Digital identification: A key to inclusive growth

April 17, 2019 | Report

New research by the McKinsey Global Institute shows how good digital ID is a new frontier in value creation for individuals and institutions around the world.

By Olivia White, Anu Madgavkar, James Manyika, Deepa Mahajan, Jacques Bughin, Mike McCarthy, and Owen Sperling

DOWNLOADS

Executive Summary (PDF-1 MB)

Full Report (PDF-2 MB)

Digital identification, or "digital ID," can be authenticated unambiguously through a digital channel, unlocking access to banking, government benefits, education, and many other critical services. The risks and potential for misuse of digital ID are real and deserve careful attention. When 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. In this research, we develop a framework to understand the potential economic impact of digital ID, informed by an analysis of nearly 100 ways in which digital ID can be used in Brazil, China, Ethiopia, India, Nigeria, the United Kingdom, and the United States.

In our seven focus countries, extending full digital ID coverage could unlock economic value equivalent to 3 to 13 percent of GDP in 2030, with just over half of the potential economic value potentially accruing to individuals. Realizing this value is by no means certain or automatic—it necessitates multiple high-value use cases and high levels of usage—and not all of these potential sources of economic value may translate into GDP. Yet, with careful system design and policies to promote uptake and mitigate risks, digital ID could be a powerful key to inclusive growth, offering quantifiable economic value to individuals, beyond significant noneconomic benefits.

TABLE OF CONTENTS

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

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

- *Verified and authenticated to a high degree of assurance:* High-assurance digital ID meets both government and private-sector institutions' standards for initial registration and subsequent acceptance for a multitude of important civic and economic uses, such as gaining access to education, opening a bank account, and establishing credentials for a job. High-assurance authentication maintains these same standards each time the digital ID is authenticated. This attribute does not rely on any particular underlying technology. A range of credentials could be used to achieve unique high-assurance

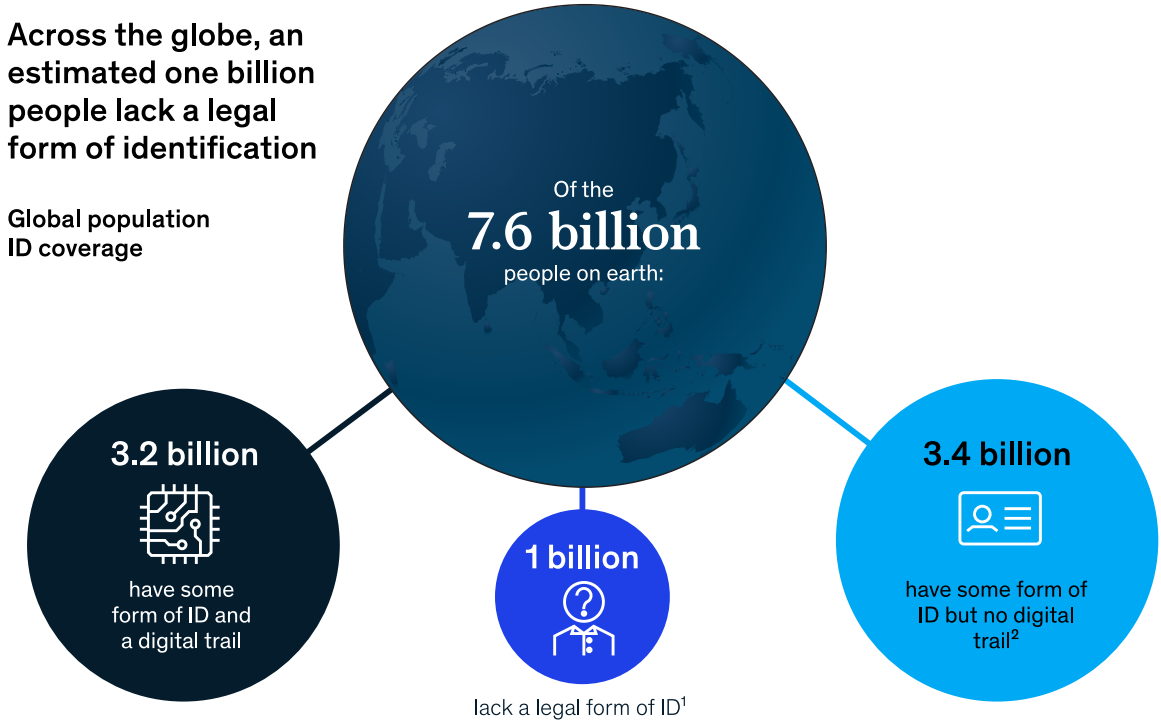
authentication and verification, including biometrics, passwords, QR codes, and smart devices with identity information embedded in them.

- *Unique:* With a unique digital ID, an individual has only one identity within a system, and every system identity corresponds to only one individual. This is not characteristic of most social media identities today, for example.
- *Established with individual consent:* Consent means that individuals knowingly register for and use the digital ID with knowledge of what personal data will be captured and how they will be used.
- *Protects user privacy and ensures control over personal data:* Built-in safeguards to ensure privacy and security while also giving users access to their personal data, decision rights over who has access to that data, with transparency into who has accessed it.

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

According to estimates from the World Bank's ID4D database, almost one billion people globally lack any form of legally recognized identification. An additional 3.4 billion who have some type of legally recognized identification have limited ability to use it in the digital world. The remaining 3.2 billion have a legally recognized identity and participate in the digital economy but may not be able to use that ID effectively and efficiently online (Exhibit 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.

Exhibit 1



[1] Legal ID coverage figures are based upon World Bank ID4D reporting of the latest registration levels for national ID, with voter registration used as a proxy where national ID does not exist or data are not available.
[2] Calculated as population with active social-media use, as reported in the *Global Digital Report 2018* from We Are Social. These social-media users are presumed to be within the population that has some form of legally recognized ID.

McKinsey & Company

Furthermore, 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. 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.

Video

Why is digital ID necessary in India?

So far, the state of adoption of digital ID is mixed, indicating room for improvement and growth. Forty or more national or non-national digital identity programs exist today. Roughly 1.2 billion people with digital IDs live in India alone, registered in the Aadhaar program, which began in 2009. Programs led by banking consortiums have been successfully integrated into financial and government services in Norway and Sweden, and the Estonian e-ID has led a successful transition to e-government services.

“Roughly 1.2 billion people with digital IDs live in India alone, registered in the Aadhaar program.”

Yet many digital ID programs have achieved low coverage levels, with the percentage of the population included as low as single digits. Most enable only a small fraction of the nearly 100 uses we have

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

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

Thoughtful system design with built-in privacy provisions like data minimization and proportionality, well-controlled processes, and robust governance, together with established rule of law, are essential to guard against such risks. To help promote sustainable digital ID systems that minimize risks, the World Bank Group and the Center for Global Development facilitated the development of ten principles on identification for sustainable development, endorsed by many organizations, such as the Bill & Melinda Gates Foundation and Omidyar Network.

Yet even when digital ID is used expressly for creating value and promoting inclusive growth, risks of two major sorts must be addressed. First, digital ID is inherently exposed to risks already present in other digital technologies with large-scale population-level usage. Indeed, the connectivity and information

sharing that create the value of digital ID also contribute to potential dangers. Whether data breaches at credit agencies or on social media, failure of technical systems, or concerns over the control and misuse of personal data, policy makers around the world today are grappling with a host of potential new dangers related to the digital ecosystem. Technological failure could include problems with the functionality of the hardware or software associated with a digital ID as well as infrastructure problems preventing uninterrupted and effective system use.

"By 2025 the global datasphere will grow to 163 zettabytes (one zettabyte is a trillion gigabytes), ten times the level in 2016."

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. In addition, shifting regulations and consumer preferences are placing increasing emphasis on data privacy and control for all digital systems. Examples of new privacy measures include the General Data Protection Regulation in the EU, the California Consumer Privacy Act in the United States, the Data Privacy Act of 2012 in the Philippines, and South Korea's Personal Information Protection Act.

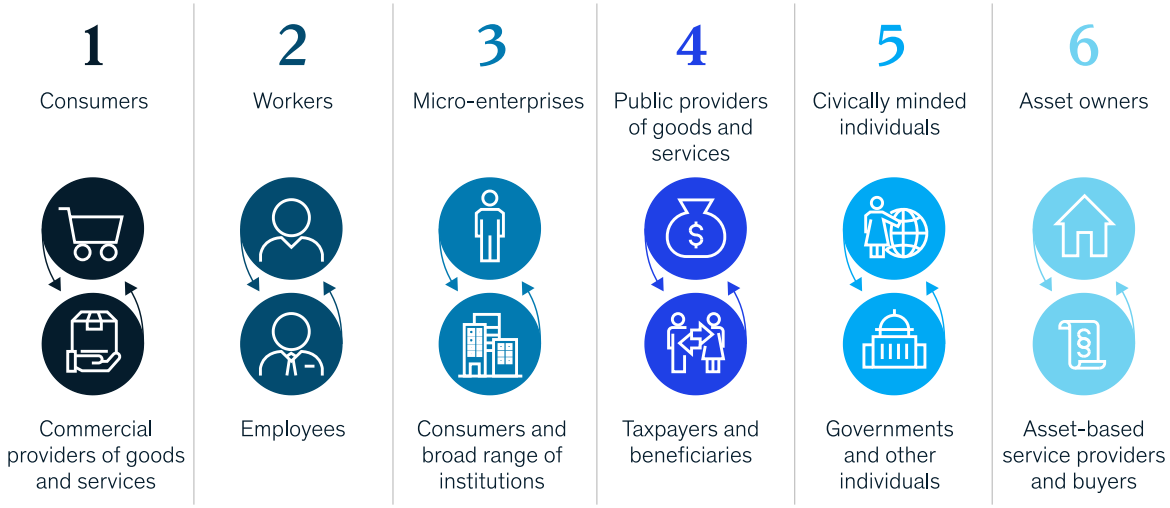
Second, some risks associated with conventional ID programs also pertain to digital ID. They include human execution error, unauthorized credential use, and the exclusion of individuals. Digital ID could meaningfully reduce those risks by minimizing opportunity for manual error or breaches of conduct.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

Individuals 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 2). Correspondingly, institutions can use an individual's identity in a variety of positions: as commercial providers of goods and services, interacting with consumers; as employers, interacting with workers; as public providers of goods and services, interacting with beneficiaries; as governments, interacting with civically minded individuals; and as asset registers, interacting with individual asset owners. In our analysis, we quantify the benefits of digital ID through bottom-up microanalysis of nearly 100 ways of using digital ID, organized by the roles played by individuals and institutions.

Exhibit 2

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

Our analysis examined in detail nearly 100 use cases across six roles



Example use cases associated with each role

- Streamlined registration and authentication
- Secure digital payments
- e-KYC[1] for financial services

- Facilitated talent matching
- Automated background verification
- Efficient payroll services

- Formalized business registration
- High-assurance contracting and transacting

- Streamlined e-government services
- Digital tax filing
- Direct disbursement of government benefits

- Online voting
- Verification of political donations
- School enrollment

- Formalized land ownership
- Facilitated sales and purchases

[1]Know your customer.
Source: McKinsey Global Institute analysis

McKinsey & Company

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. 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.

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

We make a distinction between basic digital ID, which enables verification and authentication, and digital ID with advanced applications, which we call advanced digital ID or advanced ID. Advanced ID enables storing or linking additional information about individual ID owners and thus can facilitate advanced data sharing, with informed user consent. For example, when an individual pays taxes, an advanced ID system would allow the individual to give the tax authority consent to digitally access the relevant bank information, investment accounts, and employment records necessary for filing quickly and without error. Advanced ID programs like these should be designed with principles of data minimization and owner agency in mind. Public and private data aggregators need to protect user privacy and be responsible about the data they collect and process, while owners of data—in this case the digital ID holders—need to be educated and empowered to provide informed consent and exercise control over the use of their data. In many cases, the lines between basic and advanced digital ID may blur because broader digital ecosystems can be built on top of a basic digital ID that enables an underlying ability to authenticate over digital channels.

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

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

- *Addressable share.* This is the share of the economy consisting of those types of interactions that digital ID could improve or, in other words, the bottlenecks that digital ID can address. It is characterized by indicators such as government spending on benefits, overall wages, and healthcare spending. The share of investment-led output, which determines the economic impact of new sources of capital from financial inclusion, also contributes.
- *Potential for value creation.* This is the aggregate potential for greater formalization, inclusion, and digitization. It measures the degree to which digital ID could directly improve economic interactions. It is characterized by indicators such as current levels of coverage of digital and conventional ID, informal share of GDP and of employment, employment level, potential for new deposits and loans from financial inclusion, and fraud rate.

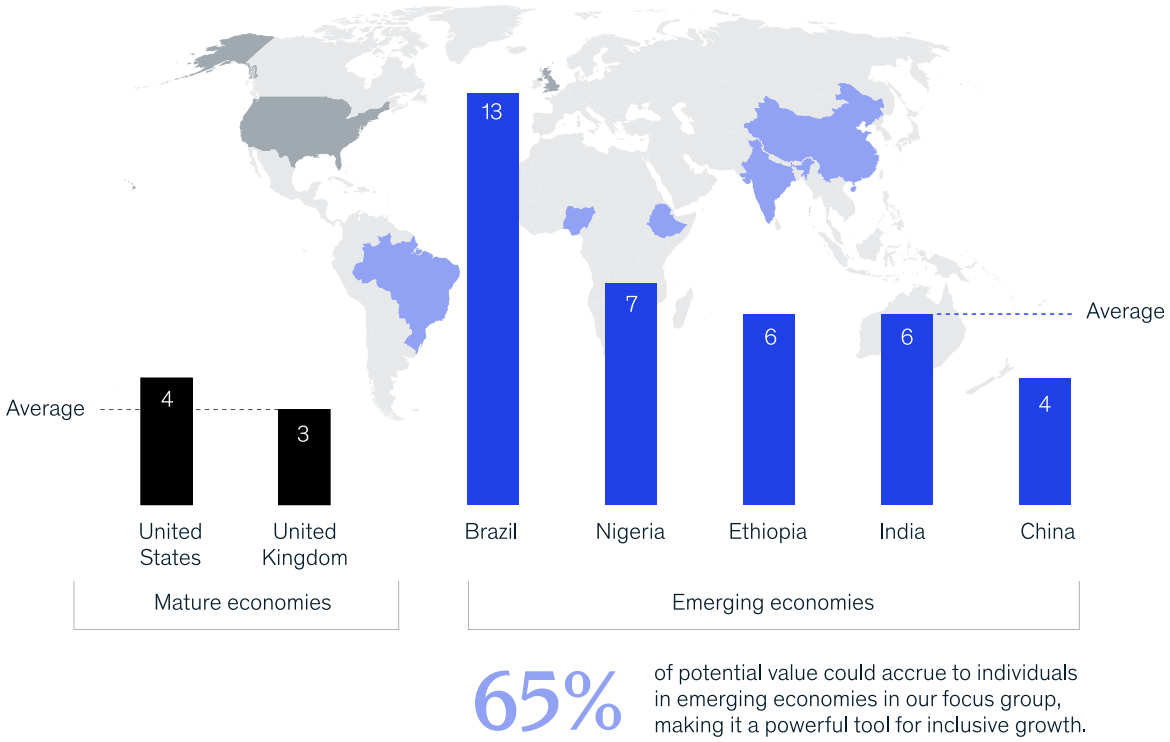
We assess a broader set of 23 countries on the factors that drive potential value from digital ID—addressable share of the economy and potential for improvement in inclusion, formalization, digitization, and ID coverage. Based on country-level patterns of these factors, we develop directional estimates 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 (Exhibit 3). In emerging economies, much of the value could be captured even through basic digital ID with essential functionalities. For mature economies, many processes are already digital and potential for improvement is more limited, necessitating advanced digital ID programs with data-sharing features. Of the potential value, we estimate that in emerging economies, some 65 percent could accrue to individuals, while in mature economies, about 40 percent could flow to individuals.

Exhibit 3

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

Increase in economic value from high levels of digital ID adoption in each country by 2030, % of GDP



65% of potential value could accrue to individuals in emerging economies in our focus group, making it a powerful tool for inclusive growth.

Note: Average is calculated over the range of 23 mature and emerging economies in our analysis. Value estimates assume the digital ID program enables multiple high-value use cases, attains high levels of adoption and usage, and has the attributes required of good ID, including that it is established with individual consent, protects user privacy, and ensures control over personal data.

McKinsey & Company

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.

Digital ID can also help enforce rights nominally enshrined in law. For example, in India, the right of residents to claim subsidized food through ration shops is protected because their identity—and claim—is authenticated through a remote digital ID system, rather than at the discretion of local officials. By providing greater legal protection, digital ID could help in the elimination of child labor and help enforce laws against child marriage. 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.

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

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

Employees at a textile company in Ethiopia check out after work by fingerprint.

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

"Governments, businesses, and civil society actors should think through several important questions as they shape the course of digital ID programs in their countries."

Governments, businesses, and civil society actors should think through several important questions as they shape the course of digital ID programs in their countries. These include how to address potential misuse of the digital ID system, approaches to safeguard user privacy and ensure control over personal data, what may be an optimal approach to system design or a standard that can be developed regardless of varying country characteristics, and how to accelerate implementation and adoption. Some immediate steps that stakeholders can take to help capture the value of digital ID include:

- Governments can consider developing policies and legal frameworks to enable acceptance of digital identities, while protecting user privacy and other rights, collaborating with international bodies to develop cross-border standardization, and partnering with private-sector institutions to understand country-specific economics of digital ID and to explore public-private and consortium-led models of provision.
- Businesses can innovate processes that could leverage digital ID to boost efficiency and improve customer experience, work to facilitate development of global standards, and collaborate with governments to conduct bespoke cost-benefit analysis of digital identity and develop new digital ID programs.
- Civil society institutions could help ensure that individuals capture the value of digital ID while retaining control over how their data are used and also being protected from misuse. For example, they could petition politicians, regulators, and institutions to develop digital ID programs that are safe, accessible, and socially beneficial along with policies that support and foster good digital ID.

Digital ID offers individuals social, civic, and political benefits, from increased inclusion, formalization, and transparency to better control of online data. Designed carefully and scaled to high levels in multiple application areas, it can also create significant economic value, particularly in emerging economies, with benefits for both individuals and institutions. Yet with that potential comes risk from deliberate misuse of digital ID programs by government and commercial actors as well as broader risks common to other large-scale digital interactions, such as technology failure and security breaches.

The design, governance, and use of digital ID is a rapidly evolving area deserving additional research. Topics for further investigation include system design, incorporating features to protect user privacy and ensure fully informed consent both at sign-up and during ongoing usage; economic quantification of risks,

encompassing design decisions and associated costs; relative benefits and downsides of different models for digital ID system governance and ownership—public or private as well as centralized, federated, or decentralized; and continued accumulation of an evidence base documenting benefits by use cases, including the link to specific design decisions and drivers of usage and adoption.

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

How relevant and useful is this article for you?

☆ ☆ ☆ ☆ ☆

ABOUT THE AUTHOR(S)

Olivia White is a partner in McKinsey's San Francisco office, where **Owen Sperling** is a consultant. **Anu Madgavkar** is a partner of the McKinsey Global Institute, where **James Manyika** is a director and chairman, and **Jacques Bughin** is a director. **Deepa Mahajan** is a partner in the Silicon Valley office, and **Michael McCarthy** is an associate partner in the London office.
