# United States House Committee on Oversight
# Subcommittee on Government Operations

*Emerging Fraud Threats and the Evolving Fraud Landscape*

Testimony of Jay Stanley, Senior Policy Analyst, ACLU

July 15, 2026

Chairman Sessions, ranking member Mfume, and members of the subcommittee, thank you for your attention to the issue of digital identification and its potential role in combating fraud, and thank you for inviting me to testify today. I would like to leave you with two overarching points: a digital ID system would be a disaster for individual freedom if it is not done right, and the digital ID system that currently has the most momentum, mobile driver's licenses (mDLs) issued by the states, is not being done right. We must ensure that America does not become a "checkpoint" society where it is impossible to engage in everyday life without demands to prove your identity at every turn.

Digital IDs pose a real danger of turning into a true national identity card system of the kind that Americans have long opposed — a "super ID" that is used to track and control us, traps Americans in a regimented, bureaucratic system, shifts power from ordinary people to companies and government, and basically functions as an electronic ankle bracelet monitor that we cannot escape. And the more a digital ID becomes a legal or practical requirement for everyday life, the more it will shut out people who are less likely to have a smartphone or the easy ability to navigate technology, like seniors.

Make no mistake, a digital ID will be just such an exclusionary "super ID" unless it is constructed with great care. Fortunately, a wide variety of better approaches to digital identity are being developed around the world. Interest in digital identity systems has fueled the emergence of an entire community of technologists, entrepreneurs, academics, and others who have been working on identification for many years — including the problem of how to allow for online identification and authorization without creating a system for centralized tracking and control.[1] That movement has created a fertile variety of proposed systems and standards.

[1] For example, the Internet Identity Workshop (IIW), focused on user-controlled digital identity, has been held semi-annually since 2005. *Internet Identity Workshop*, Wikipedia, https://en.wikipedia.org/wiki/Internet_Identity_Workshop.

That is also true when it comes to the field of privacy-enhancing cryptography, which is advancing quickly with a great deal of creative research that promises to allow us to "have our cake and eat it too" when it comes to privacy and security across a wide variety of applications. For example, a privacy-enhancing technology called "zero knowledge proofs" allows people to prove they know certain things without revealing what those are — a privacy-preserving technique that is still in the process of being applied in new areas.[2]

A digital ID such as an mDL could contain all the information that is now on our physical driver's licenses, including full legal name, address, weight, height, organ donor status, your unique driver's license number. Many of these fields, alone or in combination, can be used to uniquely identify you. Depending on how it is designed, a digital ID might also provide other electronic fingerprints that uniquely identify you.

If we are to build a digital identity system — or preferably multiple decentralized competing systems — it's vital that they make use of all this research and innovation. If a system can reduce fraud and provide other benefits *without* enabling a system of tracking and control, why would we build one that *does enable* such tracking and control?

## I. A DIGITAL ID DONE BADLY WOULD CREATE FAR-REACHING HARMS

The creation of a digital ID infrastructure — especially one that could be used over the internet — would be a turning point that could have enormously harmful effects on our privacy, on the right to anonymous speech, on the accessibility of crucial life functions by many Americans, and more. If any such system is to be adopted, it must be done so with great care and deliberation. It must be designed to be under the control of users, privacy-protecting, open rather than proprietary, and non-exclusionary. It must be accompanied by both technological and legal protections against the negative side effects the creation of a digital ID is otherwise likely to have.

### a. Digital IDs will lead to an explosion in demands that we prove our identity

Sometimes there is a legitimate need to identify people, but there are also a lot of other parties that don't really need to access your fully DMV-vetted, cryptographically locked-down proof of identity — but will want to anyway for their own purposes.

A digital ID would make it much easier to present a cryptographically locked-down super-ID, but that also means it will become much easier for all manner of offline and online parties to *request or demand* that super-ID, since it would be a much smaller ask than the elaborate procedures often required today to prove identity remotely. By removing such friction, digital ID

[2] *See* Jay Stanley, *Paths Toward an Acceptable Public Digital Currency*, ACLU (Mar. 3, 2023), https://www.aclu.org/sites/default/files/field_document/cbdc_white_paper_-_0882_0.pdf (on encryption tools in digital payments); Jay Stanley & Daniel Kahn Gillmor, *New Mobile Phone Service Shows We Can Have Both Privacy and Nice Things*, ACLU (Feb. 15, 2023), https://www.aclu.org/news/privacy-technology/new-mobile-phone-service-shows-we-can-have-both-privacy-and-nice-things (on the use of privacy-enhancing technologies in a telephone network); Kaitlin Asrow & Spiro Samonas, *Privacy Enhancing Technologies: Categories, Use Cases, and Considerations*, Fed. Rsrv. Bank S.F. (June 1, 2021), https://www.frbsf.org/banking/wp-content/uploads/sites/5/Privacy-Enhancing-Technologies_FINAL_V2_TOC-Update.pdf.

could create a checkpoint society where we get asked for ID at every turn. Want to enter a convenience store? Scan your ID. Want to enter a national park? Scan your ID. Want to browse a bookstore, buy groceries, or park your car? Scan your ID.

And that dynamic becomes even more intense once it's extended to the internet, where every web site and service starts demanding not just an email address, but your full, inescapable super ID. We already live in a digital advertising ecosystem that goes to great lengths to connect our online and offline activity to key identifiers. There is already far too much tracking of people online in general, and polls show Americans are very uncomfortable with it.[3] But that tracking is far from perfect and has been the subject of growing pushback in recent years.[4] If not properly designed and executed, digital IDs may make such tracking inescapable. We may wake up one day and find that overnight, if we want to watch a YouTube video, or log on to social media, or look at a news site, we get a popup demanding that we "click here to send us your digital ID."

Currently, people have a lot of flexibility to offer different log-in information for different accounts. Depending on how much we trust a web site, we can use different email addresses, different login handles, and choose whether to provide real full names. This flexibility empowers individuals. It allows us to choose when and to whom we wish to reveal our identity, and when we want to remain anonymous or pseudonymous. To provide your real identity is to enter a lifetime relationship with a company or web site — they will always be able to find you. For many reasons, people don't always want that.

A powerful Big Tech motivation for demanding super IDs is likely to be marketing. As some other techniques for tracking people online, such as cookies, lose their utility, companies are hungry for alternate ways of identifying people so they can collect reliable personal data for advertising, have a reliable unique identifier so they can track us across different sites, and increase the value of the data they collect.[5] In addition to marketing, this data can also enable companies to engage in surveillance pricing, where people are charged different prices based on data collected about them and what that suggests about the intensity of their need, what they are

---

[3] Michelle Cao, *Nearly Three-Fourths of Online Households Continue to Have Digital Privacy and Security Concerns*, Nat'l Telecomms. & Info. Admin. (Dec. 13, 2021), https://www.ntia.gov/blog/2021/nearly-three-fourths-online-households-continue-have-digital-privacy-and-security-concerns; Colleen McClain et al., *How Americans View Data Privacy*, Pew Rsch. Ctr. (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

[4] Jane Wakefield, *Facebook v Apple: The Ad Tracking Row Heats Up*, BBC (Apr. 25, 2021), https://www.bbc.com/news/technology-56831241; Anthony Chavez, *The Next Step Toward Phasing Out Third-Party Cookies in Chrome*, Google (Dec. 14, 2023), https://blog.google/products-and-platforms/products/chrome/privacy-sandbox-tracking-protection/.

[5] The loss of utility comes from several sources, including the "death of tracking cookies," the influence of EU privacy law, and changes to the operating system on Apple's phones, which limit advertisers from accessing an iPhone user identifier. Google has also moved toward limiting the tracking technology in its Chrome browser and in the Android phone operating system. *See* Owen Ray, *Tracking Cookies are Dead: What Marketers Can Do About It*, Invoca Blog (Oct 2. 2023), https://www.invoca.com/blog/tracking-cookies-are-dead-what-marketers-can-do-about-it; Brian X. Chen, *To Be Tracked or Not? Apple Is Now Giving Us the Choice*, N.Y. Times (Sept. 29, 2021), https://www.nytimes.com/2021/04/26/technology/personaltech/apple-app-tracking-transparency.html; Brian X. Chen & Daisuke Wakabayashi, *You're Still Being Tracked on the Internet, Just in a Different Way*, N.Y. Times (Apr. 6, 2022), https://www.nytimes.com/2022/04/06/technology/online-tracking-privacy.html.

willing or able to pay, or just who they are.[6] Other motivations are likely to be cybersecurity ("We need to know who is on our site in case they turn out to be a bad actor"), terms-of-service enforcement ("We need to make sure you aren't someone we've previously banned"), a desire to screen out AI bots, and age verification.

These kinds of dynamics could lead us toward a "checkpoint society" where an increasingly dense net of identity checkpoints and access controls is woven throughout American life, online and off. It could become impossible to do anything without proving your identity. That would mean a significant loss not only of privacy and control, but also an erosion of Americans' ability to engage in anonymous speech, learning, and association. Anonymous speech has been an important American tradition since the nation's founding — the Federalist Papers and many pro-revolutionary pamphlets were written anonymously, for example — and it brings many benefits, including the ability to speak truth to power, to freely associate and exchange ideas, and to seek information about and support for conditions and experiences that many find embarrassing to disclose.[7]

Verification of a person's real identity is currently difficult, cumbersome, and expensive, and as a result is not usually asked of customers unless absolutely necessary. Once we create a way of proving our identity that is quick and easy, demands will proliferate.

**b. Digital IDs enable centralized tracking of presentations**

Another danger posed by a digital ID is that, depending on how an ID system is architected, it could allow people's presentations of their ID to be tracked. When I present my plastic driver's license at a wine store to prove I'm over 21, generally, no record of that interaction is created, and it remains between me and the clerk.[8] Digital technology, however, magnifies the potential for those presentations to be recorded, reported, and tracked.

In digital identity systems that permit such tracking, information could be gathered by the issuer (in the case of digital driver's licenses, that would be motor vehicle departments or the contractors that they hire) about every bar, club, casino, office lobby, bank, pharmacy, doctor's office, sporting arena, concert venue, and airport that an ID holder visits; every convenience store beer purchase, equipment rental, or hotel check-in; every application for social services; and every other circumstance in which they may be asked to show an ID. And again, if a digital identity system starts being used online, that list could grow exponentially to cover the web sites and online services a person uses. And digital IDs would also make it trivial for those stores, bars, banks, and other establishments to gather and share data to tie every transaction to your real identity, and then monetize that data, unless Congress provides meaningful safeguards.

---

[6] Jay Stanley, *Digital Driver's Licenses Could Make "Surveillance Pricing" Much Easier for Companies*, ACLU (Sept. 15, 2025), https://www.aclu.org/news/privacy-technology/surveillance-pricing-and-ids.

[7] *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995) (anonymous election- and issue-related leaflets); *Talley v. California*, 362 U.S. 60 (1960) (anonymous handbills).

[8] See Heather Brown, *What Do Driver's License Scanners Do With Our Information?*, CBS News (Mar. 3, 2022), https://www.cbsnews.com/minnesota/news/drivers-license-scanners; Dana Fowle, *Retailers Scanning Drivers Licenses Raises Privacy Issues*, Fox 5 Atlanta (Jan. 21, 2022), https://www.fox5atlanta.com/news/retailers-scanning-drivers-licenses-raises-privacy-issues.

Some digital ID systems may also provide for IDs that electronically ping their issuers at regular intervals, or allow issuers to arbitrarily reach into users' wallets to alter or revoke their IDs. This sets the stage for abuses (such as taking away IDs from the authorities' political opponents or revoking IDs without due process) and threatens to invade identity holders' privacy by providing the issuer with information about the holder such as their IP address, which can reveal location and other information.[9]

### c. Further disadvantaging those without technology

If digital IDs become mandatory, either legally or practically, that would have significant implications for equity and the "digital divide" by disadvantaging those who don't have a smartphone or other necessary devices. That is a surprisingly large group of people, including many from our most vulnerable communities. Studies have found that about one in ten people in the US do not own a smartphone, including over one-fifth of people over age 65.[10] People with disabilities are less likely to own a smartphone, and many who are unhoused also lack access.[11] Some may lack the resources to afford a smartphone and mobile data access, while others may lack the technological literacy to use them; in 2018 a study found that about 40% of seniors weren't able to install a mobile app on a smartphone.[12] While the number unable to do so has probably grown since that study was published, there almost certainly is a portion of the population who remains unable to do so.

To worsen inequality, digital IDs need not become legally mandated, just practically required. There's no law that says every American has to get a credit card or driver's license, but it's hard to participate fully in society without one, and those who lack them suffer significant disadvantages in today's world. If digital credentials also become practically required, the negative effects would be even more intense, even though there is also no law that says every person has to own a smartphone.

### d. Capture by private companies

The provision of driver's licenses and other government identity documents is a public act. The showing of identity or attribute authentication for government services or where required by law is not something people will have a choice over. Therefore, any digital identity system should be considered essential public infrastructure, and people should not be required to do business with any one company or small number of companies in order to participate in this system. Yet there is a danger that one company or a small number of companies (such as the dominant wallet providers Apple and Google) come to play gatekeeper roles in a digital identity system. That may allow them to abuse their position to cement their market power, engage in blocking and censorship of ID uses, the tracking of individuals, or the imposition of fees or other rent-seeking

---

[9] Jay Stanley, *How to Give the Government New Power to "Un-Person" Someone, in Three Easy Steps*, ACLU (Jan. 5, 2026), https://www.aclu.org/news/privacy-technology/un-personing-with-digital-id.

[10] *See Mobile Fact Sheet*, Pew Rsch. Ctr. (Nov. 20, 2025), https://www.pewresearch.org/internet/fact-sheet/mobile/.

[11] *See* Andrew Perrin & Sara Atske, *Americans With Disabilities Less Likely Than Those Without to Own Some Digital Devices*, Pew Rsch. Ctr. (Sept. 10, 2021), https://www.pewresearch.org/short-reads/2021/09/10/americans-with-disabilities-less-likely-than-those-without-to-own-some-digital-devices/.

[12] Chui Yin Wong et al., *Usability and Design Issues of Smartphone User Interface and Mobile Apps for Older Adults*, 886 Commc'ns in Comput. & Info. Sci. (2018), https://link.springer.com/chapter/10.1007/978-981-13-1628-9_9.

behavior within the identity ecosystem. Or they may simply deny people the ability to do business with other companies in a healthy free market.

## II. IF A DIGITAL ID SYSTEM IS CREATED, IT MUST BE DONE RIGHT

If we are to create a digital identity system in the United States, we need to make sure we build it in such a way that it does not become an infrastructure that allows us to be tracked and regimented in new ways. If digital IDs are not to become the functional equivalent of a national ID ankle monitor everyone is forced to wear, they need to have certain technological features and certain legal protections. We urge Congress to require and ensure that any digital ID systems have these features.[13]

### a. Technological safeguards

The technological protections that should be incorporated into a digital ID include (but are not limited to):

1. **No tracking.** A system must not allow ID issuers visibility into where and when an ID is presented to a verifier.
2. **Holder control.** An ID holder — the individual to whom the ID belongs — should have technological control over what data they reveal to a verifier, allowing them to reveal some fields of data and not others, and to reveal characteristics such as "over age 21" without revealing details such as the holder's date of birth, or "resident of county" without revealing their address. Such "selective disclosure" is one area where a digital ID can have advantages for privacy over a physical ID, and that advantage should be fully made use of.
3. **Unlinkable presentations.** When the holder presents their digital credentials, the verifier should be unable to link that presentation with others from the same holder. For example, the verifier should not be able to tell that the "over 21" person buying a case of beer today is the same person who bought a bottle of wine last week. This limits the ability of any verifier (or their vendors) to assemble a map of data about who does what where.
4. **Verifier transparency.** An ID holder should have transparency into who is requesting identifying or authenticating information, their authority for making that request, what the specific circumstances and purpose of the request are, what information is and has been transmitted, and if that transmission involves third parties.
5. **Open, not proprietary.** If the United States is to adopt a digital ID, it's also vital that that ID be open and free of proprietary strings. There must be no one corporation, or small handful of corporations, that Americans are de facto required to deal with in order to participate in a digital identity system. The system must be clearly documented and open enough that it is possible for any party with the relevant skills to build an interoperable digital wallet that any legitimate ID holder can use or an interoperable verifier tool that any legitimate verifier can use. No system that our society depends upon should be built on proprietary specifications, proprietary hardware, or patent-encumbered technology.

[13] For more detail on the ACLU's recommended safeguards on digital IDs, see *ACLU Digital ID State Legislative Recommendations*, ACLU (Oct. 2024), https://www.aclu.org/publications/aclu-digital-id-state-legislative-recommendations.

**b. Legal safeguards**

In addition to technical protections built into digital IDs, Congress should consider establishing legal safeguards to protect individuals from surveillance and governmental incursions:

1. **An empowering option, not an imprisoning requirement.** It is vital that people be provided with multiple options when it comes to identifying themselves. Providing a means for digital identification or authentication can be empowering if it gives people a new choice in how they do so. For people with certain disabilities, it can be critically important to have remote options (to verify their ID from their home, for example, rather than in a Post Office). At the same time, remote processes can be inaccessible for the many individuals who lack access to smartphones with cameras, reliable internet service, or who simply are less familiar with how to use complex technology. People should never be locked out of critical services because of a lack of technology to engage in identity verification processes.

   The use of digital IDs should never become mandatory as either a legal or practical matter. We believe that people should have a right to obtain and use paper, plastic, or other physical identity documents instead of or in addition to a digital ID. Digital IDs should be accompanied by policies that bar those engaging in identification from refusing to accept physical IDs on a reasonably equal basis. Government verifiers should also be required to provide a meaningful in-person option. Digital identification must be an empowering option for people rather than a disempowering requirement. Otherwise, a digital ID system will inevitably deny significant numbers of vulnerable people access to benefits to which they are legally entitled.
2. **Protections against excessive identity demands.** As discussed above, a digital identity system, by making it very easy to share our ID, is likely to lead to a significant expansion in the times and places where our IDs are demanded. As a result, no digital identity system should be rolled out without properly enforced legal limits on when those engaged in commerce or other regulated activities may demand that people prove their identity with these super IDs.
3. **Protections against data collection by verifiers and wallet providers.** Verifiers in any system of digital IDs should have concrete legal obligations to minimize collection and retention of data, with appropriate consequences for violations. This should include a duty of loyalty, such as has already been adopted by at least one state.[14] Wallet providers must also be barred from surveilling their users.
4. **Protection of an open wallet ecosystem.** To prevent the insertion of a private for-profit company in an identity infrastructure, policymakers must create the regulatory conditions for a flourishing open wallet marketplace that allows anyone, including open-source providers, to create a wallet that can host a digital identity document, provided they meet general security and other standards. The provisioning process by which data from issuers is loaded onto people's devices should be standardized so that anyone meeting the standards can write a wallet app and holders will have choices in which wallet they use.

[14] Jay Stanley, *Utah Passes Nation's Strongest Digital Identity Bill*, ACLU (Mar. 30, 2026), https://www.aclu.org/news/privacy-technology/utah-digital-id-law.

## III. DIGITAL DRIVER'S LICENSES ARE THE MOST LIKELY FORM OF DIGITAL ID TO BECOME WIDESPREAD

A broad variety of proposals for digital identification systems have been created, and it would be preferable if we could create a future where there are multiple, independent digital ID systems giving individuals choices. But digital versions of the driver's licenses (or non-driver IDs issued by state motor vehicle agencies) are the avenue by which most people are likely to end up initially using or being forced to use a digital identity.

**a. Driver's licenses are already the most common form of identification used by Americans**
The nation's motor vehicle departments have long had the power to put an identity document in most Americans' pockets. While it is important to stress that a significant number of people in the US do not have government IDs, 85% of Americans 14 and older have some form of driver's license according to the Federal Highway Administration, with some additional number having non-driver's IDs.[15] That is why DMV-issued identification is the most commonly used form of government ID. That makes driver's licenses a natural foundation for a digital ID; the DMVs have the administrative capacity to verify and produce IDs, and many Americans are already accustomed to getting their IDs there — and have to do so anyway in order to drive. The deeply problematic but now decades-old Real ID Act further recognized and entrenched the DMVs as the de facto source of identification for most Americans.

**b. Significant problems with current ID-proofing techniques will drive adoption of digital driver's licenses**
Many are looking to digital driver's licenses because existing forms of digital identity verification are deeply problematic. Perhaps even more than a digital driver's license, these systems require the ability to have and use technology — a computer, a camera, a good internet connection, and the technological literacy to use all of them according to the verification services' instructions. This can pose significant barriers to individuals legitimately claiming government benefits.

The collection and use of detailed surveillance information on individuals that is collected in often unethical ways (such as through phone apps that secretly report location data) without their meaningful knowledge or consent is also deeply problematic. Biometric and behavioral analytics tools used for remote fraud monitoring may improperly capture and retain user information, including sensitive health information. For example, mouse movements have been used to identify cognitive impairments and screen individuals for Parkinson's disease.[16]

Companies that assemble information about individuals from diverse sources will also face a constant incentive to monetize that data for purposes unrelated to identify verification. In addition, when Congress eventually enacts the kind of strong overarching privacy legislation that

[15] *Highway Statistics 2024*, U.S. Dep't of Transp. Fed. Highway Admin. (Feb. 2026), https://www.fhwa.dot.gov/policyinformation/statistics/2024/dl20.cfm.
[16] Kryzstof Gajos et al., *Computer Mouse Use Captures Ataxia and Parkinsonism, Enabling Accurate Measurement and Detection*, Wiley InterScience (Jul. 8, 2019), https://movementdisorders.onlinelibrary.wiley.com/doi/10.1002/mds.27915.

Americans want, much of the surveillance data now being used for identity verification will dry up.

Layered on top of that data collection is the problematic use of AI algorithms for analyzing the data to make decisions. As the ACLU explained in comments to the National Institute for Standards and Technology (NIST) on its digital identity guidelines, risk-scoring tools can introduce errors and biases into fraud detection, often in ways that are difficult for victims or regulators to understand.[17] The opacity of AI, in addition to the opacity of private, for-profit companies, makes it hard for victims of false-positives to receive due process.

**c. There is already significant interest and activity in the states on digital driver's licenses**
An estimated 20 states have already implemented mobile driver's licenses, with others in various stages of preparation or consideration of doing so.[18]

**d. Even the federal government is also moving to rely on state driver's licenses**
In addition, the federal government's Login.gov site is reportedly preparing to accept digital driver's licenses as part of its identity-verification procedures. That will place driver's licenses squarely in the middle of not just state and private-sector identity verification, but federal government verification as well.[19]

## IV. THE MOBILE DRIVER'S LICENSES THAT MANY STATES ARE ADOPTING SHOULD NOT BECOME THE STANDARD

The mDLs that many states are starting to adopt do not have the design qualities or legal protections needed to protect people's rights. mDLs are based on a standard created by the International Organization for Standardization (ISO) behind closed doors by a secretive international committee that, so far as we can tell, included representatives of US security agencies like DHS, tech giants, and authoritarian governments. The text of the standard is not available for democratic debate and discussion because it is secret, and it can only be obtained by paying the ISO. If you do pay, you cannot share it or post it online because it is copyrighted.

This is in no way how public policy should be made. The ISO standard is not a legitimate basis on which to move forward and risks creating a national identity system of the kind that Americans have long opposed, especially when embraced without the accompanying legal protections that it requires. Yet the TSA is embracing it, NIST is working with it, and state legislatures are being pushed to adopt it.

---

[17] Elec. Priv. Info. Ctr. & ACLU, Comment to NIST on Digital Identity Guidelines: Enrollment and Identity Proofing, Initial Public Draft (Apr. 14, 2023), *available at* https://epic.org/documents/epic-and-aclu-comments-on-nists-2023-digital-identity-draft-guidelines/.
[18] *Implementation Tracker Map*, mDL Connection, https://www.mdlconnection.com/implementation-tracker-map/
[19] Miranda Nazzaro, *Login.gov Looks to Accept Mobile Driver's Licenses in 'Near Future'*, FedScoop (July 14, 2025), https://fedscoop.com/login-gov-mobile-drivers-license-user-friendly-fraud/; Natalie Alms, *Government is Making Moves on Mobile Drivers Licenses, GSA Administrator Says*, NextGov (July 14, 2025) https://www.nextgov.com/digital-government/2025/07/government-making-moves-mobile-drivers-licenses-gsa-administrator-says/406704/.

Reflecting the lack of public and public-interest stakeholder input, the ISO standard contains provisions for the centralized tracking of presentations (although due to the ISO's opaqueness it's unclear whether they have been removed from the latest official version under pressure from activists and the digital identity community).[20] It also lacks provisions ensuring selective disclosure is implemented to ensure maximal individual empowerment, or requiring unlinkable presentations, verifier transparency, or an open wallet ecosystem free of proprietary standards or patent-encumbered technology. It also lacks protections against abusive revocations.

This form of digital ID is being adopted by states with very little federal input. It is being pushed by tech companies, banks, and the DMVs and their private association in Washington, the American Association for Motor Vehicle Administrators (AAMVA). Although the TSA has the power under the Real ID Modernization Act to influence the shape of this ID, it has so far not been using that power to ensure it doesn't become a national ID system — and to the contrary has incorporated the ISO standard by reference into its regulations, even though those standards are not viewable by the public or by stakeholders unable or unwilling to pay to see them.[21]

Much of the policymaking around mDLs is being done by an opaque and democratically unaccountable private organization, AAMVA, the policies of which lack the force of law and can be changed at any time without public input.

Alternatives to adoption of the illegitimate ISO standard exist. For example, an alternate standard created by the World Wide Web Consortium (W3C) called Verifiable Credentials (VCs) is a superior basis on which to build a digital identity system. And the state of Utah has spurned the mDL model and is building an alternative called State-Endorsed Digital Identity (SEDI), which, while not perfect, includes a great number of the protections that a digital identity system should have and may be gaining support in other states.[22]

## V. COMBATING GOVERNMENT FRAUD IS NOT A SUFFICIENT JUSTIFICATION FOR CREATING A NATIONAL DIGITAL IDENTITY SYSTEM THAT WILL TAKE AWAY AMERICANS' FREEDOMS

Fraud against the government, including through improper payments, has long been a problem, and efforts to reduce it should remain unceasing in any well-governed nation. That said, a certain amount of fraud or theft is always a cost of doing business for any government or private sector program or enterprise.

---

[20] *See, e.g.*, *No Phone Home*, https://nophonehome.com/.

[21] ACLU, Ctr. for Democracy & Tech., Elec. Priv. Info. Ctr., & Elec. Frontier Found., Comments to TSA on Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Waiver for Mobile Driver's Licenses (Oct. 16, 2023), *available at* https://www.aclu.org/documents/comments-to-the-transportation-security-administration; Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Waiver for Mobile Driver's Licenses, 89 Fed. Reg. 85340 (Oct. 25, 2024), https://public-inspection.federalregister.gov/2024-23881.pdf.

[22] Jay Stanley, *Utah Passes Nation's Strongest Digital Identity Bill*, ACLU (Mar. 30, 2026), https://www.aclu.org/news/privacy-technology/utah-digital-id-law.

Perspective is also important. In its April 2026 report "Payment Integrity," the U.S. Government Accountability Office (GAO) estimates that improper payments amounted to about $186 billion in 2025.[23] That is by any measure a significant amount of money. At the same time, it does not justify imposing upon the American people a national identity system that will increase tracking and control of ordinary people, diminish online freedom, including the freedom to engage in anonymous speech, and exclude a significant number of people from accessing important benefits and services.

Furthermore:

- The GAO found that 82% of the improper payments it identified are not payments to unqualified parties, but overpayments to parties who were legitimately eligible for some amount. Overpayments is not a problem that better identity proofing can solve.
- Some proportion of the $186 billion figure is a result of better reporting. The GAO says that the $24 billion increase from 2024 "is largely attributable" to better reporting. In addition, the GAO notes that Congress in 2019 required agencies to begin estimating and reporting on improper payments in programs they administer. We should expect that the reported numbers after that year would be higher than prior years even given an unchanging amount of improper payments.
- Yet, despite that more rigorous reporting, the GAO's data, when adjusted for inflation, shows the amount of overpayments in 2025 is roughly on par with the annual overpayments from the previous 15 years, with the exception of a Covid-era spike that appears to have ended. That suggests that we are not seeing a sudden new plague of improper payments fraud emerging.

Overall, the improper payments problem does not justify imposition of a digital identity system that leads to a checkpoint society and significantly erodes the freedom of Americans, especially when the most significant problem — overpayments — would not be solved by a digital ID system.

[23] *Payment Integrity: Agencies' Estimated Improper Payments Increased to $186 Billion in Fiscal Year 2025*, U.S. Gov't Accountability Off. (Apr. 27, 2026), https://www.gao.gov/assets/gao-26-108694.pdf.