Atlantic Council
GEOTECH CENTER

Exploring the global digital ID landscape

Clear leaders, varied paths, and steps to realize their potential

Coley Felt and Will LaRivee

Atlantic Council
GEOTECH CENTER

The Atlantic Council GeoTech Center has a mission to shape the future of technology and data to advance society.

Authors
Coley Felt
Will LaRivee

Program director
Raul Brens Jr.

Cover: IMAGO/Zoonar via Reuters Connect.

Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

Acknowledgments

This report has been made possible by the assistance of the following GeoTech Center staff: Trisha Ray, Ryan Pan, and Marina Meyjes.

Exploring the global digital ID landscape

Clear leaders, varied paths, and steps to realize their potential

Coley Felt and Will LaRivee

Table of contents

Executive summary 2

Introduction 3

Analog identity 3

Identity in the digital domain 4

Government goes digital 4

Common digital ID 5

Benefits of digital IDs 7

Limitations of digital identities 9

Technical limitations 9

Political limitations 9

International coordination 9

Social limitations 10

Governments 11

Private sector 11

Civil society 11

Recommendations for design and implementation 11

Case studies 12

Estonia 12

India 12

African Union 13

EU eIDAS 13

United States 13

About the authors 15

About the program director 15

Endnotes 16

Executive summary

In an increasingly digital world, digital identity systems represent a fundamental transformation in how personal information is authenticated and managed, shifting from traditional physical identification methods to electronic credentials that enable access to digital services across government and private-sector platforms. These systems utilize authenticated credentials that verify individual qualifications and personal information to establish trusted digital documentation, spanning use cases from health certificates to mobile identification for travel security and banking verification.

The worldwide adoption of digital identity systems varies significantly across regions and implementation approaches. Estonia's comprehensive e-ID system, mandatory for all residents, demonstrates transformative societal impact by connecting organizations through distributed databases and blockchain technology. India's Aadhaar program serves a massive population, proving that large-scale digital identity systems can operate in developing countries while bringing previously undocumented populations into formal economic systems, albeit not without criticism. The European Union's eIDAS framework mandates that all member states offer digital identity wallets to citizens and businesses, creating interoperability across member states. The African Union has faced infrastructure and data-protection challenges, while the United States remains fragmented with individual states implementing mobile driver's licenses without federal coordination.

Digital identity systems offer a breadth of benefits including enhanced convenience, improved access for underserved populations, stronger privacy protections through data minimization principles, and significant cost savings for organizations. These systems hold tremendous potential to transform the delivery of government services and industry interactions, though there are potential risks and limitations to be considered.

Despite promising advantages, limitations across technical, political, and social spheres present an array of challenges. Technical limitations include interoperability between different systems, cybersecurity vulnerabilities, and accessibility barriers in regions with limited digital infrastructure. Political obstacles include insufficient regulatory frameworks, lack of adherence to international standards, and coordination issues between jurisdictions. Social limitations center on concerns over public trust, particularly regarding surveillance and privacy, along with unequal access that can further marginalize vulnerable populations including refugees, elderly citizens, and those with limited digital literacy.

Successful implementation of digital identity systems requires coordinated efforts across sectors. Governments must adopt user-first design principles, ensure interoperability through technical standards, tailor systems to local contexts, and establish effective public-private partnerships. Private-sector actors should prioritize transparency, data security, and accessibility while implementing privacy-enhancing technologies. Civil society organizations play crucial roles in public education and representing user interests.

As digital identity systems become the cornerstone of personal identification, effective implementation depends on building systems that genuinely serve user needs while maintaining robust protections against misuse and public trust through transparency and accountability measures, particularly ensuring the protection and well-being of marginalized and disadvantaged populations.

Introduction

Digital transformation has fundamentally altered how individuals interact with governments and businesses worldwide. At the heart of this transformation is the concept of digital identity: the electronic representation of an individual's credentials and authentication information that gives access to digital services. This report explores the global digital identity (ID) landscape, examining the wide-ranging benefits and associated limitations of these systems. Through comprehensive analysis, the report provides practical recommendations to facilitate the widespread adoption of digital ID systems while safeguarding fundamental rights and ensuring inclusive access for all.

Analog identity

Tracing its origin to the Latin *idem*, or "the same," an identity comprises the traits, qualities, behaviors, and choices that define unique individuals, organizations, and entities. These largely static details amassed over time include basic identifiers, demographic information, employment details, and biometrics. Taken together, these data can establish authenticity and verify that a *claimed* entity is "the same" as a *genuine* entity, shaping how it interacts with others in the public sphere. Public and private institutions have traditionally represented these consolidated verification details with *analog*, or nondigital, identities (IDs). These material forms of authenticity include passports, business licenses, and insurance cards that prevent fraudulent activity and enable access to services otherwise unavailable to anonymous entities.

This verification method offers clear advantages of ease of control and challenge of replication. For example, as governments issue just one tourist passport per citizen, travelers can verify that no one else has access while concealing their documents in their possession. Furthermore, while forging a passport may be possible, duplication requires access to an original copy, and the authentic document can be verified with details generally stored in an external database.

However, a physical form of identification also inherently imposes constraints on its effectiveness. It must be physically present to provide its benefits, and one form of identity specific to a single institution may have limited interoperability with other institutions. Again, considering the passport, a traveler must carry their documents with them to cross borders, and a passport booklet may not be accepted as a verification method for other services, such as entering a school facility or a place of employment.

Analog IDs also offer relatively easy vectors for identity theft. Simply by stealing a wallet or a paper file, a thief can immediately access a trove of information. Printed documents lack password protection, biometric verification methods, and multifactor authentication requirements that limit visibility to sensitive details about an entity. A criminal can use all printed information to perpetrate a host of identity theft crimes, seriously disrupting the personal and professional lives of victims.

Furthermore, analog IDs grow increasingly irrelevant as modern societies digitize. Today's public commons have transformed from a physical place of interaction to a network of online connections and engagements. Community gatherings, professional workflows, and financial transactions no longer require participants to occupy the same space, instead connecting individuals, businesses, and devices across the world in real time. Analog IDs cannot establish sufficient authenticity in this domain, and the sensitivity of certain interactions requires a threshold of verification that a physical form of identity cannot provide. To meet this demand, new forms of *digital* IDs offer promising alternatives.

Identity in the digital domain

Identification principles in the digital space largely mirror those in the analog world, where an entity must verify its authenticity with a sufficient combination of unique details.[1] However, in the digital domain, real individuals are not limited to a single digital counterpart; a physical entity may be represented by several discrete digital versions of itself, either in a single database or across multiple systems. While this one-to-many ratio may be exploited with malicious intent, the ability to create multiple digital identities can also prove beneficial, enabling individuals to better organize or protect their digital footprints.

In practice, the process of *creation* and *confirmation* of identity involves six key elements: the user, the identity provider, the service provider, the established identity, the personal authentication device, and the connections between each actor.[2]

To *create* an identity, the user first connects with the identity provider online, which may be internal to the service provider or a third-party identity-as-a-service (IAAS) organization specializing in managing identity data. The user then provides a unique set of attributes to the identity provider to establish an account, which allows the real entity to exist in and interact with other entities online. This combination of attributes is recorded and managed by the identity provider internally in a database or externally through blockchain technology in a process known as identity and access management (IAM).[3]

Next, when a user attempts to access a digital service, the service provider must *confirm* that the attempt is from the genuine user by authenticating from a list of attributes shown in table 1. After verifying that the provided attributes match those stored in the IAM system, the service provider enables access to the user.

This repeatable framework to establish and verify an online persona can be crafted by any digital service provider, such as social media companies, healthcare networks, or e-commerce platforms. The created domain-specific proxy entities within these organizations establish trust between parties, enabling the seamless exchange of information, goods, and services.

Government goes digital

After decades of private-sector digital success alongside sometimes cumbersome public-sector performance, governments and their service providers have begun to transition to digital platforms. From portals for filing taxes to applications for small-business research grants, government agencies have expanded their online offerings to individuals and organizations, streamlining previously clunky and often confusing processes.[4] These systems are far from perfect; bugs and failures do sometimes interfere with critical government functions or necessary assistance. The October 2013 launch of HealthCare.gov famously failed to meet customer requirements, crashing within hours after launch, and only allowing six users to register on the first day.[5] However, the site has since been heavily overhauled, enabling tens of millions of users to register during open enrollment periods each year.[6]

Yet, as with private websites and nondigital service providers, users must still repeatedly expose elements of their personal information to establish accounts, and those accounts are often not connected across government entities, each of which manages their data and digital infrastructures differently. The repeated requirement to release private information in exchange for access is not only a barrier to access, but it also increases exposure to identity theft and fraud.

Table 1. Authentication attributes

Something the user knows	Password, PIN, mother's maiden name
Something the user is	Biometric data (fingerprints, eye scan, etc.)
Something the user has	One-time password, authentication device
Somewhere the user is	Location data for user
A combination of the above	Example: Combination of PIN and one-time password

Source: Jean-Marc Seigneur and Tewfiq El Maliki, "Chapter 17 – Identity Management," in *Computer and Information Security Handbook*, ed. John Vacca (Morgan Kaufman, 2009), 269–292, https://doi.org/10.1016/B978-0-12-374354-1.00017-0.

Still, the potential benefits of digitized public services promise to revolutionize the way governments interact with their citizens, paying dividends through enhanced transparency and public trust, and lowering service delivery costs by up to 95 percent.[7] By leveraging the power of digital connectivity and the quality of available data, public officials can transform their services into faster, safer, and cheaper alternatives for a more inclusive form of governance. To do so, they face the challenge of developing an integrated, streamlined digital infrastructure while sufficiently protecting user data and respecting the rights of individuals.

Common digital ID

Enter the modern *digital ID*. These systems offer a verifiable *one-to-one* representation of a physical identity across a range of digital applications. When sufficiently scaled, this enables a user to seamlessly access and engage with an interconnected network of institutions. In return, those institutions can better trust the authenticity of a user to ensure their services are achieving their desired effect.

The scope of these digital IDs varies widely across a broad range of services. Some systems, such as California's program and several other mobile vehicle license programs in US states, remain limited to few functions, verifying age and address at select businesses and government agencies. [8] Others, such as Estonia's e-ID system, enable access to a comprehensive list of public services, from voting to managing medical prescriptions.[9]

New digital IDs may also pair with analog IDs for a more robust process. Estonia's e-ID system combines a physical ID Card with an embedded SIM chip, a Mobile ID with encryption keys stored on a smartphone, and an online Smart ID system. This diversification allows users to access services virtually or in person, and it also backs up digital systems for cases of reduced or disrupted connectivity.[10]

Table 2. A comparison of digital IDs across selected countries and US states

System Overview		Design and Access				Services										
						Government						Commercial				
Region	Digital ID Concept	Digital/ Physical Twin	System Ownership: Government and/or Commerical	Access	ISO Standard (18013-5)	Birth/ Death Certificates	Tax Filing	Health Services	Voting	Passports	Vehicle Licensing	Bill Pay	Digital Signature	Document Storage	Banking	Education Services
Australia	Digital iD	Yes	Government and/or Commercial	Citizens	No		X	X			X	X	X	X	X	X
Brazil	Gov.br	Yes	Government	Citizens	No	X	X	X		X	X	X	X	X	X	X
Denmark	MitID	Yes	Government	Everyone	Yes	X	X	X		X	X	X	X	X	X	X
Estonia	e-ID	Yes	Government	Everyone	Yes	X	X	X	X	X	X	X	X	X	X	X
EU	eIDAs/eIDAs2/ EUDI Wallet	Yes	Both	Everyone	Yes	X	X	X		X	X	X	X	X	X	X
Finland	e-ID	No	Commercial	Everyone	No	X	X	X		X	X	X	X	X	X	X
India	Aadhaar	Yes	Government	Everyone	No	X	X	X	X	X	X	X	X	X	X	X
Kenya	Maisha Namba	Yes	Government	Citizens	No	X	X	X		X	X					X
Singapore	Singpass	Yes	Government	Citizens	No	X	X	X	X	X	X	X	X	X	X	X
Sweden	BankID	Yes	Both	Everyone	No	X	X	X		X	X	X	X	X	X	X
UAE	UAE PASS	Yes	Government	Everyone	No	X	X	X		X	X	X	X	X	X	X
California	mDL (pilot) / California Identity Gateway	Yes	Government	Citizens	Yes			X			X		X	X		
Colorado	myColorado	Yes	Government	Citizens	Yes			X			X					

Source: GeoTech Center compilation consolidated tab here.

Benefits of digital IDs

The breadth of emerging applications reflects the growing list of benefits that digital IDs offer customers of government services. Digital identities serve as a catalyst for economic growth, a facilitator of more efficient delivery of public services, and a mitigator of fraud and waste. They provide benefits to the entire ecosystem of users from government entities, financial institutions, and individuals.

Linked digital IDs across organizations offer their users the **convenience** of single sign-on (SSO) solutions. Once connected through one service provider, the common identity provider gives the user the freedom to access any of the additional in-network service providers. In the United States, the ID.me service already connects a host of federal agencies, including the Department of the Treasury and the Department of Health and Human Services, as well as several state-level government agencies and private retail companies.[11] Where once a user would have had separate accounts for applying for Veterans Affairs benefits and filing tax returns, they can now access all services under a single profile.

Modern digital IDs also improve **access** to public and private services for a broader audience. An estimated 850 million people worldwide lack an official form of documentation, a limitation most concentrated among lower-income countries in sub-Saharan Africa and South Asia.[12] Unable to easily authenticate their identity, these individuals struggle to attain government financial assistance, participate in elections, or apply for higher education. They may also lack bank accounts, requiring them to carry cash to complete transactions and contribute to commercial growth. As connectivity spreads across these regions, digital registries enable previously excluded populations to participate in a broader public sphere, with the potential to boost the gross domestic products (GDPs) of these states by 3 percent to 7 percent by 2030.[13]

Similarly, digital IDs may also improve **inclusion** for noncitizens living abroad. India's Aadhaar system allows foreign nationals living in the country for more than 182 days—and with a valid passport and Indian visa—to enroll with the Unique Identification Authority of India.[14] This capability allows visitors to more easily work with Indian financial institutions and telecom providers, streamlining business practices and improving services for visitors.

Vastly improving on analog identification methods, digital systems can strengthen the **privacy** of individuals, protecting against identity theft and allowing individuals to control the release of personal information. A digital identity reduces the need to carry multiple cards or papers to prove authenticity, consolidating those documents into an easily managed single digital wallet. Within that wallet, access to key identification data generally remains further protected behind passwords, biometric scans, or other verification measures that physical cards cannot provide. Furthermore, these wallets may also offer users the benefits of self-sovereign identity, giving them the control to limit which details are displayed to each viewer. Self-sovereign identity embodies the concept of data minimization,[15] and technologies supporting selective disclosure will allow data to be shared in a privacy-preserving manner. For example, an individual may choose to release just verified birthdate and employment information when applying for a job, while protecting other sensitive details. These measures prevent unnecessary and unintended exposure of identifying features that could be exploited or cause personal harm.

Emerging privacy-enhancing technologies

The growing list of privacy-enhancing technologies (PETs) includes several less-common technologies that promise to improve the security and control of digitized personal data.

Zero-knowledge proofs (ZKPs) confirm whether an asserted fact is true or false rather than revealing the fact to a viewer. Such a system can be used to verify age for voting systems or income for rental applications without exposing a precise birthday or income amount.

Multiparty computation (MPC) methods enable several entities to jointly use data for computation while eliminating the need for an additional party to use and verify the data's accuracy. This process reduces the exposure of specific data while enabling entities to generate insights from that data. Variants of these technologies were used for COVID-19 exposure notification measures based on location proximity and contact data without revealing the identities of specific individuals.

Blockchain systems and other *distributed ledger technologies (DLTs)* can improve data accountability by preserving a public record of previous instances of access, transfer, and processing. While the public nature of DLTs can expose data to new privacy risks, their decentralized nature can improve data governance and compliance if combined with other PETs.

Digital authentication systems also improve the **security** of identity management, which better protects the information stored in consolidated databases. Paper registries remain vulnerable to duplication, forgery, loss, and theft. If digitized in a properly designed database, personal information may be better sustained and protected through encryption, the integration of decentralized blockchain systems, and other privacy-enhancing technologies (PETs).[16] Not only do advanced databases improve security, but the user's ownership of their personal data reduces the need for companies to store as much personal information as had been the case.

These digital ID systems can greatly improve organizational **efficiency**, saving time and money for public and private institutions. Estonia estimates that its e-governance processes save more than 1,400 years of working time annually, as 99 percent of government services are available online twenty-four hours a day.[17] This access streamlines organizational flows and builds trust with users who increasingly see government institutions as working for them.

Finally, if regionally standardized, digital IDs can serve as **catalysts for economic growth**. Commonly accepted frameworks allow users to seamlessly access foreign goods and services while offering businesses international market access beyond borders. The EU's Digital Identity Wallet should offer both demand- and supply-side benefits for transactions between individuals and institutions.[18] For example, the system will allow EU citizens to seamlessly access medical prescriptions abroad and open bank accounts in non-native countries. Simultaneously, it will enable businesses to easily seek foreign funding and sell products safely and securely to customers across borders. This ease of transactions promises to boost regional commerce and improve international competitiveness for countries with such systems.

Limitations of digital identities

While digital identity systems offer numerous benefits, several technical, political, and social limitations still hinder their adoption and effectiveness.

Technical limitations

Digital ID systems often target specific services and platforms and are frequently developed in silos, creating **interoperability problems**. Not only do bespoke systems present interoperability challenges within local systems, but they also create limitations for collaboration across governments. The absence of unified infrastructure and common dataset architectures makes it difficult for partnerships across services, sectors, and jurisdictions. Worse, the varied technological infrastructure, data-collection methods, and standard limitations can lead to security gaps and reduced reliability within systems.

Cybersecurity vulnerabilities also present their own set of risks to digital ID systems. The centralized nature of some of these massive databases makes for attractive targets for cyberattacks. Data breaches can expose large amounts of sensitive, personal information, which can lead to identity theft, financial fraud, and other privacy violations. Moreover, emerging technologies such as artificial intelligence and machine learning are creating further cybersecurity liabilities, as advanced deepfake techniques and social-engineering strategies present new avenues to bypass traditional identity-verification methods with alarming precision. As digital identity systems become increasingly interconnected and comprehensive, the stakes of a single security breach escalate dramatically—a successful intrusion could now expose extensive personal data across multiple platforms and services. Another technical limitation of digital ID systems is **accessibility**. Rural and developing regions may be limited by the digital infrastructure available to develop, utilize, and maintain these systems, so these e-government programs run the risk of systematically excluding populations with restricted digital access.

As a result of limited digital infrastructure, particularly in developing regions, public trust concerns over privacy and data control have become significant. The technical challenges of maintaining secure, reliable identity systems across areas with spotty telecommunications coverage and frequent power outages undermine citizens' confidence in these programs. Even in places like rural India, where Aadhaar has been implemented, inadequate digital infrastructure leads to authentication failures that prevent people from accessing essential services, eroding trust in the system. Without addressing these fundamental infrastructure gaps, governments will continue facing skepticism from citizens who experience digital ID systems as dysfunctional rather than enablers of efficient, trusted services.

Privacy risks stretch beyond simple data collection to the potential for comprehensive personal profiling and unintended data sharing. Many digital identity systems link multiple databases, creating the potential for creating digital profiles that can track an individual's interactions across government services, financial institutions, healthcare providers, and other critical sectors. There's a fundamental tension between the efficiency these systems promise and the potential for systemic privacy erosion. The main problem is the balance between making things efficient and protecting personal privacy. These systems promise to simplify our lives, but they can also take away our freedom to keep parts of our lives private.

Political limitations

Governments play a crucial role in shaping environments for digital ID systems to meet the needs of their users. Several national and political factors of poorly designed state systems may prevent digital ID frameworks from providing their intended services to the public.

A successful digital ID system must be built atop an effective national regulatory framework, providing sufficient oversight, transparency, and stakeholder engagement. However, the rapidly evolving nature of modern technologies challenges legislators' abilities to keep pace with effective governance, and many countries **lack sufficient regulatory frameworks** for consumer protection and accessibility. The lack of sufficient data privacy rules may inhibit the integration of digital IDs, as potential users believe their data would be exposed to theft and exploitation. Additionally, an absence of cybersecurity requirements could limit the willingness of organizations and individuals to join integrated systems, where their data may be exposed at different levels across multiple systems. Furthermore, weak requirements for accessibility could limit digital inclusion of all populations, further isolating and marginalizing disadvantaged and rural populations. Digital ID systems are built on trust, and a lack of sufficient regulatory structures can prevent that trust from taking root.

Limited adherence to technical standards can also prevent the development of an effective system at the national level. Standards from the International Organization for Standardization, like ISO 18013-5 (for driving licenses), can establish common baselines for system design and use, but many governments do not take sufficient measures to incentivize or mandate their adoption. The lack of adherence to a shared technical framework can prevent sufficient interoperability, result in uncertain levels of cybersecurity and data privacy, and significantly complicate the process of updating and modernizing outdated systems. Critically, this results in a disjointed system that is challenging and opaque for users, limiting their understanding of and trust in the system.

International coordination

While international standards exist, global adoption remains uncoordinated. Digital IDs present a complex landscape of geopolitical risks, and without the implementation of consistent international standards, the centralization of personal data around the world poses significant potential for control, surveillance, and human rights abuses. In October 2023, the United Nations Development Programme (UNDP) released its Model Governance Framework for Digital Legal Identity System.[19] The model was created as a resource for government and civil-society actors aimed at developing rights-based, inclusive digital ID systems. In addition to UNDP's framework, the Organization for Economic Co-operation and Development (OECD) released its Recommendation of the Council on the Governance of Digital Identity in August 2023.[20] Similarly, the recommendation aims to ensure that digital identity is reliable, secure, and accessible, and that it respects human rights and democratic values. While these initiatives are valuable, they have limitations as insufficient governance frameworks, including the lack of enforcement mechanisms, concrete guidance on balancing privacy protections, guidelines for cross-border interoperability, and regulation on public-private partnerships.

Moreover, the global implementation of digital ID systems can create geopolitical tensions as countries with various privacy standards might be encouraged to adopt regulations that fundamentally challenge their sovereign approaches to personal data and human rights. Thus, the enforcement of robust international guidelines that consider sovereign norms but also ensure safe and responsible use of digital ID systems is crucial to widespread adoption.

Social limitations

In addition to necessity and usability, the adoption of digital ID systems is fundamentally limited by public trust. The user must believe that they will gain the benefits offered by the system while remaining protected by specific design and regulatory measures.

Most immediately, community-level concerns over surveillance and privacy violations prevent users from opting into the systems. Personal data will not be voluntarily given up if there is no trust in the system, and if governments are not transparent about the mechanisms used for the collection, storing, and handling of personal data, misinformation can further generate public trust concerns. Digital education is a critical component of building this trust, giving individuals the ability to understand how their data is used and equipping them with skills to mitigate misinformation and disinformation. Regional and generational disparities in digital skill levels can complicate public outreach efforts, so countries with large digital divides and older populations may struggle to build trust with their users.

Potential users may **lack a clear understanding of the benefits** of enrolling in and utilizing government-owned digital ID systems, and this lack of understanding further limits public-private trust. Historically, individuals have exhibited a greater willingness to entrust "big tech" firms with their data, in large part due to the tangible benefits offered by those companies. Users may feel inclined to skim or blindly agree to lengthy privacy policies required for online media or commerce services due to their expectation for rapid gratification from their products. The benefits of sharing personal data with the government, however, may not necessarily appear as clear, so citizens may be less likely to volunteer their data to state-run databases.

Moreover, the collection of biometric data presents risks to security, equality, and public trust. Biometric measurement systems, while advanced, can be compromised by malicious actors, and the features they use to verify identities cannot be changed like usernames or passwords. Once exposed, these fundamentally personal details can be repeatedly exploited. Furthermore, facial recognition technologies demonstrate significant error rates, particularly for marginalized populations, leading to potential misidentification and systemic discrimination. Algorithmic biases in biometric collection run the risk of widening privilege gaps, enabling easy access for some while creating artificial barriers for others. Digital ID systems built on biometric recognition can enable unprecedented government and institutional surveillance, transforming identity verification mechanisms into tools for social control, used by authoritarian regimes to track, monitor, and suppress their citizens.

Finally, digitizing personal identities can create many risks for marginalized communities. Systematic exclusion exists for refugees and migrants who have limited or no documentation. There are technological access disparities in the form of limited infrastructure in underserved communities, inadequate digital literacy education, and economic barriers to technology access. In addition to identification and technological challenges, communities may face discrimination in the form of biometric verification failures, such as algorithmic biases and systematic profiling. These risks could increase social marginalization and inequities across many communities.

Recommendations for design and implementation

Despite these challenges, existing digital identity systems in economies at different stages of development demonstrate the real potential for such projects to improve modern societies. However, governments, private firms, and civil society organizations must take several deliberate steps to fully materialize the benefits of these systems.

Governments

The role of governments is to implement a regulatory framework that accepts and legally recognizes digital IDs through incentives and penalties that can be enforced for all actors in the system. Public entities must approach each digital identity project with a **user-first mindset**, designing their systems around the needs, priorities, and concerns of intended individual and organizational customers. Identity databases and applications must be built to enable or improve specific services for the entirety of the public, establishing clear incentives for adoption. Associated IAMs must be designed specifically to preserve and protect user data, provide full data sovereignty to intended customers, and implement strict redress mechanisms to prevent and remedy data breaches. Registration and usage interfaces must be accessible and understandable to ensure systems are accessible to the widest possible audience. Furthermore, policymakers should establish regular public engagement and feedback mechanisms to provide users with the ability to ensure new systems meet their needs.

Governments must **ensure interoperability** between agency applications to break down silos and expand usage across public services. This process begins with the establishment and adherence to standards for data management and usage. From these standards, Governments must also craft a baseline digital public infrastructure stack, such as the India Stack, aligning approaches from common identity, payment, and data-transfer architectures.[21] With these frameworks in place, individual organizations can design bespoke applications to meet their individual needs.

Identity frameworks must be **tailored to local needs**, considering the unique socioeconomic requirements of their populations. One of the primary reasons citizens will adopt a digital identity is that it makes their interactions with the public and private sectors easier. If there is no benefit to the end user, this can be a major block to adoption. Hybrid analog and digital systems should be integrated, such as in Estonia's e-ID ecosystem, to ensure customer access across connectivity and digital literacy spectrums.[22] Public officials must expand in-person registration opportunities, particularly to areas of low broadband coverage, via regional satellite sites and pop-up offices. They must also recognize and adapt to levels of public trust in institutions. Particularly when operating in cultures with lower faith in government, developers must take an incremental and flexible approach to integrating their systems, clearly demonstrating benefits, acknowledging challenges, and responding directly to public concerns and feedback with real changes.

Finally, government officials must design **public-private partnerships** to leverage commercial expertise for their identity frameworks. Technology companies around the world retain the advantage in talent and capacity for developing digital systems, but policymakers must still shape permissive conditions for that development and ensure systems are designed in alignment with societal priorities and values. Governments should establish sufficient financial incentives, such as grant programs for standards compliance, and establish legal protections for digital identity firms. They should also prioritize the interests of intended users, requiring legal protections for their rights and opportunities for feedback. These integrated partnerships can be used to accelerate the proliferation of safe and ethical digital identity systems.

Private sector

Companies must also adopt a **user-first approach**, both prioritizing the needs and recognizing the abilities of their intended customers. Firms should engage with private individuals to ensure they understand the public's perspectives on digitizing identity and the spectrum of digital literacy skills. They should design their systems with data security as the top priority, leveraging PETs and blockchain techniques to protect user information and maximize data sovereignty. They should also employ data minimization principles, limiting access to and transfer of sensitive data to only those qualified and necessary to provide essential services. Furthermore, companies should prioritize accessibility, maximizing opportunities for all citizens to enroll in and utilize digital identity ecosystems.

Private firms must design their systems to maximize **transparency** for intended stakeholders. Users must understand who has access to each element of their identity, what that data can be used for, and how it is stored and transferred in the identity-management process. Agencies and institutions using digital identity must know where the information comes from to trust its source and verify its authenticity. Governments must have oversight of each step in the data custody chain to confirm the protection of their citizens' information and provide guidance to maximize adoption and improve public trust. Such an open process would help incentivize participation to increase and accelerate access to services.

Civil society

Organizations in the space between the public and private sectors must work to **educate the public** on the promise of digital identity systems, clearly articulating their benefits while addressing their risks. Nonprofit organizations should work to identify local perspectives, address knowledge gaps, and correct misperceptions regarding digital identities. These efforts can help create a more informed public, better prepared to meaningfully contribute to debates on the design and usage of digital identities.

These teams should also **represent user equities** through independent advisory roles in the development of identity frameworks. Civil society groups provide the unique ability to leverage the combined expertise of thought leaders in academia and industry while remaining intellectually independent. Organizations can then contribute these perspectives to critical conversations via their access to policymakers and networks of subject matter experts.

Case studies

Estonia

Estonia presents itself as a unique but crucial use case for understanding the development and adoption of digital ID systems. Now considered one of the most digitized, transparent, and least corrupt countries in the world ,[23] Estonia took a new path to digitizing its society. With a population of only 1.3 million,[24] the goal for Estonia's centralized digital ID system was to provide services to all citizens, not only those fully integrated into digital society. Introduced in 2002, e-ID has now operated successfully for more than twenty years.[25] The e-ID data kept by the Estonian government is distributed across interoperable databases and connects almost 700 organizations and public-sector entities[26] to avoid a single contact point. The data is also decentralized and backed up through a data embassy,[27] a data center located in Luxembourg under the "Tier 4" level of security—the highest level for data centers. Established in 2017, this Estonian-owned data center located outside its territorial borders has the same rights as a physical embassy, such as immunity. This innovative concept of duplicative and distributed data limits the impact of a potential data breach and is secured against spoofing attacks with blockchain technology.

Estonia's Identity Documents Act requires all residents to have a digital ID (e-ID), mandatory at age fifteen. The e-ID uses two personal identification numbers—one for identity verification and one for legally binding e-signatures—and integrates with banking (nearly 99 percent[28] of Estonian banking is online), loyalty programs, and health insurance. This comprehensive system earned Estonia a 74.2 percent score[29] on the OECD's 2023 Digital Government Index, well above the 60.5 percent average.

However, Estonia's e-ID has attracted criticism. A 2017 security lapse signaled the risk of reliance on the technology, resulting in the Estonian government removing security access for almost 800,000 affected identity cards. Users were forced to update their digital security certificates and while there was no known data theft, the security flaw had the potential to expose a citizen's full identity, allowing bad actors to access hundreds of public- and private-sector services. This incident raised concerns around Estonia's reliance on e-ID and the severe consequences of a data breach.

Estonia also launched e-Residency in 2014,[30] offering transnational digital identity verification to access EU business services online. This has created an attractive ecosystem to start and run location-independent EU companies entirely online, expanding market access for companies. The program generated €31 million[31] for Estonia's economy in the first half of 2024 alone, with over 120,000 e-residents and 33,000 companies by the end of 2024.

Estonia's success is largely due to the country's high level of digital literacy, as the government has mandated technology and computer skills be taught in schools from an early age.[32] This ensures that citizens understand how to access e-services—including filing taxes, voting in federal elections, viewing healthcare records—and that they trust that the system will protect their data and successfully deliver on its promises. Estonia's e-ID currently serves as the gold standard for safe, secure, and effective digital ID systems.

India

Launched in 2009 by India's Unique Identification Authority (UIDAI),[33] Aadhaar is the world's largest digital ID program with over 1.3 billion enrollees as of September 2023. The system assigns a unique twelve-digit number linked to biometric and demographic data. UIDAI partnered with private companies to establish enrollment centers nationwide, registering 600 million Indians in the first five years,[34] while also preventing duplicates through biometric verification.

Aadhaar has been transformational for marginalized Indians who previously lacked formal documentation. Before the program, many rural Indians couldn't leave their villages, rent housing, or open bank accounts due to missing identity papers—over a third lacked birth certificates before 2010.[35] Aadhaar, which translates to "base" or "foundation" in English, at its core was developed as a foundation for the improvement of economic and social lives of Indians.[36] As of 2023, more than 93 percent of the population is registered,[37] with Aadhaar serving as the foundation for economic and social participation.

The Aadhaar system provides a model for other developing countries seeking to adopt a similar digital identity system. Contrasting with other systems, which primarily focus on digital authentication, the Aadhaar system is primarily designed as a tool for social inclusion. Millions of underprivileged Indians now receive benefits and subsidies *directly* because of welfare programs linked to Aadhaar.[38] However, Aadhar has also faced criticism for further marginalizing populations in rural and remote areas due to unreliable internet connectivity, electricity blackouts, and faulty biometric scanners at service delivery points.

Nevertheless, Aadhaar has integrated the unbanked into the formal financial system, allowing more than 523 million bank accounts to be opened.[39] The program does face significant security challenges: In November 2017, more than 200 official government websites[40] accidentally exposed 130 million Aadhaar numbers and personal data.[41] This security flaw is not unique—app-based errors, third-party leaks, and duplicate Aadhaar cards are just some of the criticisms of India's Aadhaar program.

In response to these criticisms, the UIDAI released a two-tier security system[42] in 2018 to increase the privacy and security of Aadhaar numbers. The measure introduced a temporary sixteen-digit number, the virtual ID, for every Aadhaar user that allows authentication without using their actual twelve-digit number. In addition to the virtual ID, the creation of a "limited know-your-customer (KYC) service" prevents agencies from collecting Aadhaar numbers. More recently, to better secure biometric authentication processes, the UIDAI launched an AI-enabled mechanism in 2023,[43] enabling more comprehensive fingerprint verification. The security method confirms the liveness of the collected fingerprint, reducing the potential for spoofing attempts. Following years of negotiations, India passed its first cross-sectoral law on personal data protection,[44] the Digital Personal Data Protection Act, in 2023. The act requires individual consent prior to the processing of personal data and provides the user with "the right to access, correct, update, and erase their data." However, the law lacks a strong regulator and exempts the government from privacy regulations, undermining its effectiveness.

Despite criticisms, Aadhaar demonstrates successful large-scale digital ID implementation in communities with limited digital integration, revolutionizing e-government access for marginalized populations while highlighting the need for robust security frameworks and comprehensive regulations.

African Union

African Union member countries agree[45] that an interoperable digital ID is essential for the smooth movement of people, goods, and services across the continent. However, effective data-privacy frameworks must be established first to protect user data and build public trust.

The rollout of Kenya's digital ID, the Maisha Namba, has been halted numerous times[46] due to its noncompliance with the country' Data Protection Act of 2019. Critics argued the Maisha Namba was unconstitutional and posed potential human rights violations.[47] Though the ban was lifted in August 2024, the legal battle created a backlog affecting more than a million applicants and demonstrates the crucial role data-protection frameworks play in digital ID adoption.

South Africa exemplifies a better approach by revising identification laws while developing its digital ID. The draft National Identification and Registration Bill of 2022 aims "to establish a single, inclusive and integrated national identification system for South Africa applicable to citizens, residents and foreigners,"[48] while ensuring third-party data sharing complies with the Protection of Personal Information Act of 2013. However, frameworks must be developed with interoperability in mind, as different national approaches create both technical and governance challenges across the continent.

In an effort to increase technical and legal interoperability across Africa, Estonia has partnered with countries on numerous cooperative initiatives. The opening of Enterprise Estonia's trade office[49] in Kenya facilitates investment by Estonian companies in the nation's public and private sectors. In Namibia, Cybernteica, an Estonian information technology company, has partnered with the Namibian government[50] to implement the Nan-X system, enabling e-government capabilities and interoperability. Namibia is developing its technical infrastructure first, which will make it easier to share data across ministries, agencies, and departments, as well as with the private sector—enabling interoperability. In terms of Namibia's laws, the draft Data Protection Bill[51] aims to serve as the first comprehensive data privacy legislation.

The primary barriers to wider digital ID adoption across Africa are inadequate digital infrastructure and insufficient data governance frameworks. Digital ID systems cannot operate without proper infrastructure, and user data should not be collected without means of privacy protection. Through partnerships like those with Estonia, African countries can simultaneously develop robust infrastructure and regulations to increase both adoption rates and continental interoperability.

EU eIDAS

Implemented in 2014, the European Union's Electronic Identification, Authentication and Trust Services (eIDAS) regulation[52] creates a standardized, secure, and interoperable framework for digital identification and transactions across EU member states. eIDAS aims to eliminate digital barriers between countries and facilitate seamless cross-border digital interactions for citizens, businesses, and government entities.

The latest update, eIDAS 2.0,[53] addresses accelerated technological innovation and the shift toward digital-service delivery by introducing the European Digital Identity Wallet.[54] With the aim of simplifying verification processes, eIDAS 2.0 also highlights interoperability among member states for a consistent digital market. The EU Digital Wallet Consortium is a public-private joint venture[55] focused on leveraging the benefits of this wallet. Member states must fully implement digital identity wallets by 2026, adhering to the existing eIDAS guidelines.

Unlike India's centralized Aadhaar system, eIDAS establishes a collaborative framework where each member state develops its own electronic identification systems while ensuring mutual recognition and compatibility. Citizens can use their national digital identities to access public services in other EU countries such as remotely submitting tax declarations, enrolling in universities, opening bank accounts, and completing administrative procedures. For businesses, the regulation simplifies cross-border digital transactions through consistent legal frameworks for electronic identification and trust services. Furthermore, the European Digital Identity Wallet will harmonize standards and processes, reduce costs, and enhance security and privacy protections across the EU, promoting digital innovation and economic integration.

United States

While the United States lacks a national digital identity program, a growing number of states are embracing mobile driver's licenses (mDLs). Louisiana introduced the first digital ID in the United States in 2018, enrolling 66 percent of eligible adults by 2023.[56] By August 2024, fifteen states and Puerto Rico had mDL programs, with eleven more states and Washington, DC planning similar initiatives. Current uses are limited to select identification processes and Transportation Security Administration verification at certain airports, though states plan expanded applications in travel, banking, and government services. With the enforcement of the REAL ID beginning on May 7, 2025, four states have received wavers for their mDLs, authorizing residents of those states to continue to use their mDLs at participating airports[57].

The National Institute of Standards and Technology (NIST) released Digital Identity Guidelines in 2004,[58] outlining technical requirements for federal agencies to employ digital ID

services. However, NIST's guidelines serve as standards, not law. Bills aiming to establish a government-wide approach to digital identity improvement (by creating an Improving Digital Identity Task Force within the Executive Office of the President) were introduced in the 118th Congress in the US Senate[59] and the House of Representatives.[60] The Senate Homeland Security and Governmental Affairs Committee referred an amended bill to the full Senate in 2023; in the House, the bill was referred to the Committee on Oversight and Accountability in 2024. Neither version of the Improving Digital Identity Act received a floor vote. To date, the legislation has not been reintroduced in the 119th Congress.

These recent efforts to establish federal regulation around the adoption and use of digital IDs in the United States demonstrate the importance of standards to ensure interoperability across the country. Because these mobile driver's license systems are developed and operated by the private sector, it is critical that the federal government implements regulation to foster safety and compatibility.

About the authors

Coley Felt is an assistant director at the GeoTech Center where she contributes to projects at the intersection of geopolitics and emerging technologies. Prior to joining the Atlantic Council, she earned a master's degree in global security with a concentration in cybersecurity at Arizona State University where she researched international technology policy and disinformation. Felt is proficient in Spanish and her areas of interest include artificial intelligence, the Internet of things, and data ethics.

Felt holds a bachelor's degree from the University of Washington where she completed undergraduate research focused on artificial intelligence and the future of warfare and studied international relations and Spanish.

Will LaRivee is a resident fellow at the Atlantic Council's GeoTech Center, where he researches the interplay between international security issues, global political currents, and the technology frontier.

Prior to joining the GeoTech Center, LaRivee served as a strategic planner at Headquarters Air Force, where he managed portfolios for manned and unmanned combat aircraft. He is a graduate of the Air Force Fighter Weapons School. He has served operational tours flying F-22s in Alaska and Hawaii, where he integrated joint US capabilities with Indo-Pacific allies and partners.

LaRivee holds a master of arts in security studies from Georgetown University's School of Foreign Service and a bachelor of science in economics from the US Air Force Academy.

About the program director

Raul Brens Jr. is director at the GeoTech Center, part of the Atlantic Council Technology Programs. In this capacity, he is responsible for directing the center's research, strategy, program development, and policy implementation in science and technology. As a former diplomat, he brings nearly two decades of combined expertise in science and technology research and policy and international diplomacy. Before joining the Atlantic Council, Brens had a career in academia and the public sector, focusing on science and technology policy, research, and development, and social- and health-policy issues.

Brens has made significant contributions to public policy efforts in the United States and Australia, particularly in projects aimed at assisting vulnerable social groups and employing emerging technologies to combat climate change and tackle other societal challenges. He previously served as an international affairs advisor to the under secretary and chief scientist at the US Department of Agriculture, where he worked on international science and technology research, development, and research security, focusing on climate and food security issues.

Brens also served as a diplomat at the US Department of State, working on international security, nuclear nonproliferation, nuclear energy, nuclear cooperation, and management of the nuclear fuel cycle issues. He has led large-scale projects bridging data divides within the federal, state, and territory governments of Australia to draw data-driven insights into vulnerable cohorts and improve service delivery, earning recognition from the United Nations Convention on the Rights of Persons with Disabilities.

At the outset of his career, Brens conducted interdisciplinary research in earth and atmospheric sciences as a research scientist. His work included research and development in Australia's agricultural sector, specifically aimed at mitigating greenhouse gas emissions through the adoption of cutting-edge technologies. Brens is also a former science and technology policy fellow with the American Association for the Advancement of Science. Alongside his extensive academic achievements, Brens is fluent in Spanish. He holds PhD and MSc degrees in geosciences and geochemistry and a bachelor's degree with a dual major in earth sciences and history, with a focus on international relations.

Endnotes

1 Juanita Blue, Joan Condell, and Tom Lunney, “A Review of Identity, Identification and Authentication,” *International Journal for Information Security Research* 8, no. 2 (2018): 795, https://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-8-2018/A-Review-of-Identity-Identification-and-Authentication.pdf.

2 Jean-Marc Seigneur and Tewfiq El Maliki, “Chapter 17 – Identity Management,” in *Computer and Information Security Handbook*, ed. John Vacca (Morgan Kaufman, 2009), 269–292, https://doi.org/10.1016/B978-0-12-374354-1.00017-0.

3 Blue, Condell, and Lunney, “A Review of Identity,” 799.

4 “E-file Options to File Your Return,” US Internal Revenue Service, last modified October 28, 2024, https://www.irs.gov/filing/e-file-options; and “America’s Seed Fund,” US Small Business Administration, https://www.sbir.gov/.

5 “The Failed Launch of www.HealthCare.gov,” Harvard Business School, November 18, 2016, https://d3.harvard.edu/platform-rctom/submission/the-failed-launch-of-www-healthcare-gov/.

6 “Marketplace 2024 Open Enrollment Period Report: Final National Snapshot,” Centers for Medicare & Medicaid Services, January 24, 2024, https://www.cms.gov/newsroom/fact-sheets/marketplace-2024-open-enrollment-period-report-final-national-snapshot.

7 Paula Algarra et al., “How Digital Technology Can Delivery Government Services More Cost Effectively,” Inter-American Development Bank, March 30, 2023, https://blogs.iadb.org/ideas-matter/en/how-digital-technology-can-deliver-government-services-more-cost-effectively/.

8 “Mobile Driver License,” American Association of Motor Vehicle Administrators, https://www.aamva.org/topics/mobile-driver-license#?wst=d5a5f5751f7474b62a5bb2b374692b61.

9 “e-Identity,” e-Estonia, Accessed November 2024, https://e-estonia.com/solutions/estonian-e-identity/id-card/.

10 “e-Identity,” e-Estonia.

11 “About Us,” Id.me, Accessed November 2024, https://id.me/.

12 “Identification for Development Global Dataset,” World Bank, Accessed November 2024, https://id4d.worldbank.org/global-dataset.

13 “Digital ID to Unlock Africa’s Economic Value if Fully Implemented, Say Experts,” United Nations Economic Commission for Africa, February 20, 2024, https://www.uneca.org/stories/digital-id-to-unlock-africa%E2%80%99s-economic-value-if-fully-implemented%2C-say-experts.

14 “I Am a Resident Foreign National, Can I Enroll for Aadhaar?,” Unique Identification Authority of India, Accessed November 2024, https://uidai.gov.in/en/circulars-memorandums-notification/296-english-uk/faqs/enrolment-update/aadhaar-enrolment-process/16483-i-am-resident-foreign-national-can-i-enrol-for-aadhaar.html.

15 “What is Data Minimization and Why is it Important?,” Kiteworks, Accessed June 23, 2025, https://www.kiteworks.com/risk-compliance-glossary/data-minimization/

16 “Emerging Privacy-enhancing Technologies,” Organisation for Economic Co-operation and Development (OECD), March 8, 2023, https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html.

17 “e-Governance,” e-Estonia, Accessed November 2024, https://e-estonia.com/solutions/e-governance/government-cloud/.

18 “European Digital Identity,” European Commission, Accessed November 2024, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en.

19 “UNDP Model Governance Framework for Digital Legal Identity System,” United Nations Development Programme Digital Legal ID Governance4ID, in collaboration with Norwegian Ministry of Foreign Affairs, (Accessed November 2024), https://www.governance4id.org/.

20 OECD, Recommendation of the Council on the Governance of Digital Identity, OECD/LEGAL/0491, Accessed November 2024, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491.

21 Sreevas Sahasranamam and Jaideep Prabhu, “Digital Public Infrastructure in the Developing World,” *Stanford Social Innovation Review*, March 25, 2024, https://ssir.org/articles/entry/digital-public-infrastructure-developing-world.

22 “Estonia among the Least Corrupt Countries, Rising to 12th Position Globally: Report,” Invest in Estonia, e-Estonia, March 2024, https://investinestonia.com/estonia-among-the-least-corrupt-countries-rising-to-12th-position-globally-report/.

23 “Estonia among the Least Corrupt,” Invest in Estonia.

24 “Estonia: Population, Demographic Situation, Languages, and Religions in Estonia,” Eurydice (network), European Commission, July 15, 2024, https://eurydice.eacea.ec.europa.eu/national-education-systems/estonia/population-demographic-situation-languages-and-religions.

25 “e-Identity: Estonia’s e-ID: The Cornerstone of a Seamless Digital Society,” e-Estonia, (Accessed October 2024., https://e-estonia.com/solutions/estonian-e-identity/id-card/.

26 Jake Maxwell Watts, “One Country’s Uber-Convenient, Incredibly Invasive Digital ID System,” *Wall Street Journal*, May 9, 2019, https://www.wsj.com/articles/the-digitization-of-your-identity-11557403060.

27 “e-Governance: Data Embassy,” e-Estonia, Accessed November 2024, https://e-estonia.com/solutions/e-governance/data-embassy/.

28 “Estonia Country Commercial Guide,” US Department of Commerce, March 15, 2024, https://www.trade.gov/country-commercial-guides/estonia-market-overview.

29 “Estonia among the Best Countries to Provide Digital Public Services according to the OECD,” e-Estonia, January 31, 2024, https://e-estonia.com/estonia-among-the-best-countries-to-provide-digital-public-services-according-to-the-oecd/.

30 “e:Identity: e-Residency,” e-Estonia, Accessed October 2024, https://e-estonia.com/solutions/estonian-e-identity/e-residency/.

31 Sten Hankewitz, “Estonian e-residents Contribute Millions to the Economy,” *Estonian World*, June 3, 2024, https://estonianworld.com/business/estonian-e-residents-contribute-millions-to-the-economy/.

32 “Estonia: The Most Advanced Digital Society in the World,” Global Ties KC, April 25, 2024, https://globaltieskc.org/estonia-the-most-advanced-digital-society-in-the-world/.

33 Billy Perrigo, “India’s Supreme Court Rules Aadhaar Is Constitutional,” *Time*, September 28, 2018, https://time.com/5409604/india-aadhaar-supreme-court/.

34 Michael Totty, “Addressing Its Lack of an ID System, India Registers 1.2 Billion in a Decade,” Research Brief, UCLA Anderson School of Management, April 13, 2022, https://anderson-review.ucla.edu/addressing-its-lack-of-an-id-system-india-registers-1-2-billion-in-a-decade/.

35 Michael Totty.

36 Ted O’Callahan, “What Happens When a Billion Identities Are Digitized?,” Faculty Viewpoints: K. Sudhir and Shyam Sunder, *Yale Insights*, March 27, 2020, https://insights.som.yale.edu/insights/what-happens-when-billion-identities-are-digitized.

37 Manya Rathore, “Share of Population Covered under Aadhaar in India as of Financial Year 2018 to 2023,” Statista, July 24, 2024, https://www.statista.com/statistics/1170678/india-share-of-population-covered-under-aadhaar/#:~:text=As%20of%20financial%20year%202023,to%20all%20across%20the%20country.

38 India’s Ministry of Electronics & IT underscored that “Aadhaar has been a powerful tool in bringing people into the formal financial system.” See Press Release 2067940, Press Information Bureau, Government of India, October 24, 2024, https://pib.gov.in/PressReleasePage.aspx?PRID=2067940#:~:text=Aadhaar%20has%20been%20a%20powerful,into%20the%20formal%20financial%20system.

39 Press Release 2067940, Press Information Bureau, Government of India.

40 “Over 200 Govt Websites Made Aadhaar Details Public: UIDAI,” *Times of India*, November 19, 2017, https://timesofindia.indiatimes.com/india/210-govt-websites-made-public-aadhaar-details-uidai/articleshow/61711303.cms.

41 Tech2 News Staff, “130 Mn Aadhaar Numbers Were Not Leaked, They Were Treated as Publicly Shareable Data: CIS,” *Firstpost*, May 3, 2017, https://www.firstpost.com/tech/news-analysis/130-mn-aadhaar-numbers-were-not-leaked-they-were-treated-as-publicly-shareable-data-cis-3702187.html.

42 Anuj Srivas, “Data Breaches, Leaks: UIDAI Rolls out New Security Measures,” *Wire*, January 10, 2018, https://thewire.in/tech/data-breaches-leaks-uidai-rolls-new-security-measures.

43 Sneha Kulkarni, “Aadhaar Authentication to Become More Secure with New System; Know Details,” *Economic Times*, last updated March 1, 2023, https://economictimes.indiatimes.com/wealth/save/aadhaar-authentication-to-become-more-secure-with-new-system-know-details/articleshow/98324038.cms?from=mdr#google_vignette.

44 Anirudh Burman, “Understanding India’s New Data Protection Law,” Paper, Carnegie Endowment for International Peace, October 3, 2023, https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en.

45 African Union, *Interoperability Framework for Digital Identity in Africa*, African Union, February 2022, https://au.int/sites/default/files/documents/43393-doc-AU_Interoperability_framework_for_D_ID_English.pdf.

46 Chris Burt, “Kenyan High Court Pauses National Digital ID for Third Time in 4 Years,” Biometric Update, July 25, 2024, https://www.biometricupdate.com/202407/kenyan-high-court-pauses-national-digital-id-for-third-time-in-4-years.

47 Ayang Macdonald, “Kenya’s Digital ID Delivery Back On; Court Sets Aside Latest Injunction,” Biometric Update, August 13, 2024, https://www.biometricupdate.com/202408/kenyas-digital-id-delivery-back-on-court-sets-aside-latest-injunction.

48 Melody Musoni, Ennatu Domingo, and Elvis Ogah, *Digital ID Systems in Africa*, ECDPM Discussion Paper 360, European Centre for Development Policy Management, December 2023, https://ecdpm.org/application/files/5517/0254/4789/Digital-ID-systems-in-Africa-ECDPM-Discussion-Paper-360-2023.pdf.

49 Kevin Rotich, “Estonia Opens Trade Office in Nairobi with 8 Firms,” Capital Business (Kenya), April 14, 2023, https://www.capitalfm.co.ke/business/2023/04/estonia-opens-trade-office-in-nairobi-with-8-firms/.

50 “Estonia’s Thriving Digital Partnership with Africa,” e-Estonia, July 10, 2023, https://e-estonia.com/estonias-thriving-digital-partnership-with-africa/.

51 “Data Protection Laws in Namibia,” DLA Piper, 2025, https://www.dlapiperdataprotection.com/index.html?t=law&c=NA#:~:text=freedoms%20of%20others.-,Save%20for%20the%20constitutional%20right%20to%20privacy%2C%20Namibia%20has%20not,and%20for%20matters%20connected%20therewith.

52 “eIDAS Regulation,” European Commission, last updated May 5, 2025, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

53 “eIDAS 2.0: A Beginner’s Guide,” Dock.io, June 9, 2025, https://www.dock.io/post/eidas-2.

54 “EU Digital Identity Wallet Home,” European Commission, Accessed October 2024,, https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home.

55 “Members”, European Wallet Consortium, Accessed June 23, 2025, https://eudiwalletconsortium.org/about-us/members/

56 “Mobile Driver’s Licenses (MDL) State Adoption,” IDScan.net, Accessed November 2024, https://idscan.net/mobile-drivers-licenses-mdl-state-adoption/?srsltid=AfmBOooTmfS5RCAaBxqcZ-TvY8Edog6vppp4trABtA1UmShfNldK3CJY.

57 “REAL ID Mobile Driver’s Licenses (mDLs),” Transportation Security Administration, Accessed June 23, 2025, https://www.tsa.gov/real-id/real-id-mobile-drivers-license-mdls

58 Ash Johnson, “Path to Digital Identity in the United States,” Information Technology and Innovation Foundation, September 23, 2024, https://itif.org/publications/2024/09/23/path-to-digital-identity-in-the-united-states/.

59 Improving Digital Identity Act of 2023, S. 884, 118th Cong., https://www.congress.gov/bill/118th-congress/senate-bill/884/text.

60 Improving Digital Identity Act of 2024, H.R. 9783, 118th Cong., https://www.govtrack.us/congress/bills/118/hr9783.

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

(202) 463-7226

www.AtlanticCouncil.org