United States House Committee on Homeland Security
Subcommittee on Transportation and Maritime Security
Identity Management Innovation: Looking Beyond REAL ID
Testimony of Jay Stanley, Senior Policy Analyst, ACLU

Chairman Gimenez, Ranking Member Thanedar, and members of the subcommittee: thank you for your attention to the emerging issues around next-generation identity proofing and thank you for inviting me to testify today. I would like to focus on one component of this still-developing ecosystem: digital IDs and the Transportation Security Administration's role in setting applicable government-wide standards. I will touch on three dimensions of digital IDs and TSA's related work: the risks to security, privacy, and equal opportunity; necessary safeguards; and the importance of the TSA slowing down adoption of digital driver's license standards to address those risks and corresponding safeguards.

We believe that a digital identity system could have far-reaching consequences for people's privacy and other civil liberties, potentially leading to an explosion in identification demands. A digital identity system could allow for new ways of tracking us, and further disadvantage those who don't use the technology. Any such system, therefore, must be accompanied by careful technological and legal protections.

If we are to have a digital ID system, it's vital that we take the time to do it right. There is a lot of innovation underway in the digital identity space, including when it comes to privacy protection. The TSA proposes to adopt a "mobile driver's license" standard set by the International Organization for Standardization (ISO) — a standard that was created behind closed doors by a secretive committee at the ISO that, so far as we can tell, was made up of representatives of U.S. security agencies like DHS, tech giants, and authoritarian governments. This ISO standard is inadequate and incomplete when it comes to the protection of our privacy.[1]

In particular, it is vital that any digital ID system this nation adopts be based on open, non-proprietary standards. We are concerned that the TSA also appears to be working extremely closely with one company, Apple, Inc., even signing over to Apple the agency's patents governing the operation of its airport mobile drivers' license checkpoints.[2]

It's also unclear that the TSA has the authority to issue interim compliance waivers for digital IDs, as the agency proposes to do in its August Notice of Proposed Rulemaking.[3] There are also larger questions about why the TSA, with its relatively narrow mission, has been

[1] See Jay Stanley, "Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom," *American Civil Liberties Union* (May 2021), https://www.aclu.org/sites/default/files/field_document/20210913-digitallicense.pdf.
[2] See Jason Mikula, "Apple's Homeland Security Deal Yields Checkpoint, KYC, Voter ID Patents, Documents Suggest," *Fintech Business Weekly* (Sept. 11, 2022), https://fintechbusinessweekly.substack.com/p/apples-homeland-security-deal-yields.
[3] Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Waiver for Mobile Driver's Licenses, 88 Fed. Reg. 60056, 60072 (proposed Aug. 30, 2023).

positioned to determine the shape of an identity system that will affect all of the federal government, and indeed all of U.S. society.

I. A DIGITAL VERSION OF OUR ID MIGHT SOUND SIMPLE BUT WOULD HAVE FAR-REACHING CONSEQUENCES.

A movement is underway to create a digital identity system that would allow people to carry their ID on their phones or on digital smart cards and, eventually, use them over the internet. That might sound handy at first blush, but it would not be as simple as it might sound. The creation of a digital ID — 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 financial access, and more. The adoption of any such system must be approached with great care and deliberation, and accompanied by both technological and legal protections against the negative side effects the creation of a digital ID is likely to have.

The current discussion centers largely around digital versions of people's plastic driver's licenses that can be used for in-person presentations such as at TSA checkpoints, known as "mobile drivers' licenses." But the real game for big tech companies and government agencies is a digital ID that can be used online, and while the former is not without potentially significant ramifications, it is the online digital ID that will be a real game-changer. Since the dawn of the internet, online speech and activity has been relatively anonymous, and much policy discussion in the past three decades has centered on questions of whether, when, and how to verify identities online. Those questions — and their answers — would be fundamentally altered by the development of an easily presentable and ubiquitous digital ID. The possibility that our digital IDs would be required to access not just online governmental services but also social media platforms, news sites, and digital services is reason for great caution in this space. As I will touch on soon, the future of digital IDs and the future of these questions can very much be shaped by Congress and the TSA.

Some say a digital ID is inevitable. We don't know whether that's true. There do seem to be a lot of forces gathering to make it happen, including big banks, tech companies, and other online advertisers. Digital driver's licenses currently being adopted in a number of states are based on a standard created by the International Standards Organization (ISO) — and that organization is currently working to expand the standard to cover online, at-a-distance ID presentations. Even if another standard is adopted instead, it is likely that we will see a continued push for an ID that can be used online. Some of these institutions just want to make existing verification systems easier, while others likely would love to use a digital identity system to track people. If a digital ID system does come about, we do know that this new infrastructure will have a lot of unanticipated consequences, as is always the case with a major new technological and identity infrastructure, going back to the Social Security card created in the 1930's.

Some of those consequences, however, we can anticipate. Negative side effects that a digital ID would predictably create include:

a. An explosion in demands that we prove our identity

A digital ID would make it much easier to present one's full, cryptographically signed, DMV-vetted proof of identity. That also means it will become much easier for all manner of stores and online sites to *request or demand* proof of identity, since it wouldn't be a big ask. A digital ID could create a world where we get asked for ID at every turn. Want to enter a 7/11? Scan your ID. Want to enter a national park? Scan your ID. Want to browse a clothing store, buy a cup of coffee, 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 demands not just an email address, but your full, DMV-vetted ID. We already live in a digital ecosystem that goes to great lengths to connect our online and offline activity to key identifiers. If not properly guarded, digital IDs may simply facilitate that effort. 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 are asked to "press a button and send us your driver's license."

A powerful Big Tech motivation for that 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.[4] 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"), enforcement ("We need to make sure you aren't someone we've previously banned due to violations of our terms of service"), and age verification ("For our legal due diligence, we need to know you're over 13 or we can't market to you"). [5]

Without protections in place, any digital ID that emerges that can be used online is likely to lead to an explosion in online identity demands. The ease and convenience of using a pre-built, government-sanctioned identify proofing as a single-sign on method is likely to prove game-changing. Currently people have the 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 real or fake names and other data. This flexibility empowers individuals. It allows us to choose when we wish to reveal our identity, and when we

[4] 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 Chen, "To Be Tracked or Not? Apple Is Now Giving Us the Choice," *The New York Times* (April 16 2021), https://www.nytimes.com/2021/04/26/technology/personaltech/apple-app-tracking-transparency.html; Brian Chen and Daisuke Wakabayashi, "You're Still Being Tracked on the Internet, Just in a Different Way," *The New York Times* (April 6, 2022), https://www.nytimes.com/2022/04/06/technology/online-tracking-privacy.html.

[5] The Children's Online Privacy Protection Act bars the online collection of personal information from children under 13 without parental permission. 15 U.S.C. § 6502.

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. People don't always want that.

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 also become impossible to do anything without proving your identity. That would mean a significant loss not only of privacy, but also an erosion of Americans' ability to engage in anonymous speech. 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 support online for conditions and experiences that many find shameful to disclose.[6]

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. 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.[7] 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; any applications for social services; and any 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. Digital IDs would also make it trivial for those stores, bars, banks, and other establishments to tie every transaction to your real identity and monetize that data, unless Congress provides meaningful safeguards.

The ISO standard that the TSA proposes to embrace allows for systems in which the verifier (such as a liquor store or web site) electronically pings the ID issuer to confirm that the

[6] McIntyre v. Ohio Elections Commission (1995) (anonymous election- and issue-related leaflets); Talley v. California, 362 U.S. 60 (1960) (anonymous handbills).

[7] See Heather Brown, "What Do Driver's License Scanners Do With Our Information?", *WCCO* (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.

ID is valid. That "server retrieval" method gives the ID issuer a variety of data that can give them a bird's-eye view of when, where, and to whom a person is presenting their ID. The ISO standard also permits offline verifications, which unlike remote over-the-internet verifications don't require the verifier to connect to the issuer or any other third party when doing an ID verification.[8] This is how any digital identity system should work, but we are concerned that some states may use the server retrieval method, thereby creating an infrastructure that allows for the tracking of ID holders.

Some digital ID systems, such as the ISO standard, may also provide for IDs that "phone home" to their issuers at regular intervals. This also 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.

c. Further disadvantaging those without technology

If digital IDs become mandatory, either legally or practically, it could also 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 more than 40 percent of people over 65 and 25 percent of people who make less than $30,000 a year do not own a smartphone.[9] People with disabilities are 16 percent less likely to own a smartphone, and many who are homeless also lack access.[10] Some may lack the resources to afford a smartphone and mobile data access, while others spurn smartphones to protect their privacy or because they just don't see the need. In other cases, a single phone may be shared among family members.

To worsen inequality, digital IDs need not become legally mandated, just practically required. There's no law that says anybody 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 become similarly practically required, the effects would be even worse. This is why we have called for a "right to paper" (see below).

II. ANY DIGITAL ID SYSTEM MUST OFFER SAFEGUARDS

If we are to have a digital ID, we need to make sure we build it in a way so that it does not become an infrastructure that allows us to be tracked and regimented in new ways. That means building both technical and legal safeguards that protect our privacy and guard against overuse.

---

[8] The verifier will need to periodically download verifiers' public encryption key, which is used to cryptographically verify that the digital ID has been digitally signed by the DMV or other issuing party and has not been altered.

[9] See "Mobile Fact Sheet," *Pew Research Center* (April 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/.

[10] See Andrew Perrin and Sara Atske, "Americans with disabilities less likely than those without to own some digital devices," *Pew Research Center* (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/.

a. Technological safeguards

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

- **No tracking.** A system must not allow ID issuers visibility into where and when an ID is presented to a verifier, as discussed above.
- **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 the holder's date of birth, or "resident of county" without revealing their address. This is one area where a digital ID can have advantages for privacy over a physical ID, and that advantage should be made use of.
- **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.
- **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.
- **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 corporate 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.

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:

- **No police access to phones**. By placing people's mobile phones at the center of law enforcement driver's license checks, a digital identity system raises the risk that police officers will gain warrantless access to people's phones, a potentially severe violation of privacy. No one seems to be contemplating a system that *as a technological matter* requires people to hand over their phones, but that is not enough. Many people, especially vulnerable people such as the elderly, immigrants, and members of marginalized communities, may not feel able to decline a police request to hand over or unlock their phone. Despite a crystal-clear constitutional requirement that police must obtain a

warrant for smartphone searches, questionable "consent-based" police searches of people's cell phones happen thousands of times a day.[11] A police officer's request — "mind if I look at your phone?" — may make a search "voluntary" in the eyes of the law, but few searches based on such police requests are truly voluntary. That is especially true for members of poor and marginalized communities. Police officers should be legally prohibited from making requests for "voluntary" taking or search of people's phones.

- **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 legal limits on when those engaged in commerce or other regulated activities may demand that people identify themselves.

- **"A right to paper."** 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. The use of digital IDs should never become mandatory as a legal or practical matter. Digital IDs should be accompanied by policies that bar those engaged in commerce or other regulated activities from refusing to accept physical IDs on a reasonably equal basis.

- **Protections against data collection by verifiers.** Verifiers in any system of digital IDs should come with concrete legal obligations to minimize collection and retention of data, with appropriate consequences for violations. One tempting business model for verifiers will be to offer free verification terminals (for in-person use) or software (for network use) in order to collect data about where and when a person is using their ID. This could be for marketing, surveillance, or other purposes. Even where vendors are well-intentioned, these data collections are attractive targets for hackers, criminals, and espionage agencies.

III. WE NEED TO TAKE THE TIME TO DO THIS RIGHT

Because the emergence of a digital identity standard is likely to have significant consequences and to require development of mitigating policies such as those we outline above, it is important that the United States take care to minimize the negative impacts a digital ID would have. That will take some time.

a. A lot of work is still underway on ID standards and technology.

The standards and technologies we need to build an identity system that protects the interests of ordinary people including privacy are not yet ripe. There is an enormous amount of innovation, invention, and discussion still underway with regards to this technology and to encryption technologies that can allow us to protect privacy even while retaining many useful functions of an ID card.

[11] Riley v. California, 573 U.S. 373 (2014); Logan Koepke et al., "Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones," *Upturn* (2020), https://www.upturn.org/work/mass-extraction/.

As the TSA itself has pointed out, the privacy protections governing mobile driver's licenses are "evolving and unsettled."[12] The ISO standards for mobile driver's licenses (currently ISO/IEC 18013–5:2021) are currently incomplete and address only some aspects of a digital identity system.

One example is the provision in the ISO standard under which IDs "phone home" to their issuers. Under a privacy-protective architecture, an ID holder who needs to perform a specific task such as an update or renewal should be in control of when and how they connect to the DMV (or another issuer) rather than having that built into their phone. These sorts of check-ins should be minimized and infrequent, should be doable over anonymized networks such as Tor and Apple Private Relay, and should be subject to strict data destruction requirements on any metadata gathered by the issuer or their vendor during these check-ins. None of these considerations have been addressed, and if they were debated at all within the ISO the public had no role in or visibility into it. These are the kinds of considerations that need more mature development.

Another example of the system's current immaturity is the implementation of unlinkable presentations, in which a verifier has no way of knowing that the person who is proving they're over 21 is the same person who proved that last week. One way to do this is with a stack of unique, single-use "tickets" (cryptographic tokens signed by the issuer). But there has been little if any discussion of that kind of functionality as part of the ISO standards process, so far as we know.

Other missing components include standards governing the design of digital wallets and their privacy protections, protections for data stored on the phone, mechanisms for the ID holder to receive information about the legitimacy of the requester, and provisioning (the process states use to install a mobile drivers' license in people's wallets).

Even the incomplete ISO standard that the TSA proposes to embrace is only one of a number of approaches to digital identity that are being developed around the world. Interest in digital identity systems has fueled the emergence of an entire community that has been working on the problems of online identity and authorization for many years, including privacy. That movement has created a variety of proposed systems, including a promising open standard created by the World Wide Web Consortium (W3C) called Verifiable Credentials (VCs). VCs are regarded as superior by many in the digital identity community, and should be given time to further evolve and ripen before TSA pushes a standard that is likely to become locked in. Simply put, people are still figuring things out.

[12] Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Waiver for Mobile Driver's Licenses, 88 Fed. Reg. 60056 (proposed Aug. 30, 2023), at 60072.

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 technique that is still in the process of being applied in new areas.[13] As a Federal Reserve Board report put it, privacy-enhancing technologies remain "an emerging category of tools."[14]

b. Any standard that emerges is likely to become "locked in"

We need to be extremely careful about the details of any digital identity system we adopt, because it's going to need to be interoperable across all the states, and potentially across the world. It will likely be adopted by federal agencies, companies, and small businesses across the nation. Therefore, once put in place, it is going to be very difficult to change.

It would be a pity to find ourselves locked into a sub-standard ID system that doesn't make use of the newest innovations in technology, the way we're locked into our QWERTY keyboard standard, where the keys are intentionally placed to slow down typists because early typewriters jammed easily. Yet that is what is in danger of happening.

IV. THERE IS NO NEED FOR THE TSA TO RUSH A DIGITAL ID SYSTEM INTO OPERATION

The TSA's rapid movement toward setting standards (even supposedly interim ones) for state digital driver's licenses is premature and unnecessary, and threatens to create just the kind of lock-in of a substandard system that we should seek to avoid.

a. The federal government has the power to rapidly standardize a digital ID system

Whatever rules the TSA comes up with for federally compliant digital IDs will force the states to comply and are likely to govern what the nation ends up with. Requirements and standards that the TSA sets for federal acceptance of digital identification are going to force states departments of motor vehicles to meet those requirements. The nation's DMVs, in turn, put credentials in the pockets and purses of most Americans, an enormous power that could stifle efforts to create other, superior ID systems. While it's possible that alternative, parallel, competing identity systems emerge and find broad acceptance — which would be a good

---

[13] See Jay Stanley, "Paths Toward an Acceptable Public Digital Currency," *American Civil Liberties Union* (March 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 and Daniel Kahn Gillmor, "New Mobile Phone Service Shows We Can Have Both Privacy and Nice Things," *American Civil Liberties Union* (February 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).

[14] See Kaitlin Asrow and Spiro Samonas, "Privacy Enhancing Technologies: Categories, Use Cases, and Considerations," *Federal Reserve Bank of San Francisco* (June 1, 2021), https://www.frbsf.org/banking/wp-content/uploads/sites/5/Privacy-Enhancing-Technologies_FINAL_V2_TOC-Update.pdf.

thing — it's likely that the driver's license will continue to remain the primary ID that Americans use when asked to prove their identity, age, or residency.

b. TSA is adopting standards that are not optimal

The TSA proposes to adopt an ISO "mobile driver's license" standard that was created behind closed doors by a secretive committee at the ISO that, so far as we can tell, was made up of representatives of U.S. security agencies like DHS, tech giants, and authoritarian governments. This ISO standard would allow for IDs that "phone home" to the DMV (or its corporate contractor), and allow tracking of where, when, and to whom an ID holder is showing their ID. As discussed above, it is also incomplete. [15]

The TSA also appears to be working extremely closely with Apple, Inc. Documents obtained by journalist Jason Mikula reveal that the TSA has entered into contracts that appear to give Apple significant power over the implementation of mobile drivers' license checkpoints. For puzzling and unclear reasons, the TSA even signed over to Apple the agency's patents governing the operation of its airport mobile drivers' license checkpoints.[16]

c. There's no hurry for the TSA.

Any increased use of digital driver's licenses won't speed people through airline security — ID checking is not the bottleneck — and it won't free people from having to carry their physical ID cards, since, as the TSA warns, "You must still carry your physical ID."[17]

Nor is there a popular clamor for digital IDs from residents of the states. Those that have rolled out digital driver's licenses have not had substantial public sign-on. Alabama, for example, has had a digital driver's license available to residents since 2015, but was rarely used even as mobile payments skyrocketed. Digital IDs are being driven by vendors and other corporations, eager to define digital driver's licenses as "the future" and conjure a non-existent public excitement about the technology.[18]

d. There are serious questions about the TSA's authority to dictate ID standards for the whole U.S. government

The authority of the Department of Homeland Security to regulate the forms of identity that are accepted by the federal government stems from the Real ID Act of 2005 and the Real ID

---

[15] See Jay Stanley, "Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom," *American Civil Liberties Union* (May 2021), https://www.aclu.org/sites/default/files/field_document/20210913-digitallicense.pdf.

[16] See Jason Mikula, "Apple's Homeland Security Deal Yields Checkpoint, KYC, Voter ID Patents, Documents Suggest," *Fintech Business Weekly* (Sept. 11, 2022), https://fintechbusinessweekly.substack.com/p/apples-homeland-security-deal-yields.

[17] See "Biometric and Digital Identity Solutions For TSA PreCheck Members," *Transportation Security Administration,* https://www.tsa.gov/digital-id.

[18] See Lauren Walsh, "Alabama's digital driver's license: What you need to know," *ABC 33/40* (Oct. 8, 2018), https://abc3340.com/news/local/alabamas-digital-drivers-license-what-you-need-to-know.

Modernization Act of 2021.[19] Those acts direct the Secretary of DHS to promulgate regulations specifying compliance requirements, and to certify state compliance therewith. Those acts do not contemplate the issuance of interim compliance waivers that permit the federal acceptance of identity documents that are not subject to requirements created through the regular regulatory process, which is what the agency proposes in its August Notice of Proposed Rulemaking.[20]

Also questionable is DHS's decision to delegate its authority under these acts to its sub-agency TSA. This creates a situation, not contemplated by Congress, in which an agency with a narrow mandate of protecting the safety of aviation, and which has an interest only in one narrow use of identity documents (matching against airline tickets), is positioned to determine the shape of an identity system that will affect all of the federal government, and indeed all of U.S. society.

V. CONCLUSION: THIS IS A BIG DECISION WITH FAR-REACHING RAMIFICATIONS, AND WE SHOULD TAKE THE TIME TO GET IT RIGHT.

The major questions about any digital identity system are whether it will be designed to protect privacy to the maximum extent possible, and whether people will be forced to participate in it. Will it be built to give control *to* people, or built to spy on people and increase the control of government agencies and companies *over* people? Making somebody show ID is sometimes necessary, but it's also an act of power. Who should be able to require someone else to identify themselves? What can the requestor do with that information once they have it? What recourse does the identified person have if the requestor misuses the information? These questions should be answered before we rush into locking in a sub-optimal digital identity system.

[19] REAL ID Act of 2005, Pub. L. 109–13, div. B, title II, § 202(a)(1), (c)(3), 119 Stat. 311 (2005) (codified as amended at 49 U.S.C. § 30301 note); REAL ID Modernization Act, Pub. L. 116–260, div. U, title X, § 1001(b)(2)(D), 134 Stat. 2304 (2020) (codified at 49 U.S.C. § 30301 note) (amending the REAL ID Act § 202).
[20] Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Waiver for Mobile Driver's Licenses, 88 Fed. Reg. 60056, 60072 (proposed Aug. 30, 2023).