ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

The Path to Digital Identity in the United States

ASH JOHNSON I SEPTEMBER 2024

Digital IDs are a more convenient, secure, and versatile option than physical IDs, but few Americans currently have one. With the right investments and collaboration between federal and state governments, Americans could realize the full potential of digital IDs.

KEY TAKEAWAYS

- A well-designed digital ID is more convenient, secure, privacy-protective, and usable than a physical ID.
- Countries around the world have started offering digital IDs since the advent of the 21st century, taking many different approaches to digital identity that the United States could learn from.
- Currently, 13 states offer mobile driver's licenses, a type of digital ID, and have faced challenges such as interoperability, accessibility, usability, and trust.
- The few federal efforts at a national digital identity system have resulted in only limited progress toward that goal.
- To ensure that all Americans have access to well-developed digital IDs, the federal government should coordinate a nationwide effort to promote digital ID development, implementation, and use.

CONTENTS

Key Takeaways 1
Introduction 2
The Case for Digital Identity 3
Digital Identity Trends 4
The Current Patchwork 7
Mobile Driver's Licenses 7
Challenges 10
Efforts at a National Standard 12
NIST Digital Identity Guidelines 12
National Strategy for Trusted Identities in Cyberspace 12
Improving Digital Identity Act 13
The Future of Digital Identity 14
Endnotes 16

INTRODUCTION

The overwhelming majority of smartphone-owning Americans live their day-to-day lives with the world virtually at their fingertips. They can stay in touch with friends and family, buy and sell products and services across borders, and access a seemingly endless library of information and entertainment at the touch of a screen. But for most Americans, if they want to prove their identity, they still need to reach into their wallet and pull out a physical form of ID, even though the technology exists to upgrade this process.

As more of Americans' everyday activities move online, the lack of digital identity solutions becomes more of a problem. Countries around the world have forged ahead in offering digital ID, leaving the United States in the dust. Here at home, a handful of states have risen above the rest by offering mobile driver's licenses (mDLs), but these efforts are uncoordinated and unavailable in most of the country. There is a better way, one spearheaded by a national initiative to ensure all Americans have access to convenient, accessible, and trustworthy forms of digital ID.

This report lays out a path toward achieving that goal. To start, it outlines the benefits of digital ID over physical forms of identification. It then analyzes trends in digital identity around the world, looking at various countries' digital ID offerings and how the private sector plays a role in making digital ID widely available. It explores the current patchwork of digital identity in the United States and the early efforts at creating a national standard for digital ID implementation. Finally, it recommends policies federal and state governments should take toward the future of digital identity in America.

THE CASE FOR DIGITAL IDENTITY

Simply put, a digital ID is a digital version of an identification document, such as a driver's license or passport. Typically stored on an individual's mobile device and accessible via an app, digital ID holds the potential to increase convenience, security, privacy, and usability as compared with physical IDs. With a well-developed digital ID system, individuals could access all their relevant identity documents in one place and use those documents to complete a wide range of activities that require identity verification.

The convenience factor of digital ID is the first and most obvious benefit. According to Pew Research Center, 90 percent of Americans owned a smartphone as of 2023, including 97 percent of Americans under 50.[1] With the rise of digital payments and digital ID, these individuals would no longer need to carry around a physical wallet.

For an even more convenient experience, digital ID platforms could allow individuals to upload other relevant documents—permits, licenses, vaccination cards, and more—further reducing the need for a physical wallet. Digital ID could also communicate additional attributes tied to identity, such as "veteran" or "enrolled student," eliminating the need for separate ID cards—such as student IDs—that communicate these attributes.

The increased convenience of digital IDs compared with their physical counterparts benefits governments as well as individuals. According to a 2019 report by McKinsey Digital, digital ID could save 110 billion hours globally by streamlining government services. The resulting cost savings and fraud reduction could amount to $1.6 trillion. In the United States specifically, full digital ID coverage could unlock economic value equivalent to 4 percent of gross domestic product (GDP) in 2030.[2]

The transition from physical wallets to mobile wallets also brings with it increased security. Thieves can easily steal a wallet off an individual and access their personal belongings and any information on their physical ID. However, while thieves can just as easily steal a smartphone off an individual, as long as the phone is secured using built-in features such as passwords or biometrics, the information stored on the phone will remain encrypted. Pew Research Center found in 2023 that 83 percent of smartphone owners take advantage of their smartphone's security features to safeguard their data.[3]

If designed correctly, digital ID can also be more privacy-protective than physical ID. Currently, when individuals hand over a physical ID in person or upload a photo of their physical ID online, the recipient can view all of the personal information displayed on the ID, including the individual's full name, date of birth, home address, and photograph. But governments could design digital IDs to display a barcode, QR code, or other scanning method that only reveals relevant information. For example, when purchasing alcohol, a digital ID would only reveal that the purchaser is over 21.

Finally, digital ID comes with increased usability compared with physical ID. Designed properly, digital ID would enable individuals to complete any transaction they currently complete with a physical ID: entering age-restricted spaces, purchasing age-restricted products, interacting with law enforcement, passing through airport security checkpoints, voting, and more. They would also simplify online transactions that require identity verification, including accessing age-

restricted content, purchasing age-restricted products, securely signing legal documents digitally, and executing contracts.

Because of this increased usability, if widely deployed and adopted, digital IDs could play a key role in age verification for online services, limiting access for individuals below a certain age. Age verification is a controversial approach to ensuring children's safety online by keeping children out of adult-oriented online spaces. There are multiple ways online services can verify users' ages, with ID checks being the most accurate but also the most invasive option. Digital ID could make this process less invasive by only sharing necessary information about individuals—for example, whether they are over the age of 18.[4]

Digital ID could also enable easier access to financial services, which typically require identity verification, and help businesses comply with know-your-customer and anti-money laundering laws. Globally, digital ID could provide access to financial services to 1.7 billion individuals who are currently financially excluded, according to McKinsey Digital.[5]

The current state of digital ID in America—passports equipped with electronic chips that hold identifying information about individuals and a limited patchwork of state-issued mDLs—has only begun to deliver on some of the promises of digital ID. Currently, most Americans do not have a digital ID, and those who do can only use it in a limited number of use cases. But the technological capability exists to offer fully realized digital ID that can perform all the functions previously listed, and with the right investments and collaboration between federal and state governments, Americans could realize the full potential of digital ID.

DIGITAL IDENTITY TRENDS

Since the advent of the 21st century, countries around the world have begun introducing and implementing forms of identification that can operate in both physical and digital environments. Early forms of such identification were electronic ID cards, physical cards equipped with radio-frequency identification (RFID) chips for online authentication.[6] More recent technology uses smartphone applications for a similar purpose, with a visual representation of an individual's ID and a QR code or barcode for scanning.

Countries have introduced these forms of digital ID for a variety of reasons, including many of the previously listed benefits—such as increasing convenience for users accessing government and other services and simplifying online identity verification—as well as other motivations, such as increasing the availability of identification for underserved populations. Countries also take different approaches to digital ID, with some spearheading a government-led effort to develop and distribute digital forms of identification and others relying on public-private partnerships to accomplish the same goal.

In order to ensure that their residents can travel with their digital ID, some countries have engaged in standards-setting with other countries in order to mutually accept each other's digital IDs. For example, a group of countries including Australia, Canada, Finland, Israel, the Netherlands, New Zealand, Singapore, and the United Kingdom established the Digital Government Exchange Digital Identity Working Group in 2020 to agree on principles and definitions for digital ID and lay the groundwork for international agreements.[7] Additionally, both the European Union and the African Union have initiatives aimed to create interoperable digital ID systems for their member states.[8]

Examples of Digital ID in Other Countries

Estonia

Estonia's electronic ID (e-ID) system, which issues a digital identity to every Estonian, has existed for over 20 years. The system includes a mandatory national ID card with a chip that enables users to verify their identity in an electronic environment for digital signatures, voting online, checking medical records, submitting tax claims, logging into bank accounts, traveling within the EU, and more. Ninety-nine percent of Estonians have such an ID card, and the cards have enabled 800 million digital signatures so far.[9]

Estonians can also use their mobile phone as a form of digital ID. Users request a special SIM card from their mobile phone operator to access this form of digital ID, which operates the same as an ID card but without the need for a card reader. Nineteen percent of Estonians use this form of digital ID.[10] Meanwhile, users without the required SIM card can instead download the Smart-ID app, which enables legally binding digital signatures and online identity verification. The Smart-ID app has over 730,000 Estonian users—51 percent of the country's population—and works across countries.[11]

Figure 1: A sample Estonian national ID card[12]

Estonia launched its e-ID system as a result of the country's Tiger Leap Initiative, started in 1996, which aimed to develop information technology infrastructure within the country to catch up to the West just five years after Estonia gained independence from the Soviet Union. The initiative led to the creation of not only e-ID but also online banking solutions, online taxes, mobile parking, online voting, electronic health records and prescriptions, online marriage applications, and more.[13]

India

India started on the path toward digital ID in 2009 with the creation of the Unique Identification Authority of India (UIDAI) to solve multiple problems. In 2010, 40 percent of India's population was unregistered and 60 percent was unbanked. Only 60 million people—less than half the country's population—had passports. UIDAI created Aadhaar, a system that issues a unique, biometrically secured 12-digit ID number to each individual. In other words, with a fingerprint or iris scan—or, lacking biometric scanners, a QR code—individuals with an Aadhaar can verify their identity to access government, financial, and other services. Individuals can also request a "virtual Aadhaar ID," a separate number to provide to each company the individual wants to do business with that verifies the individual's identity while preventing multiple companies from linking a person's behavior.[14]

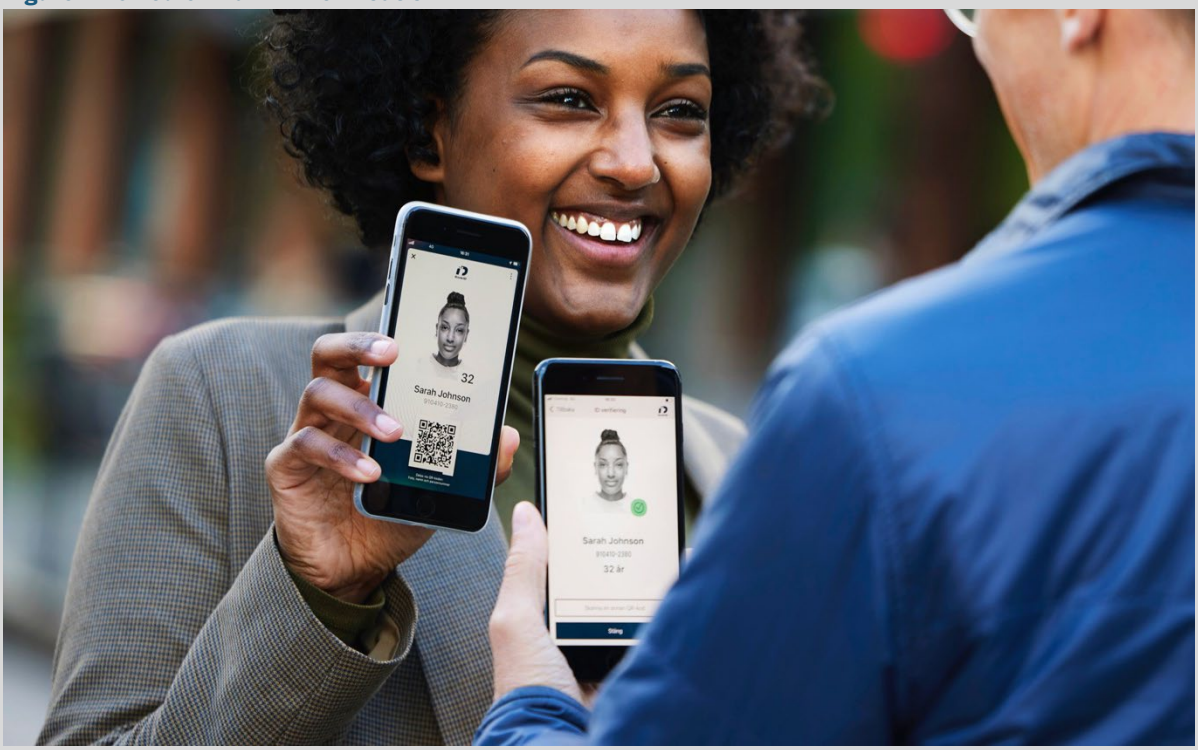
E-Aadhaar is a password-protected electronic copy of an individual's Aadhaar that is equally valid as a physical copy in all cases. Users can download their e-Aadhaar off UIDAI's online portal or via a mobile app.[15]

India's Aadhaar program successfully registered 1.2 billion people in 10 years. A 2019 survey found that 95 percent of Indian adults used their Aadhaar ID at least once a month and 90 percent were satisfied with the program. The program cost $1.5 billion to implement, but has been credited with saving $12 billion as of 2018 by reducing fraud.[16]

Sweden

Sweden's e-ID system, BankID, traces its roots to 2001, when a consortium of major Swedish banks formed to develop the infrastructure for digital IDs that both the government and businesses would accept as a form of identity verification. This form of digital ID, called BankID, was first issued in 2003 and today has 8 million users and enables an average of 18 million identifications and digital signatures every day. From the beginning, Swedes could use their BankID not just to prove their identity to financial institutions but also government agencies, such as the Swedish Tax Agency and Swedish Social Insurance Agency, which were early adopters.[17]

Figure 2: Swedish BankID verification[18]



To obtain a BankID, which almost every Swedish adult now has, an individual must have a valid passport or personal identity number—a unique 10-digit number that identifies each Swedish resident—and be a customer of a participating bank. Upon receiving a BankID, individuals can access their digital ID via the BankID app and either display a visual representation of the card for in-person validation or a QR code for scanning. Unfortuantely, though individuals can use their BankID for identity verification and digital signatures, it is not a valid travel document nor can it replace a driver's license.[19]

Government actors are not the only parties involved in providing digital ID to the general public. As exemplified by Sweden's BankID, financial institutions can offer digital ID to their customers as an alternative to traditional means of identity verification, such as PINs and passwords. However, even when not issuing a digital ID, governments are still responsible for establishing a person's legal identity. Governments may also work with device manufacturers such as Apple and Google to ensure that individuals can access their digital ID via the Wallet app on their mobile devices, or partner with another company to develop a standalone app that hosts users' digital ID.

Finally, governments can experiment with blockchain technology for digital ID to enhance security, resilience, transparency, and interoperability. Blockchains are digital ledgers that record information that is distributed among a network of computers and consist of a series of digital "blocks" that are securely linked together using cryptography. These blocks record information—in this case, an individual's digital ID. Each computer in the network stores a copy of the blockchain, forming a distributed peer-to-peer network where updates are shared and synchronized.

The blockchain eliminates the need for a central authority, such as a bank or government agency, to ensure the integrity of records. Instead, blockchains maintain agreement between all participants using a "consensus protocol"—a set of rules that allows each computer in the network to determine when to add new information to the blockchain.[20] However, even when using blockchain, government agencies still play an important role in verifying and authenticating a person's identity before issuing a digital ID.

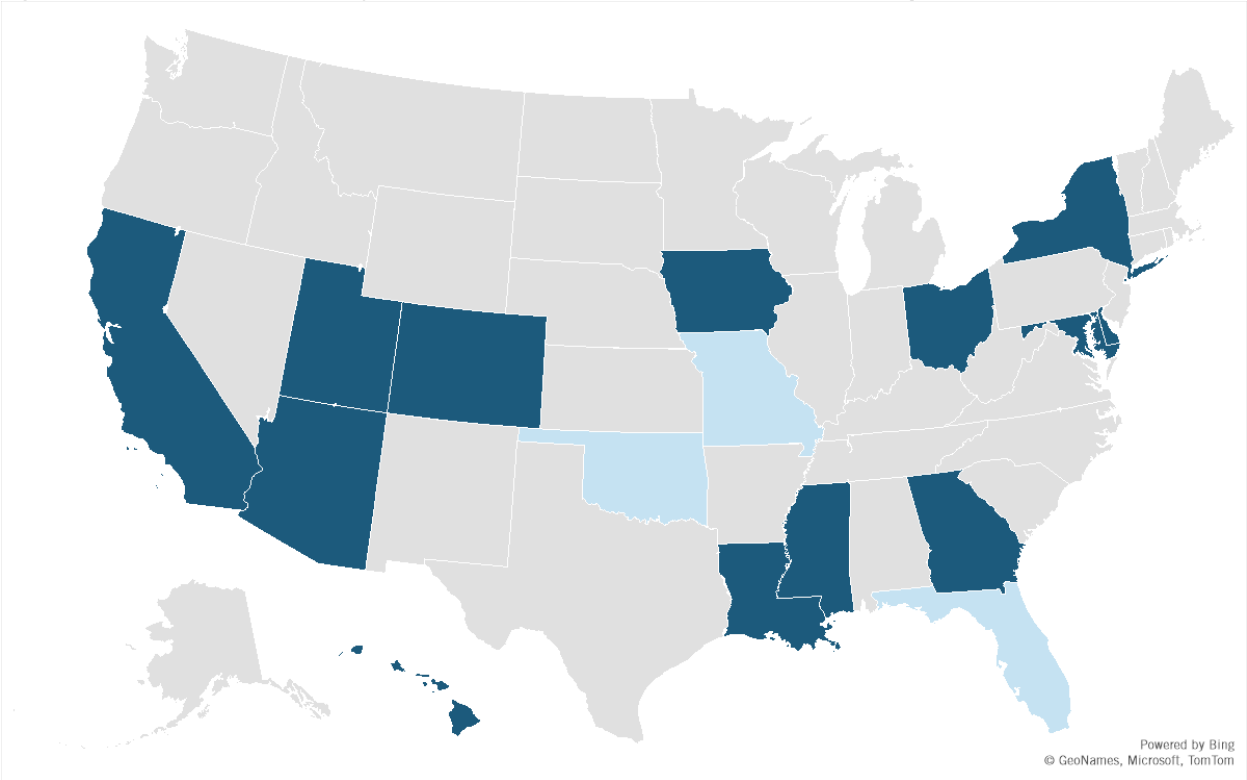
THE CURRENT PATCHWORK

In the absence of a national standard for digital identity, a handful of forward-thinking states have begun offering digital ID in the form of mDLs, which are still early in their implementation, with relatively few adopters and limited use cases. Indeed, many states that offer mDLs encourage users to still carry a copy of their physical driver's license for interactions with law enforcement and businesses. Exacerbated by the ad hoc nature of mDL offerings across the country, states grapple with challenges such as interoperability, accessibility, usability, and trust that further limit mDLs' appeal to consumers.

Mobile Driver's Licenses

The term "mobile driver's license" refers to state-issued digital versions of an individual's driver's license. Only 13 states have mDLs as of September 2024: Arizona, California, Colorado, Delaware, Georgia, Hawaii, Iowa, Louisiana, Maryland, Mississippi, New York, Ohio, and Utah. An additional three states—Florida, Missouri, and Oklahoma—used to offer mDLs but no longer do.[21] (See figure 3.) Oklahoma shuttered its mDL program over accessibility concerns, Florida's Department of Highway Safety and Motor Vehicles issued a statement that it is switching to a different vendor to issue mDLs, and Missouri seems to have quietly discontinued its program with no explanation.[22]

Figure 3: Thirteen states currently offer mobile driver's licenses; three have in the past



Depending on relevant state laws, residents of states that offer mDLs can use their mDL to access age-restricted venues, such as bars and clubs, and purchase age-restricted products, such as alcohol and tobacco. Some states, such as Louisiana, allow residents to use their mDL for voting, and law enforcement in certain states may accept mDLs as verification, for example, at a traffic stop. Finally, more than 28 airports in 22 states accept digital forms of identification at Transportation Security Administration (TSA) checkpoints as the TSA continues to update the credential authentication technology in airports to the latest version, which can authenticate digital IDs.[23]

Examples of Mobile Driver's Licenses

Delaware

Delaware offers mDLs via the Mobile ID app developed by Idemia, an identity services company. Secured via a six-digit PIN and biometrics such as FaceID or TouchID, Delaware's mDL allows for contactless identity verification. Users can show a digital photo of their ID or display a barcode or QR code for scanning. For added privacy, users can opt to show their ID's barcode or QR code without displaying the ID itself, revealing only the relevant information needed for the scan, such as whether an individual is over the age of 21 for purchasing alcohol.

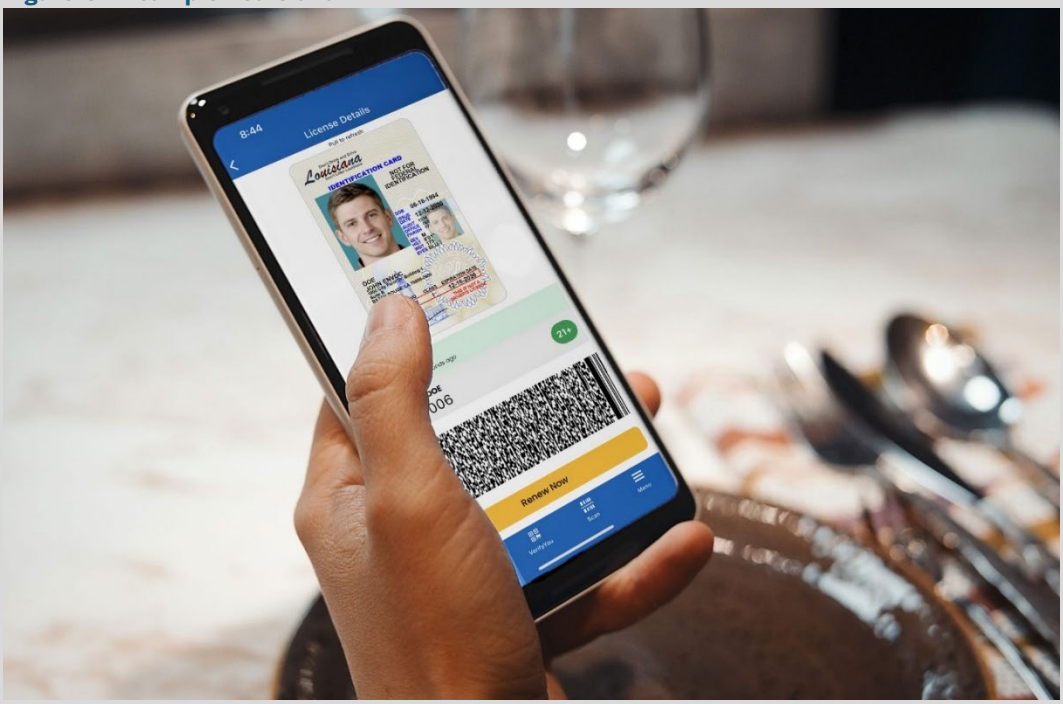
Figure 4: A sample Delaware mDL[24]

Unfortunately, Delawareans with mDLs may still need to carry their physical driver's licenses, as the law requires that individuals show a physical driver's license when requested by law enforcement.[25]

Louisiana

Louisiana offers mDLs via the state's proprietary app, LA Wallet, developed by Louisiana-based software company Envoc. The app keeps users' license information current with real-time updates from Louisiana's Office of Motor Vehicles and allows users to renew their license in app. By law, Louisiana law enforcement, state government services, and retail locations throughout the state must accept mDLs stored on LA Wallet in place of a physical driver's license.

Figure 5: A sample Louisiana mDL[26]



LA Wallet provides users with a barcode for scanning in addition to a photo of their driver's license for in-person viewing. Users can also store a copy of their digital health records, such as their COVID-19 vaccinations, as well as digital copies of their vehicle registration, hunting and fishing licenses, Medicaid cards, and concealed handgun permits. The app also enables users to anonymously and remotely verify their age, which is especially useful given Louisiana's laws requiring age verification to access social media and adult websites.[27]

Challenges

Interoperability

States have faced multiple challenges in their efforts to make mDLs available to their residents. The first of these is interoperability. There are standards that the leading mDL providers—Apple, Google, and Idemia, as well as Louisiana's LA Wallet—follow that create some degree of interoperability. These standards, developed by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) and known as ISO/IEC 18013-5, establish interface specifications that enable parties other than the issuing authority—in this case, a state government—to read and authenticate mDLs. The standards allow for regional additions, such as Real ID standards in the United States.[28]

While all providers currently offering mDLs in the United States adhere to ISO/IEC 18013-5, there is no requirement that future providers do so. Instead, it is up to each individual provider to decide whether to follow these standards. Without a guarantee of interoperability, there is the possibility that residents of a state that offers mDLs via one provider could run into issues in a state that offers mDLs via another provider, proving especially frustrating for Americans who live in one state but work in another or with a job or lifestyle that require regular travel. Additionally, residents of states that do offer mDLs are unlikely to find many use cases when traveling to a state that does not offer mDLs, which currently represents the vast majority of the country.

Open standards such as ISO/IEC 18013-5—or, similarly, the World Wide Web Consortium's verifiable credentials, a standard for digital credentials—are important to ensure interoperability between not only mDLs but also different types of digital ID.[29] Ideally, in a world where all identity documents and credentials have digital versions available—from driver's licenses and passports to library cards and student IDs—individuals could store all these various documents in the same digital wallet.

Accessibility

Another challenge that led one state to discontinue its mDL is accessibility. Over 40 million Americans have a disability according to 2022 data from the U.S. Census Bureau. That includes over 12 million Americans with a hearing difficulty, over 8 million with a vision difficulty, and over 17 million with a cognitive difficulty, all of which can pose challenges when interacting with online services, including mDLs, if those services are not designed with accessibility in mind.[30]

Oklahoma discontinued its mDL app, OK Mobile ID, after the Department of Justice (DOJ) found that the app violated the Americans with Disabilities Act because individuals with vision impairments could not use the app. The app required users to upload photos of their physical ID and follow a series of on-screen instructions to take a selfie, including making a series of head and eye movements based on visual information on the screen, a process that would be difficult, if not impossible, for users with vision impairments to complete on their own.[31]

Despite DOJ's conclusion that there was "no evidence that making the OK Mobile ID App accessible would result in a fundamental alteration or an undue burden to Service Oklahoma," Service Oklahoma, an agency that provides driver and motor vehicle services in the state, announced 17 days after reaching a settlement agreement that it would shutter the app entirely, stating, "As the necessary corrections are extensive, we are also exploring the option of decommissioning the app altogether due to a lack of use cases with the current product."[32] By making accessibility a priority and building it into services from their inception, rather than treating it as an afterthought, states can avoid repeating Oklahoma's mistake.

Usability

As Service Oklahoma alluded to in its announcement that it would discontinue offering mDLs, some states' mDLs also suffer from a lack of usability or use cases that would convince residents to switch from using a physical driver's license. Until individuals can use an mDL in all instances when they would need to display a physical driver's license—including entering age-restricted venues, using age-restricted online services, purchasing age-restricted products online or offline, voting, interacting with law enforcement, or passing through TSA checkpoints at all airports—individuals will still need to carry a physical driver's license along with an mDL, in which case many individuals may decide it is simply easier to only carry a physical driver's license and not apply for an mDL.

The usability challenge is intrinsically tied to the interoperability challenge. Even if individuals can use an mDL for all of those use cases in their home state, they may not be able to do so in a state that does not offer mDLs or that offers mDLs using a different provider that is not interoperable with the individual's home state's provider. Thus, they would still need to carry a physical driver's license with them when traveling out of their home state.

Trust

Finally, a challenge that nearly every new technological development faces at some point in its life cycle is gaining and maintaining the public's trust. In part, this trust is earned through practices that safeguard the privacy and security of individuals' sensitive personal data as they use mDLs. For example, the aforementioned ISO/IEC 18013-5 standard outlines protocols for privacy and data security of mDLs.[33]

Unfortunately, while good privacy and security practices may increase public trust, the public can lose trust in a technology for often irrational reasons as part of the "privacy panic cycle," a recurring pattern of privacy fears that appear following the introduction of a new technology.[34] At first, a new technology has not yet been widely deployed and only a core group of people have knowledge, during which privacy concerns are minimal. As the technology starts to become more well-known outside this relatively small circle, privacy fundamentalists and those who do not trust government begin to raise alarms about the technology, drawing negative attention and causing others—such as the media—to start fanning the flames of fear.

Eventually, the public dismisses the privacy concerns associated with the technology as it becomes increasingly commonplace and interwoven into society. Finally, the vast majority of consumers no longer believe the claims espoused by privacy fundamentalists because they understand the technology, appreciate the benefits, and no longer fear its misuse.

Digital forms of identification such as mDLs are still at the beginning of their technological life cycle, especially in the United States, where their deployment is sporadic. These trusted

beginnings may give way to rising panic as mDLs and other forms of digital ID become more mainstream. The best states and the federal government can do to combat this privacy panic is to clearly communicate the benefits of digital ID, ensure digital ID is as secure and privacy-protective as possible while maintaining utility, and not allow overblown fears to impact regulation surrounding digital ID.

A second factor impacting public trust of digital ID, specifically in the United States, is political opposition to the concept of a national ID. However, implementing a digital ID system in the United States would not require creating a new national ID system. Instead, the system could digitize existing forms of identification, including identity documents already issued by states and the federal government such as driver's licenses and passports, respectively, proving individuals' identities with bits as opposed to atoms.

There would still likely be some opposition to any federally mandated change, as there was when the Real ID Act of 2005 passed, requiring states to standardize driver's licenses and enter them into a national database, which opponents saw as a sneaky way to implement a national ID system, even though it only improved state government standards.[35] Despite opposition, the law has remained in effect, and as of May 7, 2025, the federal government, including the TSA, will no longer accept driver's licenses that do not meet Real ID requirements.[36]

EFFORTS AT A NATIONAL STANDARD

As more states explore and offer mDLs, progress toward a national standard for digital ID has mostly stalled. However, between standards for digital identity verification by government agencies, an Obama-era digital ID initiative, and bills in Congress, the building blocks are there for the federal government to pick back up again and turn the existing ad hoc patchwork of mDLs into a cohesive digital identity option for all Americans.

NIST Digital Identity Guidelines

Originally published in 2004, the National Institute of Standards and Technology's (NIST's) Digital Identity Guidelines outline technical requirements for federal agencies to implement digital identity services.[37] NIST has updated these guidelines three times since then, with a draft of its fourth revision released as recently as December 2023.[38]

The guidelines cover proving and authenticating the identity of users—such as government employees and contractors, as well as private individuals—interacting with government systems. The latest draft aims to respond to the ways in which the digital landscape has evolved since NIST's most recent update in 2017, such as improved reliability of biometrics, and address challenges related to equality, consumer choice, and fraud prevention.[39]

Because NIST's guidelines establish protocols for online identity verification—in other words, establishing that individuals are who they say they are—they could serve as a basis for the development of digital forms of identification, particularly in ensuring that these forms of ID are usable, equitable, and secure.

National Strategy for Trusted Identities in Cyberspace

In 2011, the same year that NIST published its first revision of its Digital Identity Guidelines, the Obama administration took the next step toward establishing a national digital ID with its National Strategy for Trusted Identities in Cyberspace (NSTIC). The strategy charted a course for

public-private sector collaboration to establish trustworthy methods to reliably identify and authenticate individuals, organizations, networks, services, and devices online.[40]

NSTIC outlined an ambitious strategy that would create voluntary, privacy-enhancing, secure, resilient, interoperable, cost-effective, and easy-to-use identity solutions, eliminating the need for individuals to maintain a different username and password for each website with which they interact. It included roles for every level of government, the private sector, and international partners.

According to the strategy document, within three to five years—between 2014 and 2016—NSTIC would result in an identity ecosystem wherein individuals have the ability to choose trusted digital identities for personal and business use that they can use across multiple sectors, with a growing number of individuals and identity providers signing on to be part of the ecosystem. Within 10 years—by 2021—the identity ecosystem was supposed to be fully realized and available to anyone who chose to adopt it.

NSTIC ultimately did not realize most of its goals. Instead, the strategy led to the creation of Login.gov, launched in 2017 as a shared authentication service for government agencies.[41] In other words, members of the public can use one account and password to securely sign in to participating government websites, rather than creating separate accounts for each website. Login.gov includes an identity verification process, which requires an individual's driver's license or other state-issued ID, Social Security number, and phone number or address.[42]

In September 2023, the General Services Administration (GSA) announced that all cabinet agencies were using Login.gov, making up 15 of the over 40 federal and state agencies that participate in the service. Other participating agencies include the Small Business Administration, the U.S. Postal Service, and the Office of Personnel Management, the last of which allows individuals to use Login.gov to access USAJOBS, the federal government's official job board.[43] Notably, the Internal Revenue Service (IRS) does not use Login.gov for identity verification, arguing that it is not secure enough and lacks sufficient anti-fraud controls.[44] Instead, the IRS, as well as the Social Security Administration, uses ID.me, an American online identity company, for identity verification.[45]

Improving Digital Identity Act

There has been little progress in Congress toward establishing a national standard for digital identity, though there is a path forward. The Improving Digital Identity Act, first introduced in 2021 by Reps. Bill Foster (D-IL), John Katko (R-NY), James Langevin (D-RI), and Barry Loudermilk (R-GA) and most recently reintroduced in 2023 by Sens. Kyrsten Sinema (I-AZ) and Cynthia Lummis (R-WY), would establish a task force to coordinate a government-wide effort to promote digital identity use in the public and private sectors.[46]

The current text of the bill, which has made little headway since its reintroduction, would establish the Improving Digital Identity Task Force within the Executive Office of the President, comprising a director appointed by the president; at least 11 federal government representatives; 6 state, local, tribal, or territorial government officials; and 5 nongovernmental experts. In its work, the task force would emphasize priorities such as privacy, security, reliability, interoperability, trust, equitable access, and reducing identity theft and fraud.

The bill explicitly prohibits the task force from recommending a single national identity credential provided by the federal government. Instead, the task force would promote the development of digital versions of existing physical forms of identification, such as driver's licenses, passports, social security credentials, and birth certificates, including by identifying funding and other resources necessary to support the agencies that issue these forms of ID.

The task force would publish an initial report with its recommendations on implementing a digital identity strategy, followed by the director of the Office of Management and Budget (OMB) issuing guidance to federal agencies on implementing the task force's recommendations. OMB would also issue annual progress reports. After a year, the Government Accountability Office would submit a report on potential savings from switching to digital forms of identification. The task force would sunset three years after the bill's enactment, publishing an interim report halfway through its mandate and a final report toward the end of its three years.

THE FUTURE OF DIGITAL IDENTITY

A well-developed digital ID system should provide all the benefits of digital IDs for Americans: increased convenience, security, privacy, and usability. It could also address the challenges currently facing states' mDL implementations of interoperability, accessibility, usability, and trust. Americans from anywhere in the country could board an airplane, interact with law enforcement, purchase alcohol, enter a club, file their taxes, and much more, all with their phones.

In other words, a well-developed digital ID system could—and should—fully replace physical IDs, which requires a legal framework that accepts digital IDs as a valid form of identification in all use cases. Individuals could use their digital IDs to travel across state lines and even internationally, requiring national coordination of state efforts and international cooperation to have other countries recognize Americans' digital IDs. Users with disabilities should not face barriers to accessing a digital ID, which requires building in accessibility from the beginning and prioritizing it throughout the development process. Finally, to ensure trust, a well-developed digital ID system should be secure and privacy-protective, adhering to best practices to safeguard users' data.

Current state-level efforts to offer digital ID are innovative but sporadic. States should continue offering mDLs and passing laws that ensure mDLs are at least as usable as their physical counterparts. Additionally, in order to ensure that all Americans have access to well-developed digital IDs, the federal government should coordinate a nationwide effort to promote digital ID development, implementation, and use.

Specific steps federal and state governments should take include the following:

- States with mDLs should pass laws requiring law enforcement to accept digital ID as a valid form of identification, for example, at traffic stops so individuals with a digital ID do not have to also carry a physical ID.
- Congress should establish a grant program for states to create mDLs that comply with ISO/IEC 18013-5 to incentivize states to create interoperable mDLs.
- Congress should pass the Improving Digital Identity Act, establishing a task force to coordinate a government-wide effort to promote digital ID use in the public and private sectors.

- GSA should improve the security and fraud prevention of Login.gov and then require all government online services to use the site and start accepting digital ID for any transaction that requires identity verification.
- NIST should create accessibility and interoperability standards for digital ID that federal and state governments and private entities can follow.
- All federal agencies should start accepting government-issued digital ID, including existing state-issued mDLs, as a valid form of identification for federal purposes, such as for security in all American airports and federal buildings.
- The State Department should work to form international agreements with other countries for mutually accepting each other's digital IDs as a valid form of identification, provided they adhere to ISO/IEC 18013-5 or another agreed-upon standard.

About the Author

Ash Johnson (@ashljnsn) is a senior policy manager at ITIF, specializing in Internet policy issues including privacy, security, platform regulation, e-government, and accessibility for people with disabilities. Her insights appear in numerous prominent media outlets such as *TIME*, *The Washington Post*, NPR, BBC, and Bloomberg.

Previously, Johnson worked at Software.org: the BSA Foundation, focusing on diversity in the tech industry and STEM education. She holds a master's degree in security policy from The George Washington University and a bachelor's degree in sociology from Brigham Young University.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world's leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit itif.org/about.

ENDNOTES

1. "Mobile Fact Sheet," Pew Research Center, January 31, 2024, https://www.pewresearch.org/internet/fact-sheet/mobile/.
2. Olivia White et al., "Digital identification: A key to inclusive growth" (McKinsey Global Institute, April 2019), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.
3. "How Americans protect their online data," Pew Research Center, October 18, 2023, https://www.pewresearch.org/internet/2023/10/18/how-americans-protect-their-online-data/.
4. Ash Johnson, "How to Address Children's Online Safety in the United States" (ITIF, June 2024), https://itif.org/publications/2024/06/03/how-to-address-childrens-online-safety-in-united-states/.
5. Olivia White et al., "Digital identification."
6. Daniel Castro, "Explaining International IT Application Leadership: Electronic Identification" (ITIF, September 2011), https://www2.itif.org/2011-e-id-report-final.pdf.
7. Jack Aldane, "Eight countries set out principles for the future of digital ID," *Global Government Forum*, February 28, 2022, https://www.globalgovernmentforum.com/eight-countries-set-out-principles-for-the-future-of-digital-id/.
8. "European Digital Identity Wallet," European Commission, accessed August 8, 2024, https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home; "AU Interoperability Framework for Digital ID" (African Union, February 2022), https://au.int/sites/default/files/documents/43393-doc-AU_Interoperability_framework_for_D_ID_English.pdf.
9. "ID-card," e-Estonia, accessed July 16, 2024, https://e-estonia.com/solutions/estonian-e-identity/id-card/.
10. "Mobile ID," e-Estonia, accessed July 16, 2024, https://e-estonia.com/solutions/estonian-e-identity/mobile-id/.
11. "Smart ID," e-Estonia, accessed July 16, 2024, https://e-estonia.com/solutions/estonian-e-identity/smart-id/.
12. "2021- ID-card sample," Estonian Police and Border Guard Board, accessed July 16, 2024, https://www.politsei.ee/en/instructions/id-card-sample.
13. "Story," e-Estonia, accessed July 16, 2024, https://e-estonia.com/story/.
14. Ted O'Callahan, "What Happens When a Billion Identities Are Digitized?" *Yale Insights*, March 27, 2020, https://insights.som.yale.edu/insights/what-happens-when-billion-identities-are-digitized.
15. "E-Aadhaar," UIDAI, accessed July 16, 2024, https://uidai.gov.in/en/contact-support/have-any-question/283-english-uk/faqs/aadhaar-online-services/e-aadhaar.html.
16. Michael Totty, "Addressing Its Lack of an ID System, India Registers 1.2 Billion in a Decade," *UCLA Anderson Review*, April 13, 2022, https://anderson-review.ucla.edu/addressing-its-lack-of-an-id-system-india-registers-1-2-billion-in-a-decade/.
17. "BankID," BankID, accessed July 19, 2024, https://www.bankid.com/en/; "Our history," BankID, accessed July 19, 2024, https://www.bankid.com/en/om-oss/historia.
18. "Now easier to verify the digital ID card," BankID, April 19, 2024, https://www.bankid.com/en/om-oss/nyheter/easier-to-verify-the-digital-id-card.
19. "Digital ID card," BankID, accessed July 19, 2024, https://www.bankid.com/en/privat/digitalt-id-kort-i-bankid.

20. "ITIF Technology Explainer: What Is Blockchain?" (ITIF, October 2018), https://itif.org/publications/2018/10/03/itif-technology-explainer-what-blockchain/.
21. "Mobile drivers license & digital ID adoption," IDScan.net, accessed August 14, 2024, https://idscan.net/mobile-drivers-licenses-mdl-state-adoption/.
22. Wes Davis, "Florida's digital ID app has suddenly disappeared," *The Verge*, https://www.theverge.com/2024/7/10/24196044/florida-smart-id-digital-state-id-app-shut-down; Alex Ambrose, "Oklahoma's Failure in Digital IDs Highlights Lesson in Building Accessibility From the Start" (ITIF, April 19, 2024), https://itif.org/publications/2024/04/19/oklahoma-failure-in-digital-ids-highlights-lesson-in-building-accessibility/.
23. "Digital ID Map," TSA, accessed July 10, 2024, https://www.tsa.gov/travel/digital-id/map; "TSA introduces state-of-the-art identity verification technology at DEN security checkpoints," TSA, November 18, 2022, https://www.tsa.gov/news/press/releases/2022/11/18/tsa-introduces-state-art-identity-verification-technology-den.
24. "Mobile ID," Delaware Division of Motor Vehicles, accessed July 11, 2024, https://dmv.de.gov/mobileID/.
25. Ibid.
26. "About," LA Wallet, accessed August 22, 2024, https://lawallet.com/about/.
27. Ibid.; "Secure Online Child Interaction and Age Limitation Act," Louisiana State Legislature, accessed July 11, 2024, https://legis.la.gov/legis/Law.aspx?d=1337817; "Act No. 440," Louisiana State Legislature, accessed July 11, 2024, https://legis.la.gov/legis/ViewDocument.aspx?d=1289498.
28. "ISO/IEC 18013-5:2021," ISO, September 2021, https://www.iso.org/standard/69084.html.
29. "Verifiable Credentials," Verifiable Credentials, accessed August 14, 2024, https://verifiablecredentials.dev/.
30. "S1810: Disability Characteristics," United States Census Bureau, accessed July 10, 2024, https://data.census.gov/table/ACSST1Y2021.S1810?q=s1810.
31. Ambrose, "Oklahoma's Failure in Digital IDs."
32. "Settlement Agreement Between The United States of America and Service Oklahoma," Department of Justice, January 22, 2024, https://www.justice.gov/d9/2024-01/service_oklahoma_fully_executed_agreement.01.22.24.pdf; Kaylee Douglas, "Justice Department finds Service Oklahoma mobile app inaccessible," *KFOR*, https://kfor.com/news/local/justice-department-finds-service-oklahoma-mobile-app-inaccessible/.
33. "Mobile drivers license," IDScan.net; "ISO/IEC 18013-5:2021," ISO.
34. Daniel Castro and Alan McQuinn, "The Privacy Panic Cycle: A Guide to Public Fears About New Technologies" (ITIF, September 2015), https://www2.itif.org/2015-privacy-panic.pdf.
35. "Real ID," American Civil Liberties Union, accessed August 8, 2024, https://www.aclu.org/issues/privacy-technology/national-id/real-id.
36. "REAL ID," Department of Homeland Security, accessed August 8, 2024, https://www.dhs.gov/real-id.
37. "Special Publication 800-63," NIST, updated February 16, 2022, https://www.nist.gov/special-publication-800-63.
38. "Roadmap: NIST Special Publication 800-63-4 Digital Identity Guidelines," NIST, updated March 17, 2023, https://www.nist.gov/identity-access-management/roadmap-nist-special-publication-800-63-4-digital-identity-guidelines.
39. "SP 800-63-4," NIST, December 8, 2023, https://pages.nist.gov/800-63-4/sp800-63.html.

40. "National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy" (The White House, April 2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.
41. "About us," Login.gov, accessed June 27, 2024, https://login.gov/about-us/.
42. "Verify your identity," Login.gov, accessed August 8, 2024, https://www.login.gov/help/verify-your-identity/overview/.
43. "U.S. General Services Administration announces all Cabinet agencies are now using Login.gov," GSA, September 29, 2023, https://www.gsa.gov/about-us/newsroom/news-releases/us-general-services-administration-announces-all-cabinet-agencies-are-now-using-logingov-09292023; "Who uses Login.gov?" Login.gov, accessed June 27, 2024, https://login.gov/who-uses-login/.
44. Natalie Alms, "IRS won't add Login.gov without changes," *Nextgov/FCW*, October 6, 2023, https://www.nextgov.com/digital-government/2023/10/irs-wont-add-logingov-without-changes/391033/.
45. "ID.me," ID.me, accessed August 8, 2024, https://www.id.me/.
46. "H.R.4258 - Improving Digital Identity Act of 2021," Congress.gov, accessed June 28, 2024, https://www.congress.gov/bill/117th-congress/house-bill/4258; S.884 - Improving Digital Identity Act of 2023," Congress.gov, accessed June 28, 2024, https://www.congress.gov/bill/118th-congress/senate-bill/884.