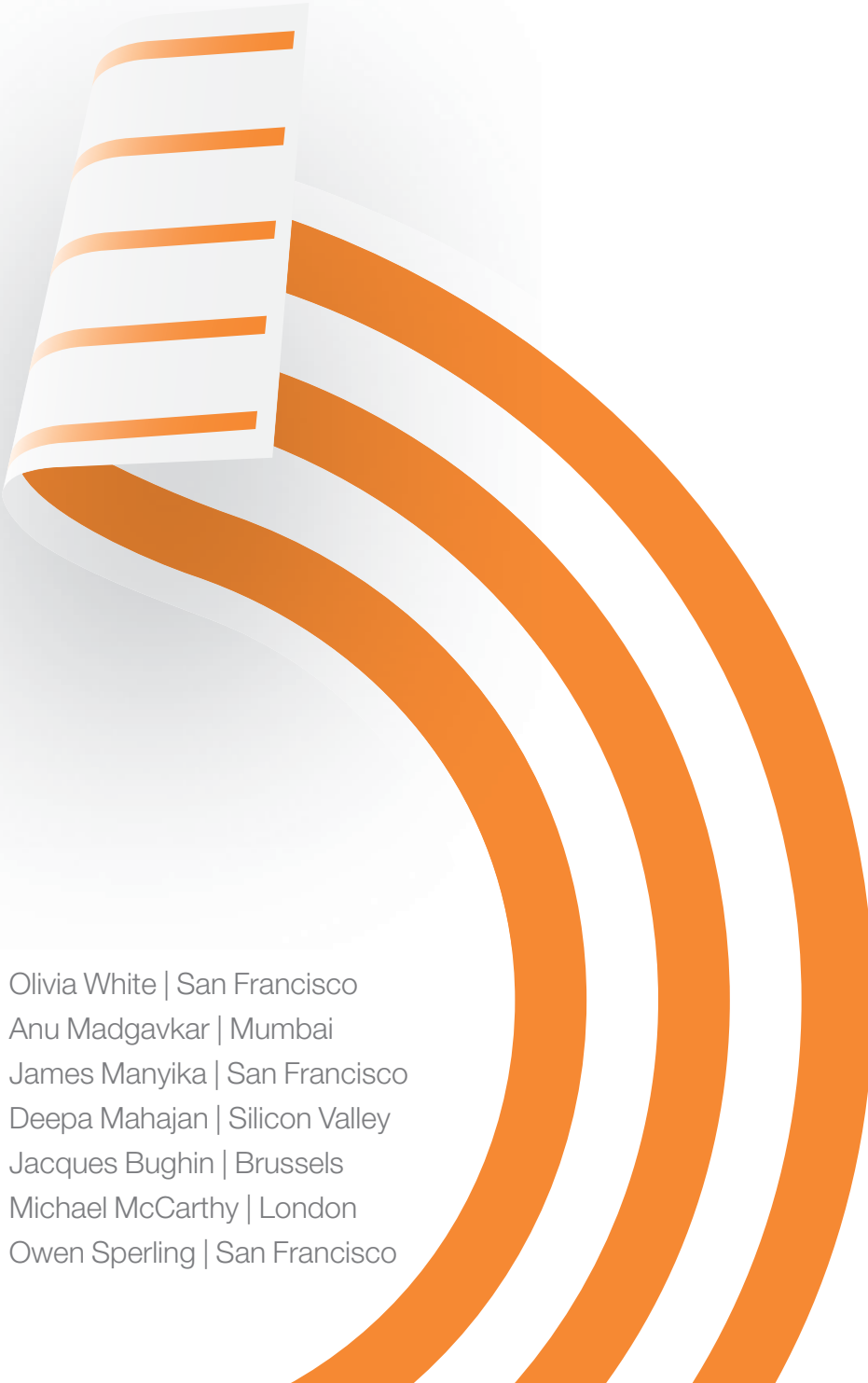
Project teams are led by the MGI partners and a group of senior fellows, and include consultants from McKinsey offices around the world. These teams draw on McKinsey's global network of partners and industry and management experts. Advice and input to MGI research are provided by the MGI Council, members of which are also involved in MGI's research. MGI Council members are drawn from around the world and from various sectors and include 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, act as advisers to 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 mckinsey.com/mgi.



DIGITAL IDENTIFICATION: A KEY TO INCLUSIVE GROWTH

JANUARY 2019



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

IN BRIEF

DIGITAL IDENTIFICATION: A KEY TO INCLUSIVE GROWTH

In an era of rapid technological change, digital identification provides a significant opportunity for value creation for individuals and institutions. Nearly one billion people globally lack a legally recognized form of identification, according to the World Bank ID4D database. The remaining 6.6 billion people have some form of identification, but over half cannot use it effectively in today's digital ecosystems. Individuals can use digital identification, or "digital ID," to be verified 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, with deep dives into seven diverse economies: Brazil, China, Ethiopia, India, Nigeria, the United Kingdom, and the United States. We find:

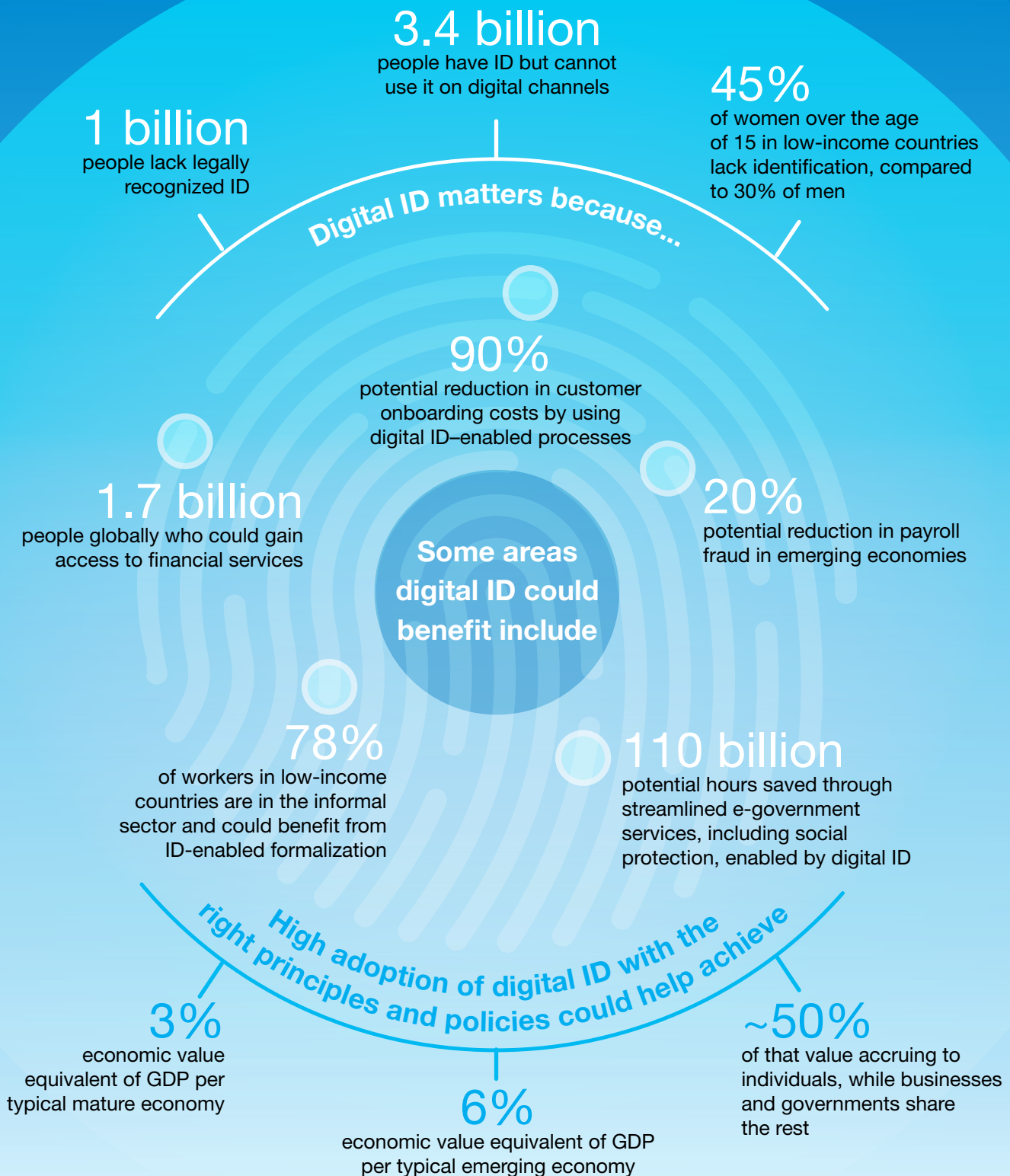
- Digital ID is a foundational set of enabling technologies that can be pivotal in a wide range of digital interactions between individuals and institutions. Digital ID technologies are also akin to "dual use" technologies that can be employed both to benefit society and for undesirable purposes by governments 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 and associated risks and challenges, 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 owners. Individuals benefit most as consumers from wider access to services, and as taxpayers and beneficiaries from time saved interacting with government. 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 ID4D Findex survey, and could help save about 110 billion hours through streamlined e-government services, including social protection and direct benefit transfers. For institutions, gains could come from higher productivity, cost savings, and fraud reduction; for example, improving customer registration could reduce onboarding costs by up to 90 percent, and reducing payroll fraud could save 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 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 over current levels. 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.

- 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, based on our modeling. Much of this value can 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 can 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 required 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. User adoption of digital ID will be accelerated if it provides value, engenders trust, and protects privacy. Institutions will be drawn to digital ID uses that lower costs, improve customer experience, or, in the case of public institutions, improve welfare.

The right digital ID technology, designed with the right principles and enforced with the right policies, can protect individuals from the risk of abuse and enable the safe inclusion of billions in the digital economy. As the landscape evolves, more work will be needed to understand the opportunities and commensurate challenges and to comprehend how stakeholders can respond.

Good digital ID

Unique, high-assurance, consent-based, digitally verifiable identification, with a range of possible credentials (eg, biometrics, passwords, smart devices)



NOTE: The concept of "good" digital identity has been developed and expanded by leading groups in the identity space including Omidyar Network and the World Bank. Building on this, in September 2018, the World Economic Forum convened a community of stakeholders from government, business, and civil society to form the Platform for Good Digital Identity, which made a commitment to advance toward a "good" future for digital identities.
SOURCE: World Bank ID4D; World Bank ID4D-Findex ; We Are Social; International Labour Organization; McKinsey Global Institute analysis

SUMMARY OF FINDINGS

It is easy to take identification for granted, particularly in mature economies. 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.¹ The rest of the world's inhabitants, about 6.6 billion people, either have some form of identification but limited access to 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 verify their identity through a digital channel, unlocking access to the digital world in the economic, social, and political realms (See Box 1, “What is digital ID?”).

In this report, we take a comprehensive approach to understanding the potential benefits of “good” digital ID for both individuals and institutions, while highlighting the potential for misuse and other challenges and risks. 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. 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.²

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.³

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 can be significant. Despite its mixed success so far, digital ID can represent an important key to unlocking inclusive growth.

¹ World Bank Global ID4D Dataset, 2018.

² *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.

³ 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.

Box 1. What is digital ID?

Unlike a paper-based ID such as most driver's licenses and passports, a digital ID can be verified remotely over digital channels, often at a lower cost. While the term "digital ID" can be used in the broader public debate somewhat loosely, we use it specifically to refer to good digital ID, regardless of whether the issuer is a government or nongovernment entity, that has the following attributes:

- **Verified to a high degree of assurance.** 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 underlying technology. A range of credentials can 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 scheme, and every scheme 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 control over what personal data will be captured and how they will be used.

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.¹ 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 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.

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. Another 3.4 billion who have some type of legally recognized identification are not active in the digital economy, proxied by absence of social media use. 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 1). 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.

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, likely driven by the absence of acceptable forms of identification.⁵ In countries such as Kenya and Malaysia, an ID or other official credential is needed for students to be allowed to sit for secondary school exams.⁶ 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 to only 30 percent of men.⁷

Digital ID also unlocks new opportunity for the 3.4 billion individuals who have some form of high-assurance ID but limited access to the digital world.⁸ Moving from purely physical ID to digital ID programs, and creating digital infrastructure and applications that use digital ID for authentication, can 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 multi-use form of identification, not a feature of many conventional national identity programs today. For example, as detailed in Exhibit 1, a 2016 study of 48 national identity programs found that very few could be used in a wide variety of sectors.⁹

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. In addition, many of the 3.4 billion people who will become digitally active in the years to come stand to gain in the same ways. Individuals around the world have significant privacy-related concerns that high-assurance digital ID can address.¹⁰ For instance, one

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 Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?*, Center for Global Development, 2018.

⁷ *ID4D-Findex survey data 2017*, World Bank.

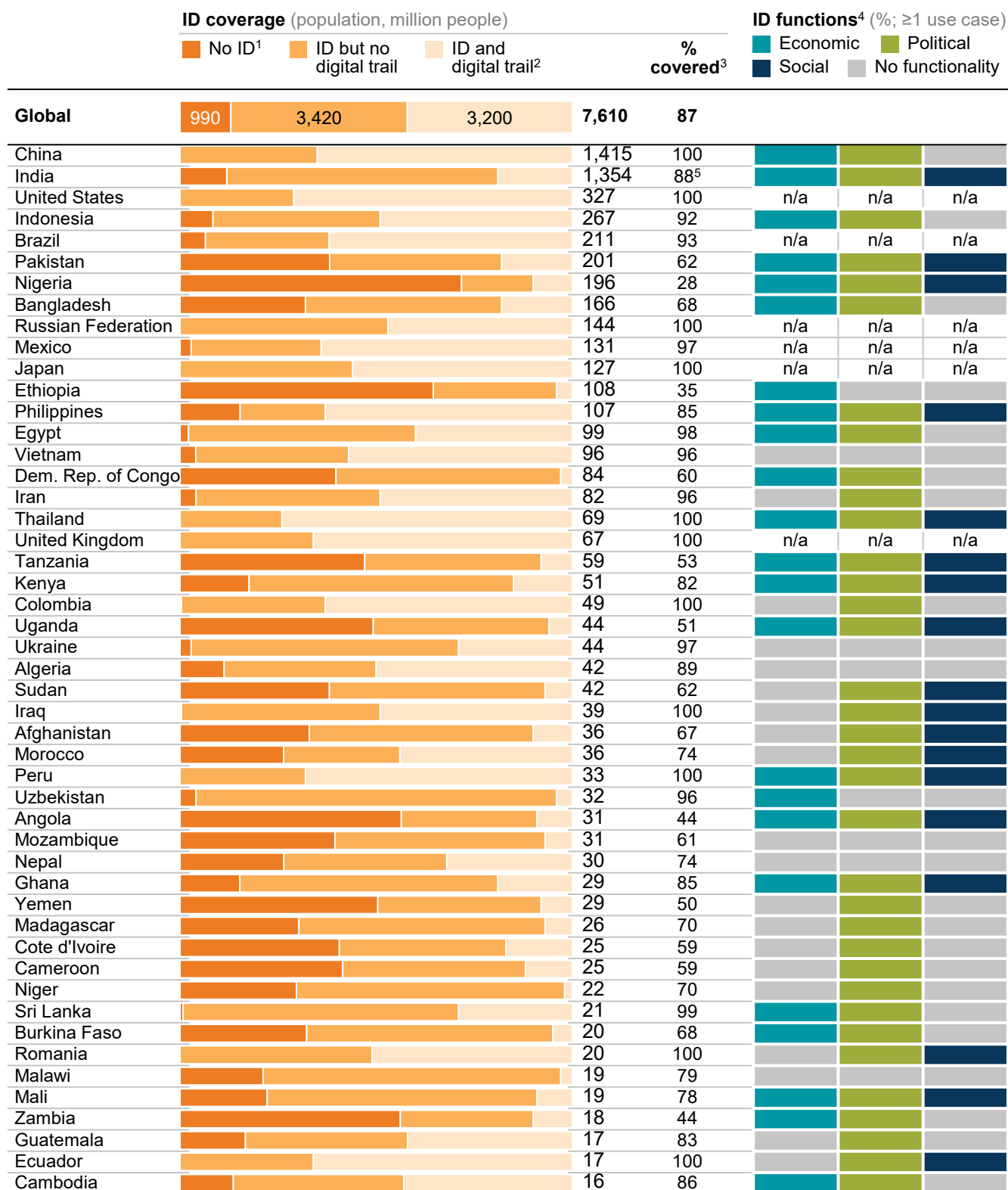
⁸ The population with access to the digital world is proxied by active social media users, captured in the *We Are Social Global Digital Report 2018*.

⁹ *Review of national identity programs*, International Telecommunication Union, May 2016.

¹⁰ Several bodies of digital ID research have focused on privacy-related requirements and guidelines. These include the Digital Identity Issue Analysis and Identities Report sponsored by Omidyar Network.

Exhibit 1

Across the globe, 1 billion people lack ID and existing ID schemes vary widely.



1 "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 is not available. Where available registration data exceeds population or where there is limited data, 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).

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 be among population with some form of legally recognized ID.

3 Percentage of total population that have an ID.

4 Data from ITU analysis based on review of academic and grey literature for 48 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 (e.g. financial services KYC), political (e.g. voting) and social (e.g. health services).

5 This percentage does not include individuals who have adopted Aadhar digital ID over the second half of 2018; according to data from the Unique Identification Authority of India, Aadhar covered ~90% of the population as of January 2019.

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

study found that 53 percent of online users do not feel that they are in control of their data.¹¹ Low-assurance interactions contribute to the potential of cybersecurity breaches, which pose increasing downside 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.¹² Beyond security concerns, many active 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 enables. For example, one study found that about 30 percent of calls to banks’ call centers are requests for account access due to misplaced or forgotten passwords.¹³

Forty or more national or non-national digital identity programs exist today (Exhibit 2). Roughly 1.2 billion people with digital IDs live in India alone, registered in the Aadhaar program, which began in 2009. Yet many digital ID programs have 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.

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.¹⁴ Meanwhile, 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 from 2008 to 2016.¹⁵

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.¹⁶ Biometric technology for registration and authentication is becoming more accurate and less expensive.¹⁷ For example, iris-based authentication technologies can give false acceptance rates as low as 0.2 percent and false rejection rates of 0.0001.¹⁸ The average selling price of a fingerprint sensor found in a mobile phone fell by 30 percent in 2017 alone.¹⁹ Bar codes on cards, which once stored only numerical data, can now secure signature, fingerprint, or facial data.²⁰ Blockchain technologies, with appropriate design and

¹¹ Mobile Ecosystem Forum 2017 survey of 6,500 individuals in ten countries: Belgium, China, France, Germany, Poland, Romania, South Africa, Spain, the United Kingdom, and the United States.

¹² 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.

¹³ *The future of identity in banking*, Accenture, 2013.

¹⁴ Global Digital Report 2018, We Are Social, January 2018; *Technology Landscape for Digital Identification*, Identification for Development, World Bank, 2017.

¹⁵ *The 2015–16 affordability report*, Alliance for Affordable Internet, 2016.

¹⁶ Luda Bujoreanu, Anita Mittal, and Wameek Noor, “Demystifying technologies for digital identification,” World Bank, February 27, 2018.

¹⁷ *Technology Landscape for Digital Identification*, Identification for Development, World Bank, 2017.

¹⁸ *Ibid.*

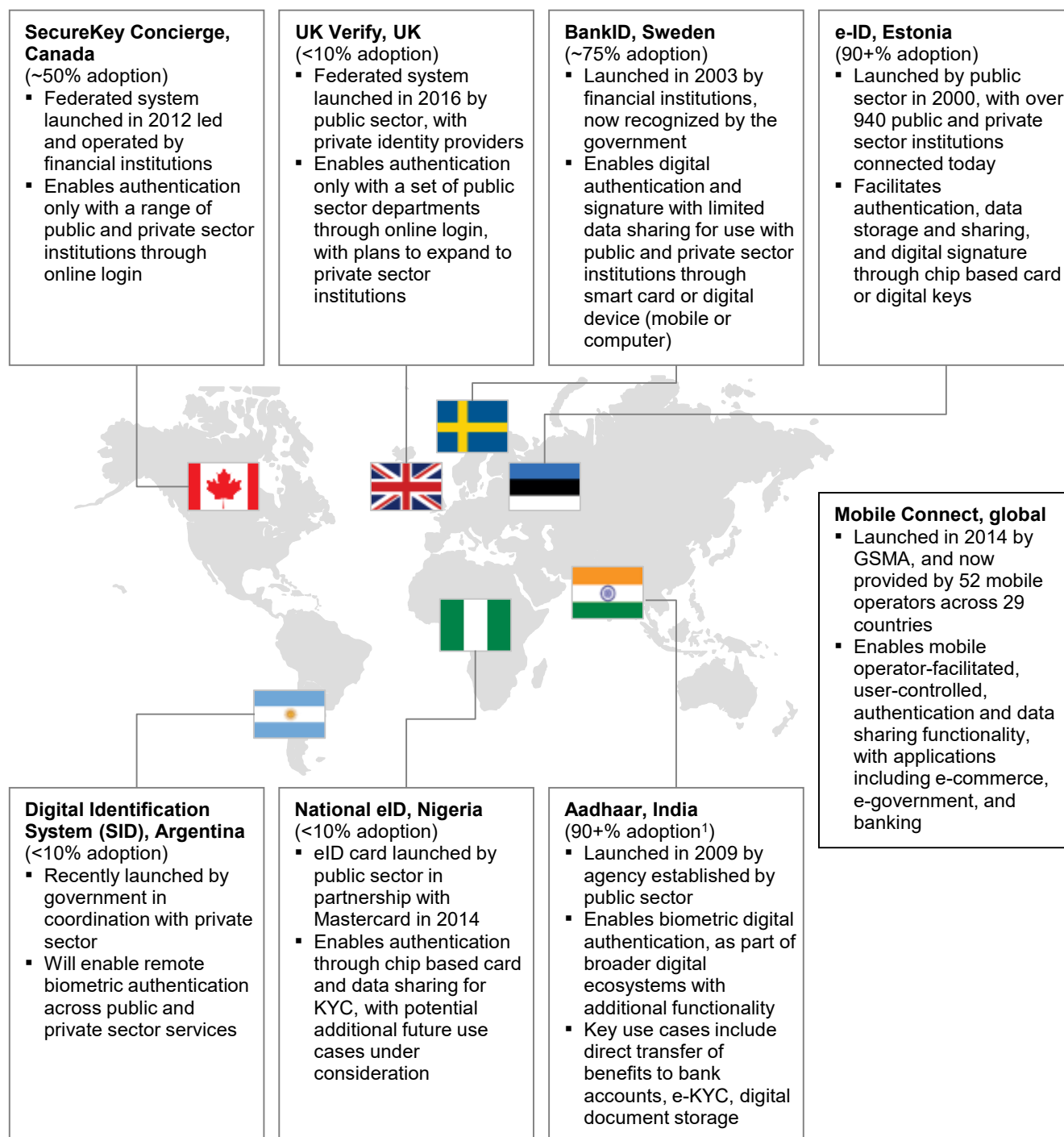
¹⁹ Chris Burt, “Fingerprint Cards reports cost cutting and changing focus after tough 2017,” *BiometricUpdate.com*, February 9, 2018; Danny Thakkar, *Biometric devices: Cost, types, and comparative analysis*, Bayometric.

²⁰ *Ibid.*

Exhibit 2

A variety of digital ID systems currently operate around the world.

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



1 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

governance, could potentially help decentralize information storage so there is no single point of failure in case of cyberintrusion or internal fraud.²¹

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 individual data. History provides ugly examples of misuse of traditional identification programs, including to track or persecute ethnic or 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. 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.²²

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 it is 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 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 2016.²³ 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 comprehensive 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 or 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

²¹ *Blockchain technology overview*, National Institute of Standards and Technology, US Department of Commerce, <https://doi.org/10.6028/NIST.IR.8202>.

²² 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.

²³ *Data age 2025: The evolution of data to life critical*, Seagate, March 2017.

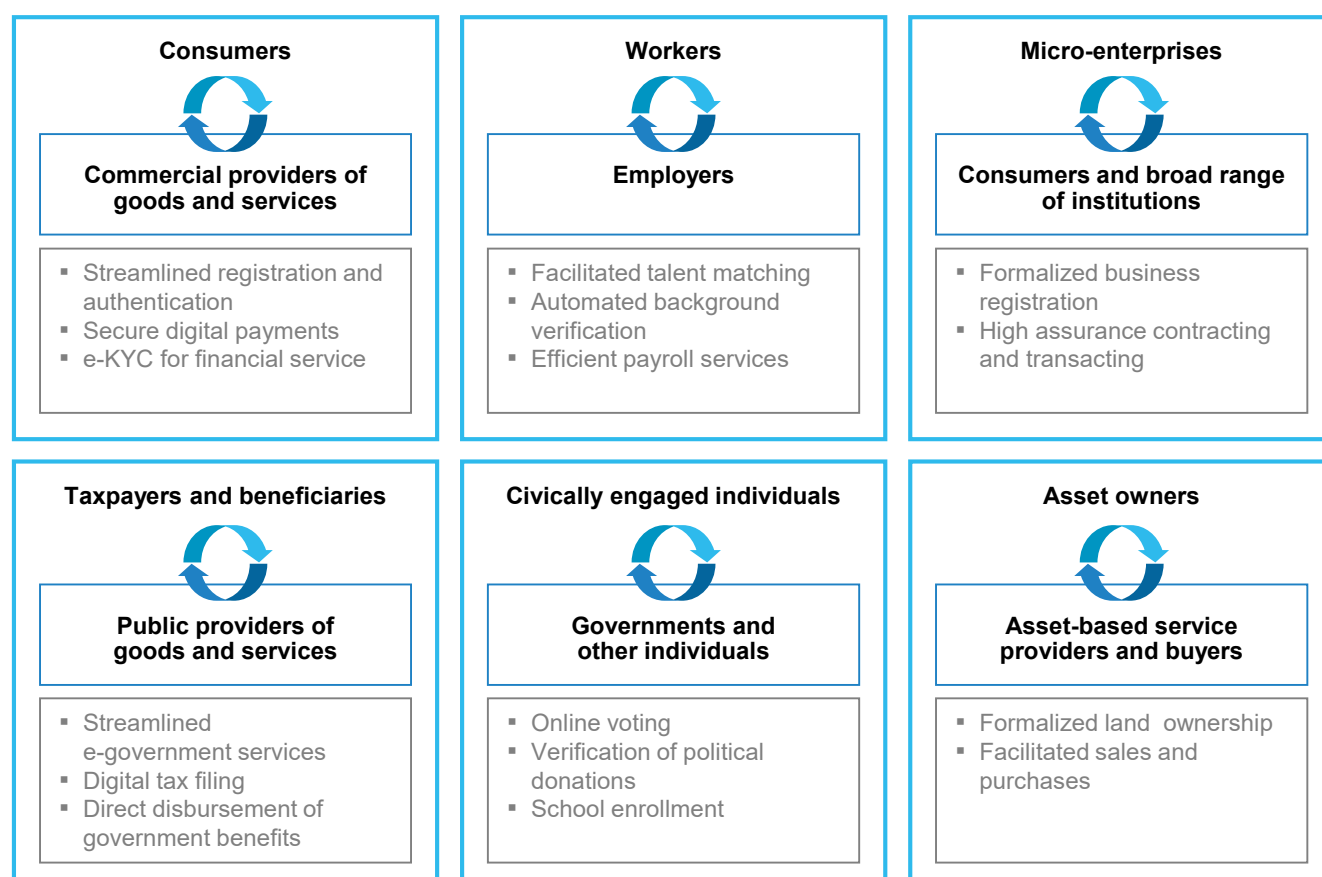
individuals use digital interfaces. For example, individuals without sufficient technological access or savvy or who do not trust a digital ID system could be completely excluded, unless alternative manual options also exist.

INDIVIDUALS AND INSTITUTIONS CAN BENEFIT FROM DIGITAL ID IN A RANGE OF INTERACTIONS

Digital ID can facilitate 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 engaged individuals, and asset owners (Exhibit 3). 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 residents; 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 2, "Our methodology").

Exhibit 3

Individuals use digital ID across 6 roles to interact with institutions and create shared value.



NOTE: Grey text indicates example use cases associated with each of the six roles. Our analysis examined in detail nearly 100 such use cases, across roles.

SOURCE: McKinsey Global Institute analysis

Box 2. 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 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 three factors: the addressable share of the economy that would be impacted, the incremental share of interactions that may adopt and use the digital ID, and the potential for value creation from each such interaction. 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 will 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 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 will 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 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 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.
- **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 the 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.

Among the ways digital ID can be used, core benefits include increased financial inclusion, improved labor market efficiency, time savings, and fraud reduction (Exhibit 4). 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 all types of interactions.

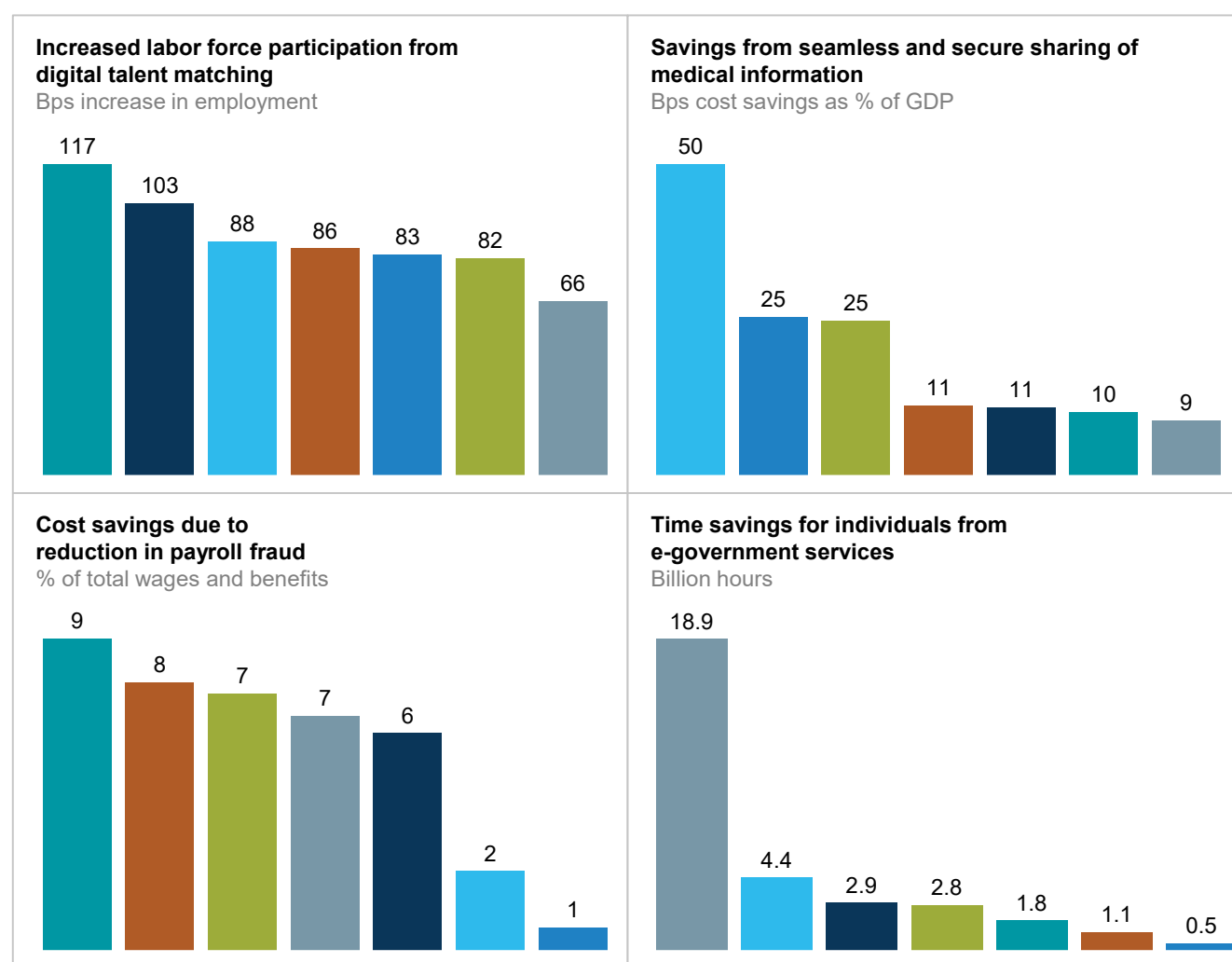
Exhibit 4

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

Four examples of how digital ID can create value

Potential benefits, 2030E

■ Brazil ■ China ■ Ethiopia ■ India ■ Nigeria ■ United Kingdom ■ United States



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.

- **Increased use of financial services.** Digital ID helps individuals meet Know Your Customer (KYC) requirements and enables remote customer registration for financial services.²⁴ 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.²⁵ We estimate that in Brazil, for example, digital ID could help 39 million adults gain access to financial services and facilitate increased extension of credit to both individuals and micro, small, and medium-size enterprises (MSMEs).²⁶
- **Improved access to employment.** Better digital talent matching and contracting platforms are enabled by digital ID programs, which allow job seekers to authenticate themselves online. Such platforms can streamline access to labor markets for inactive and unemployed workers. The combination of identification coverage and high-assurance digital platforms can 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 land ownership.** By enabling formal land titling, digital ID can help improve incentives to make larger and longer-term investment in farming. This can 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.²⁷ 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 targeted 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.²⁸ Digital ID also can 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.

In addition to direct sources of value from digital ID to individuals, we anticipate that institutions will pass on some of the value they gain through cost savings, fraud savings, and tax revenue. This may take the form of reduced prices in consumer interactions, increased income in worker or taxpayer interactions, or additional spending on benefits or infrastructure in taxpayer and beneficiary interactions.

²⁴ Ibid.

²⁵ *ID4D-Findex survey data 2017*, World Bank.

²⁶ *ID4D-Findex survey data 2017*, World Bank; *World Development Indicators 2018*, World Bank.

²⁷ 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.

²⁸ "E-identity: ID card," e-Estonia, e-estonia.com/solutions/e-identity/id-card.

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 can 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 using physical branches.²⁹
- **Fraud savings.** 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 2016.³⁰ Worldwide, theft of consumers' identities costs businesses an estimated \$141 per person.³¹ 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.³²
- **Increased sales of goods and services.** Through digital onboarding, which enables streamlined authentication and improves customer experience in digital channels, institutions can 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 using e-KYC, enabled by India's national digital ID system, Aadhaar.³³ Digital ID could also reduce opportunity costs; in the United Kingdom, for example, nearly 25 percent of financial applications are abandoned due to difficulties in the registration process.³⁴ Institutions that already rely on some form of high-assurance identities, such as banks and digital gig economy platforms like Uber, have 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 verification, and enable contracting with nontraditional workers, such as contract and gig workers. As a result, businesses can more rapidly fill open positions and find the right employee for a given position, leading to higher productivity. 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 to 42 percent in 2015, and hiring time increased by 3.4 days, or 15 percent of the average hiring cycle.³⁵

²⁹ *Digital finance for all: Powering inclusive growth in emerging economies*, McKinsey Global Institute, September 2016.

³⁰ "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 8, 2018.

³¹ *2017 cost of data breach study: Global overview*, Ponemon Institute, June 2017.

³² 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.

³³ "Jio propels India to top in mobile broadband consumption by automating world's first all-IP network with Cisco," Cisco, 2018.

³⁴ Private sector economic impacts from Identification Systems, World Bank Group, 2018.

³⁵ *Why is hiring taking longer? New insights from Glassdoor data*, Glassdoor, June 2015.

- **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.³⁶ 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.³⁷ 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.³⁸ In Latin American countries, approximately half of potential tax revenues are lost to tax evasion.³⁹

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, 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 5 and 6). We emphasize that India has already made substantial progress in unlocking value by implementing Aadhaar, leading to a somewhat lower value potential than might otherwise be expected.

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 be thoughtful about 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. 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.

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:

³⁶ *Digital revolutions in public finance*, IMF, November 2017.

³⁷ Joseph J. Atick, *Digital identity: The essential guide*, ID4Africa Identity Forum, 2017.

³⁸ Ibid.

³⁹ Eduardo Cavallo et al., *Saving for development: How Latin America and the Caribbean can save more and better*, Inter-American Development Bank, June 2016.

- **Addressable share.** This is the share of the economy consisting of those types of interactions that digital ID could improve. 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 can 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 would be 8 percent of GDP; with advanced digital ID, it would 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 can 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.

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 captures 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. The International Labour Organization estimates that 81 percent of Nigeria's workforce is self-employed, and the informal economy generates 65 percent of GDP. Digital ID can 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 can also 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, while 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 500 million voter ID.⁴⁰ 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. 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.

⁴⁰ *Aadhaar: Inclusive by design: A Look at India's National Identity Programme and its role in the JAM Trinity*, GSMA, March 2017.

India has also seeded 82 percent of public benefits disbursement accounts with Aadhaar, which has reduced fraud and leakage.⁴¹ We calculate that India can 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

In the United Kingdom, we estimate total economic value equivalent to less than 0.5 to 3 percent from digital ID high adoption. 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 can 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.

The United States is very similar to the United Kingdom, except that it could capture an additional 1 percent (relative to GDP) of value from digital ID compared to the United Kingdom, an opportunity driven in part by higher levels of healthcare expenditure.⁴³ According to the World Bank, 2015 healthcare expenditure in the United States was 16.8 percent of GDP, compared with 9.8 percent in the United Kingdom. Digital ID can create significant efficiencies in healthcare expenditures through facilitated sharing of records, and therefore the economic impact of these efficiencies in the United States will 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.

We find that the economic potential of digital ID in China is more in line with that of the United States and United Kingdom, with a total potential value unlocked by digital ID equivalent to 2 to 4 percent of GDP in 2030. Similar to the situation in the United States and United Kingdom, 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 levels of ID coverage, at 98 percent of the population according to World Bank analysis, reduce the relative gains experienced by microenterprises and asset owners relative to 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.

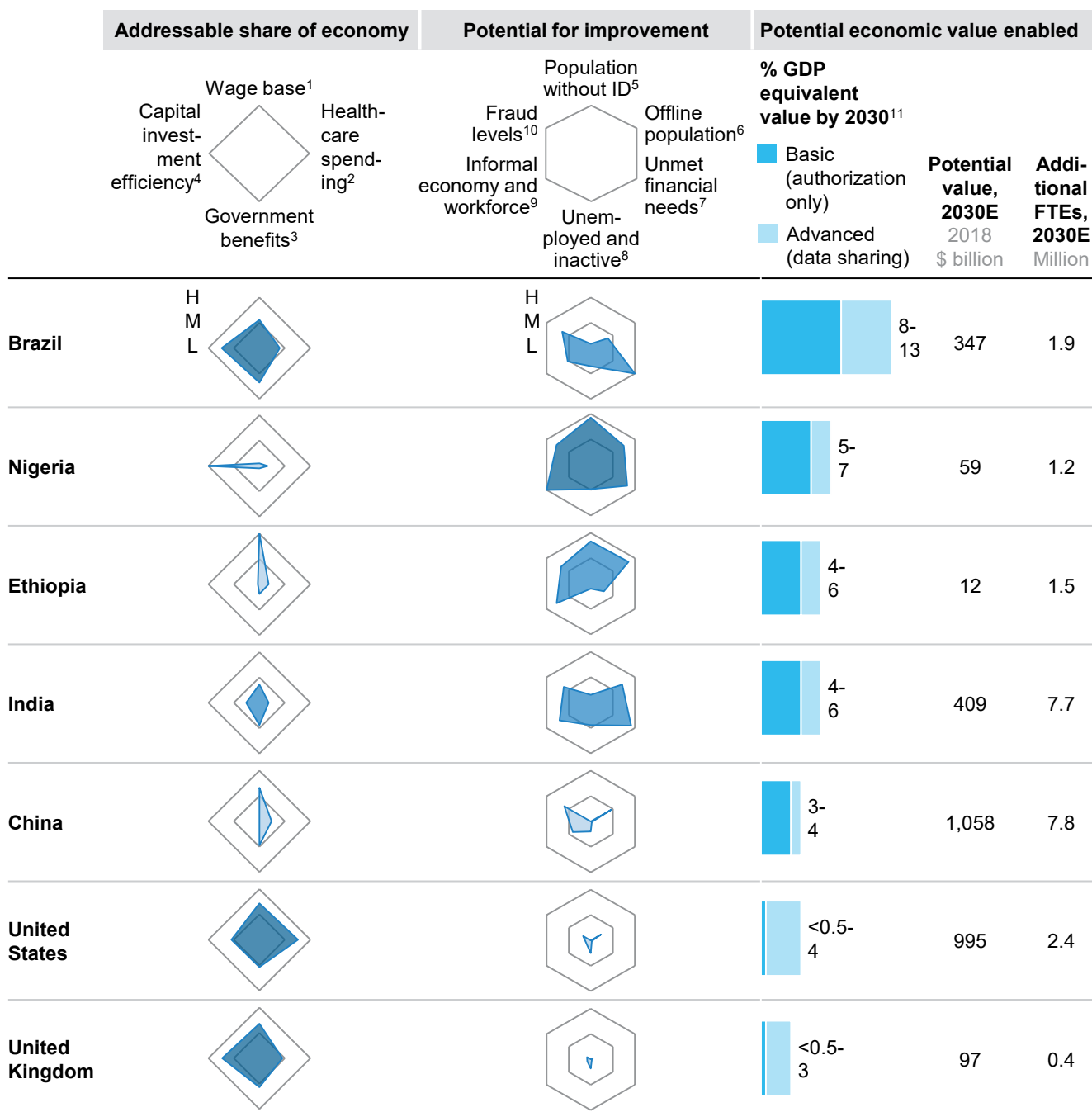
⁴¹ *State of Aadhaar report, 2017–18*, IDinsight.

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.

Exhibit 5

The magnitude and nature of potential value creation of digital ID varies across focus countries.



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 Off-line 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 corruptions 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.

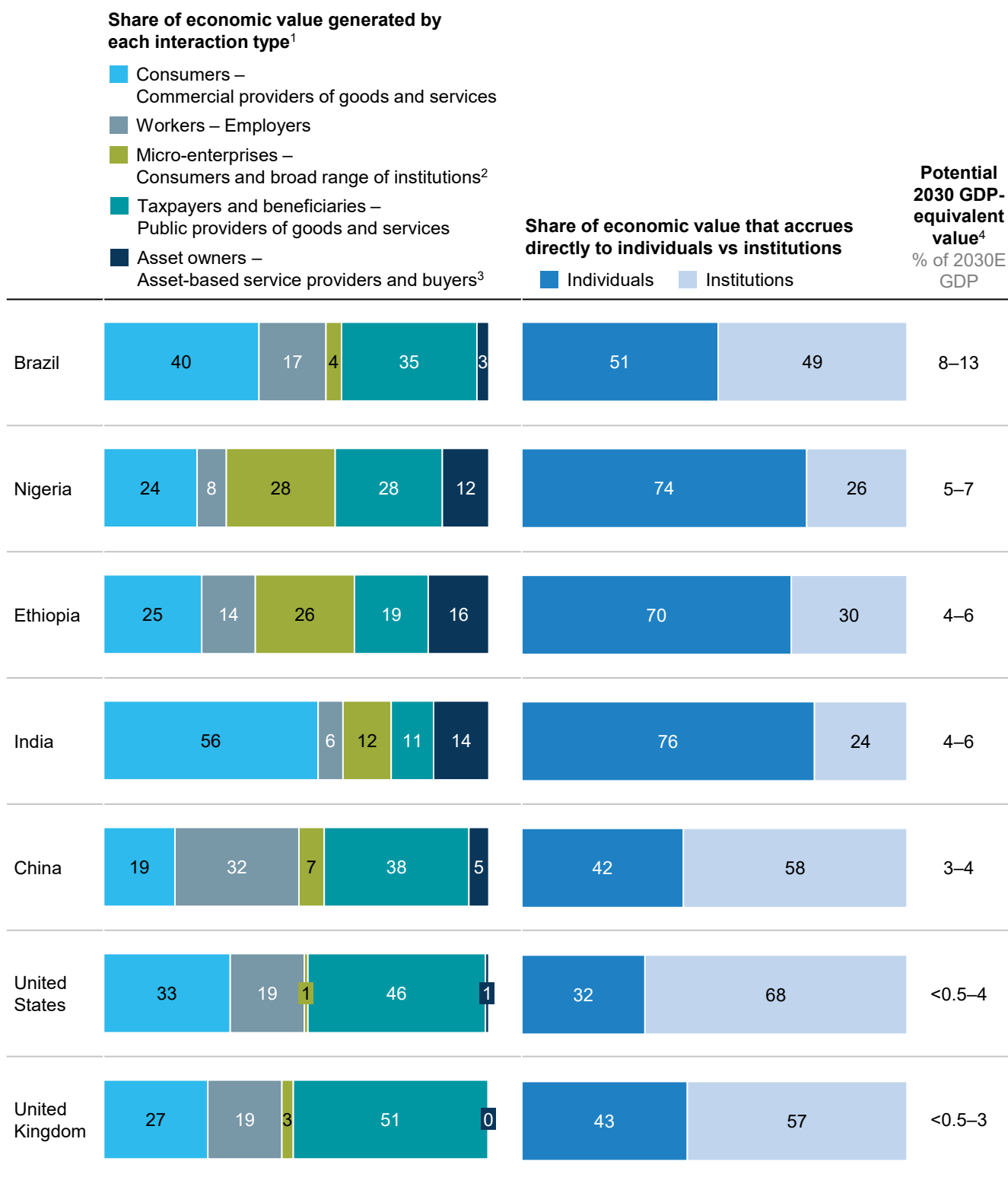
NOTE: For each chart, a larger shaded area reflects a higher contribution to economic value while a smaller shaded area reflects a smaller contribution to economic value. The charts are normalized on each dimension across a set of 217 countries. Calculation for potential economic value enabled is performed for deep-dive countries using over 100 use cases (see Methodology box). Addressable share of the economy and potential for impact based on latest available data whereas economic value estimates are 2030. Addressable share metrics represent ratios relative to GDP in a country. Addressable share of the economy and potential for impact based on latest available data whereas economic value estimates are 2030. Addressable share metrics represent ratios relative to GDP in a country. H, M, L reflects a comparison of the metrics across 217 countries where H represents the highest level of the metric across the country set.

SOURCE: ITU; World Bank; ID4D; Findex; WDI; IMF; McKinsey Global Institute analysis

Exhibit 6

Individuals stand to gain about 50% 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 We do not size economic value generated through civically engaged individual interactions with governments and other individuals.

² Includes all institutions or individuals that contract with, purchase goods or services from, or provide services to micro-enterprises.

³ Includes a range of asset-based service providers including those involved in services such as titling, financing, and leasing.

⁴ Range of potential value based on whether digital ID is basic (ie, authorization only) or advanced (full data sharing).

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

SOURCE: McKinsey Global Institute analysis

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 7). 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 high levels of adoption. In emerging economies, much of the value can 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 UK, 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 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, for example Peru, have recently strengthened identification for children in an attempt to fight child trafficking. Stronger identification can also help enforce laws against child marriage and thus contribute to its elimination and the empowerment of women and girls worldwide.⁴⁷ In Indonesia, for example, 95 percent of girls who married at 18 years of age or younger lacked a birth certificate.⁴⁸

⁴⁴ AADHAAR Dashboard, Unique Identification Authority of India, Uidai.gov; *About the e-ID Card*, 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; *E-identity*, E-Estonia.com; *This is Bank ID*, BankID.com; *About us*, BankID.no.

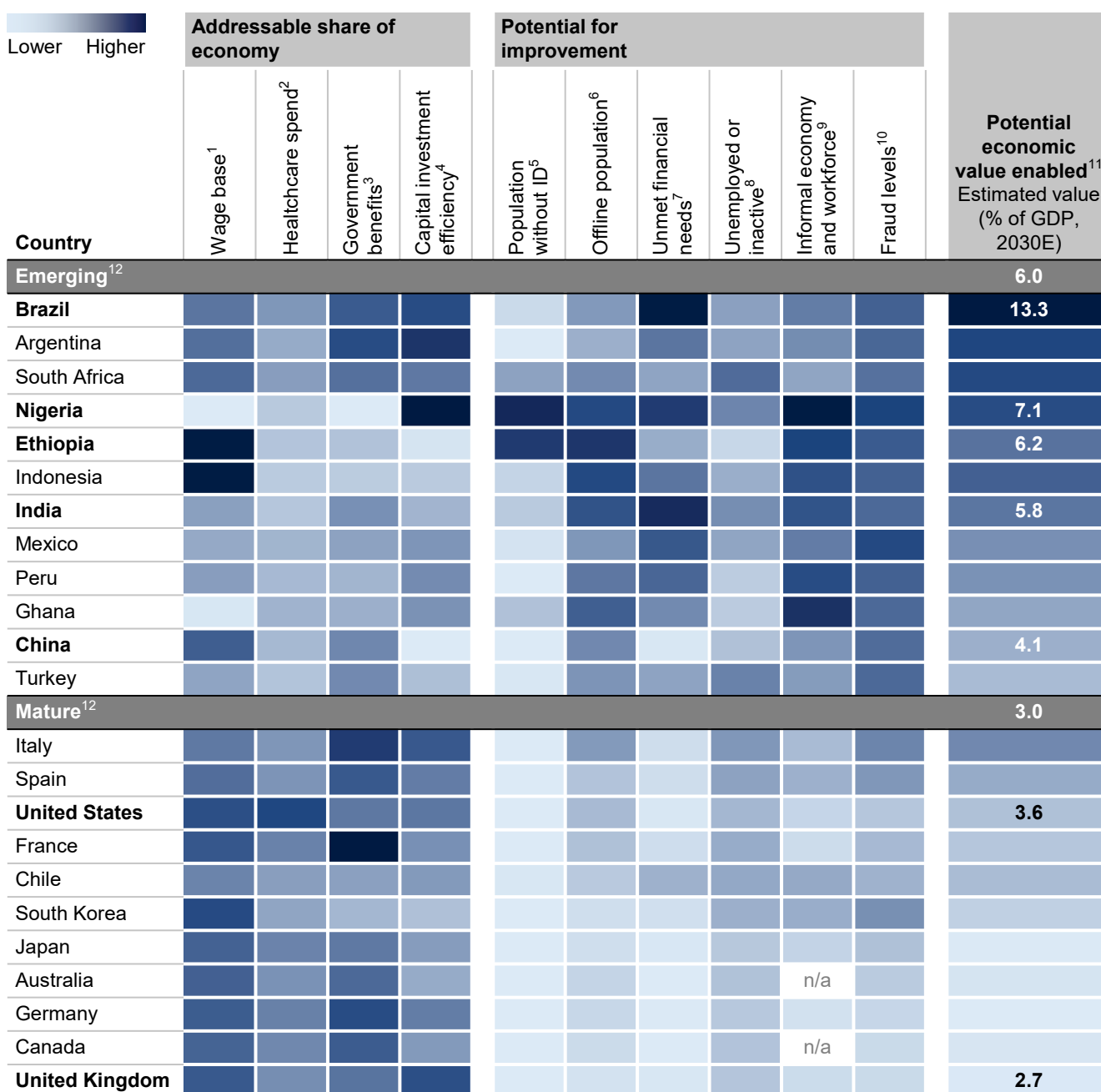
⁴⁶ *A comparative assessment of electronic voting*, Elections Canada, 2018.

⁴⁷ Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?*, Center for Global Development, 2018.

⁴⁸ Lucia Hanmer and Marina Elefante, *The role of identification in ending child marriage*, World Bank, July 2016.

Exhibit 7

Value creation from digital ID varies across countries 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 Off-line 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 corruptions 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 deep-dive countries (shown in bold) using over 100 use cases (see Methodology box). 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 whereas economic value estimates are 2030. Addressable share metrics represent ratios relative to GDP in a country.

SOURCE: ITU; World Bank; ID4D; WDI; Findex; McKinsey Global Institute analysis

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, 9 million duplicates, and 15 million entries without verifiable identities.⁴⁹

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.

Country-level implementation decisions should account for digital infrastructure, level of trust in institutions, and policy landscape

Preconditions for digital ID include a minimal level of digital infrastructure, sufficient trust in the digital ID provider, and a policy landscape that provides some safeguards to individuals. As long as they meet minimal levels, the specifics of these factors will shape choices about how digital ID is implemented in a given country.

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. Programs requiring remote access by users rely on widespread internet access, at a minimum covering internet-enabled hotspots that allow for authentication. Countries vary significantly in their level of internet access, with 99 percent of individuals in North America living in areas covered by a 3G or 4G network compared to only 60 percent in sub-Saharan Africa.⁵⁰ However, internet access is not enough. Digital ID programs require penetration of devices necessary for adoption by both users and requesting parties. These can include smartphones and a digital payments infrastructure that could be leveraged by digital ID programs to improve feasibility and reduce factors that slow adoption. Lastly, a reliable grid ensures the consistent system functionality necessary for providing predictable services and maintaining trust in the system. 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.

⁴⁹ Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?*, Center for Global Development, 2018.

⁵⁰ *World Telecommunication/ICT Development Report and database*, International Telecommunication Union, June 2018.

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.⁵¹ However, this varies across geographies. Research commissioned by Omidyar Network found that relative levels of trust differed significantly around the world, with individuals in Eastern and Central Europe much more likely to trust government relative to private companies, while individuals in Latin America were more than twice as likely to trust private companies as government.⁵² These differences imply that the institutions most likely to gain user trust for data management will differ across geographies, with implications for the optimal implementation approach and the ability of an ID provider to garner adequate adoption.

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. On the flip side, if digital ID is used to satisfy such 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.

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. In the most successful cases, such as Denmark and India, adoption rates can surpass 70 percent in less than five years, but adoption rates in other programs remain under 10 percent, as in the UK and Nigeria.⁵³ 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. 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 and stickiness. We find that government and financial services uses have the greatest potential to provide value to both institutions and individuals simultaneously, through high-frequency use cases. Digital ID can be used in the provision of e-government services and benefits, expanding access and saving time for citizens while reducing costs for governments and improving

⁵¹ *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.

⁵² “Trust and privacy,” Omidyar Network, October 2, 2017.

⁵³ *The next generation of national electronic identity and signing in Denmark*, Ministry of Finance Agency for Digitisation, April 2016; AADHAAR Dashboard, Unique Identification Authority of India, uidai.gov.in; About the e-ID Card, National Identity Management Commission, nimc.gov.ng; GOV.UK Verify Dashboard, [Gov.UK](https://gov.uk/verify); Updated as of 1/2/2019.

social welfare, when compared to existing physical touchpoints. Financial services can use digital ID in e-KYC to make it easier for individuals to access services while cutting institutional costs and reducing financial crime.

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. For example, Sweden's Bank ID program, which has a roughly 75 percent adoption rate among adults, used a mobile application that streamlined the user login and authentication process.⁵⁴ By contrast, GOV.UK Verify, which as of January 2019 had a 51 percent verification failure rate, has seen less than 10 percent adoption.⁵⁵ 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 deleting the Facebook app from their mobile device in the previous year.⁵⁶ 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, India successfully onboarded nearly one 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.⁵⁷ 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 areas. At the same time, institutions need to be able to seamlessly integrate digital ID into their services at minimal expense. This can be achieved through clear standards that make digital IDs interoperable across firms, sectors, and uses, and it may help commoditize authentication mechanisms.

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

Realizing the 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.

⁵⁴ *This is Bank ID*, Bank ID, bankid.com/en/om-bankid/detta-ar-bankid.

⁵⁵ *GOV.UK Verify Dashboard*, Gov.UK

⁵⁶ *Americans are changing their relationship with Facebook*, Pew Research Center, 2018.

⁵⁷ Alan Gelb and Anna Diofasi Metz, *Identification revolution: Can digital ID be harnessed for development?*, Center for Global Development, 2018.

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. 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. A federated structure distributes cost and dilutes potential for abuse but also requires coordinated decision making, introducing complexity that may disincentivize institutions from participating as ID providers.
- 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. Structural benefits include strong user control over data, decentralized data storage, and 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 on how people register, for example through physical or remote digital channels; what credentials they can use, such as smart cards, innate biometrics, or passwords and personal identification numbers; and how ongoing user and requesting party interaction will occur, which could include 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 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. Decision rights determine how major program management decisions are made and should be flexible enough to effectively react to dynamic problems, such as cyberbreaches. Access rights establish who user data is available to and what they can do with it. 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 is open, all access is logged, and unauthorized activity results in jail time. In Europe,

companies violating the EU General Data Protection Regulation can be fined up to 4 percent of annual global revenue.

Governments, businesses, and civil society institutions 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, 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 are outlined in this section.

Governments can play the role of requesting party, for example by asking for information or authentication about constituents; ID provider, for example as the direct provider of a state-run system; or manager of a federated multiprovider 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, 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.

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 and to protect them 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 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.

ACKNOWLEDGMENTS

Our research focuses on the economic potential of good digital ID. As an enabler of economic, social, and political activity in a digital age, 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, more research is needed in areas including system design, governance, and use, as well as the potential for misuse. However, we hope this research contributes to a greater understanding of how good digital ID, designed with the right principles and enforced with the right policies, can create significant economic benefits for individuals and institutions and 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 comprised 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 the 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); Michael Wiegand, director of the Financial Services for the Poor at the Bill and Melinda Gates Foundation; and Hal Varian, chief economist at Google and professor emeritus at the University of California Berkeley.

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

This summary of findings was edited and produced by senior editor Anna Bernasek, editorial production manager Julie Philpot, and senior graphic designers Marisa Carder, Margo Shimasaki, and Patrick White. Rebeca Robboy, together with Nienke Beuwer and Cathy Gui, managed dissemination and publicity.

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



McKinsey Global Institute
January 2019
Copyright © McKinsey & Company
www.mckinsey.com/mgi

 @McKinsey_MGI
 McKinseyGlobalInstitute