ACLU Digital ID State Legislative Recommendations

Vesion 1.0
October 2024

Topic Summary

When states consider adopting digital driver's licenses (a.k.a. mobile driver's licenses or mDLs), they often view it as a relatively minor step that merely creates a digital form of a plastic license. That couldn't be further from the truth; a digital ID will be far more powerful than a plastic one and will open up a Pandora's Box of potential privacy, equity, and other issues.

The ACLU produced an in-depth report on digital driver's licenses in 2021 where you can find more detail about this issue. But the big danger is that the infrastructure supporting digital driver's licenses will have the ability to track people's activities and to collect much more personal data than plastic licenses. These efforts may also exclude people who do not have access to mobile phones or other technological infrastructure and enshrine giant tech companies as monopolistic, voyeuristic middlemen every time Americans need to prove things about themselves. That will be even more true if such an ID expands from in-person presentations to online use, which is the real goal of many digital ID supporters.

Once it becomes easy to share your ID with the press of a button, the danger is that we start getting identity demands from all quarters. Want to enter a 7-Eleven? Scan your ID. Want to browse a clothing store, buy a cup of coffee, park your car? Scan your ID. Want to watch a video, or log on to social media, or look at a news site? "Click here to send us your digital ID." There is already far too much corporate tracking of Americans, and polls show Americans are

very uncomfortable with it. But that tracking is far from perfect. A digital ID could make it inescapable.

And in such a world, what happens to the surprisingly high number of Americans who don't have smart phones or the tech savvy to use them? What happens when someone's phone dies — will they go to jail?

A digital ID system can protect privacy and equity and yet remain cryptographically sound and just as resistant to fraud as a less privacy-protective system. But that won't happen unless the digital ID system is built to do so.

The current landscape for digital identity standards and technology is immature. It's the subject of rapid innovation as well as multiple emerging industry and government standards that are still in development. That means that it's too soon to rush to embrace incomplete and inadequate standards such as those developed by the International Organization for Standardization (ISO).

It also means that there's still space for far-sighted legislators to lead the way in creating a digital ID system that aggressively protects privacy. Today states have wide latitude in creating digital versions of driver's licenses, but eventually they're going to need to be interoperable. States must act now to direct that digital driver's licenses be designed so they can't become the kind of national identity and tracking system that Americans have always opposed.

State legislatures don't typically legislate technical details, but there are some very basic value judgments involved in how a digital ID is architected. To take just one example, should a digital ID "phone home" to the issuer every time it is verified, creating a centralized digital record of every store and web site where a person has used their ID? Or should it operate offline so that it doesn't phone home?

Some standards — particularly the International Organization for Standardization (ISO) standards being adopted in some state laws — allow for both a "phone home" functionality, and an "offline" functionality. Should the decision of which of those two architectures a state selects be up to technocrats at the state motor vehicles department? No — that architectural decision is also a *values* decision, one that is too important to leave up to implementers.

The same holds for a number of other fundamental design decisions for a digital ID. Below we outline these key decisions, as well as legal protections, that state legislators should insist upon before authorizing or enabling a digital driver's license or other digital ID system in their state. The European Union has done just this — requiring protections similar to the below while leaving the technical implementation to others. Americans should not have worse privacy with their IDs than Europeans.

Summary of recommendations

Our 12 specific recommendations are listed below, followed by proposed legislative language for each item, preceded by an explanation of each item and its importance.

1. No police officer access to phones
2. No Issuer ability to track via "phone home" mechanism
3. Granular control over data released (selective disclosure)
4. Unlinkability by verifiers (no digital ID as a 'super cookie')
5. An open ecosystem
    a. Open wallets
    b. Private wallets
    c. Transparent source code
    d. A standardized provisioning process
6. Verifier accountability
7. A reporting requirement
8. No remote government "kill switch" to disable people's IDs
9. A "right to paper"
10. Restrictions on ID demands
11. Restrictions on data use
12. Enforcement through a private right of action

Recommendations

Definitions
"Digital ID" shall mean any digital document, file, or other instrument issued to the public by or on behalf of the state, or any political subdivision thereof, and used for proof of a person's identity or of some attribute or authorization that they possess.

"Digital driver's license" shall mean a Digital ID that is a digital form of a driver's license or other non-driver state ID issued by the state.

"Digital wallet" shall mean an application accessed on device or remotely that permits a Holder to Present a Digital Driver's License or other Digital ID in-person, online, or through other remote means.

"Issuer" shall mean the state or political subdivision that issues a Digital Driver's License or other Digital ID, or an any party that acts as an agent or contractor of, on behalf of, in partnership, conjunction, or cooperation with, or who otherwise assists the state or political subdivision in producing Digital Driver's Licenses or other Digital IDs or making them available to Holders and/or Verifiers.

"Holder" shall mean the person who possesses a Digital Driver's License or other Digital ID that establishes proof of that person's identity or of some attribute or authorization that the person possesses.

"Verifier" shall mean a party who performs a check on a Holder's Digital Driver's License or other Digital ID in order to establish proof of a Holder's identity or of some attribute or authorization that they possess.

"Verification tool" shall mean a device that is used by Verifiers to exchange data with the holder's wallet during presentation and verify the authenticity of that presentation.

"Selective disclosure" shall mean the disclosure of only the data fields from a Digital Driver's Licenses or other Digital IDs that are reasonably necessary for the purpose of the Presentation, and the ability of a Holder to choose which fields of data from a digital ID are revealed during a Presentation.

"Attribute authentication" shall mean the ability of a Digital Driver's License or other Digital ID to affirmatively and accurately prove to a verifier that something the Holder claims about themselves is true without revealing the underlying data.

"Person" means a natural person or individual.

"Presentation" shall mean the act of revealing all or any portion of a Digital Driver's License or other Digital ID to a Verifier.

"Offline presentation" shall mean a presentation and verification process that involves no internet connection and no transferring, copying, or recording of electronic data between any parties other than the Holder and the Verifier.

"Open source" shall mean software that is freely available for public inspection, modification, and redistribution without restriction.

"Provisioning" shall mean the act of enrolling a Holder in a Digital Driver's License or other Digital ID scheme by an Issuer.

1. No police officer access to phones

Because of the large amount of personal data most people hold on their smartphones today, it is important to ensure that, when a person uses their phone to present their Digital ID, police officers or other verifiers do not end up gaining access to other data in that phone. Standards and technologies must be designed so that holders never need to relinquish control of their smartphone to any verifier. When it comes to law enforcement, technology design should be reinforced through policies that prohibit "voluntary" requests to hand over devices (which are never truly voluntary when the requester is a police officer).

Language Recommendation:
[State or political subdivision] shall not adopt a Digital Driver's License or other Digital ID that is designed to, incentivizes, requires, or functions better with verifiers taking possession of a person's phone during the verification process. No law enforcement officer shall, in the course of their duties, take physical possession of a person's personal digital device for purposes of verifying their identity.

2. No Issuer ability to track via phone home mechanism

One way a digital ID can differ from physical ID is that it can enable the issuers of the digital ID to track where, when, and to whom one shows their ID. This tracking can reveal very private and sensitive information about the digital ID holder — namely, when and where, online or off, they present their ID. Standards and technologies should be designed so that the issuer (or any of its agents or contractors) cannot engage in any of these forms of tracking.

Language Recommendation:
No part of the technology involved in a Digital Driver's License or other Digital ID system utilized by [state or a political subdivision]shall disclose any data regarding a Holder's presentation of their Digital Driver's License or other Digital ID to the Issuer.

3. Granular control over data released

One of the privacy advantages that digital IDs have over physical ones is that they can provide "selective disclosure." That means that a holder can reveal some parts of their driver's license — their date of birth or zip code, for example, without revealing anything else. Even better, digital IDs can allow for "attribute authentication," in which qualities of one field are shared without revealing the underlying data in that field. For example, such an ID can allow a holder to prove that they are over 21 without revealing their date of birth or exact age, or that the holder is a resident of a town without revealing their address. Since the move to digital makes these privacy protections possible, there is no reason not to incorporate them into a digital ID system.

Language Recommendation:
A Digital Driver's License or other Digital ID system shall provide for Selective Disclosure and allow for an Attribute Authentication capability, including proof of meeting the minimum age for restricted product purchases, as well as any other commonly requested eligibility standards that wallet designers see fit to provide.

4. Unlinkability by verifiers

We don't want a digital IDs to become a unique identifier — a "super cookie" that allows websites and stores to track us across the physical and online world in a way that would never be possible with a physical ID. Standards and technologies should be designed to ensure multiple Verifiers cannot work with each other to compile records of where people are presenting their digital ID. For example, a convenience store chain shouldn't be able to see all your stops as you drive across the state or country.

Available options to protect privacy against such tracking include single-use credentials (in which the DMV or other issuer provides a digital "stack" of unique IDs, each of which is used with a different verifier) or cryptographical techniques such as anonymous credentials, which let a holder repeatedly prove they have an attribute (e.g., that they are old enough to buy an age-restricted product) without sharing a unique, linkable identifier. The details would need to be worked out by implementers, but the underlying goal of Unlinkability should be dictated by the legislature.

Language Recommendation:
A Digital Driver's License or other Digital ID shall include techniques and methodologies that ensure that multiple presentations of non-unique data (selected fields and attribute authentications) by a Holder cannot be linked together by one or more Verifiers.

5. Open and private wallets, transparent source code, and a standardized provisioning process

The provision of driver's licenses and other government identity documents is a public act, and any digital identity system should be considered essential public infrastructure – not outsourced to a private company, which may abuse its position to cement its market power. The showing of identity or attribute authentication where required by law is not something people will have a choice over. Therefore, people should not be required to do business with any one company or small number of companies in order to participate in this system. Nor should anyone be required to install and execute government software on their phone or other personal device.

The best way to ensure that these things do not happen in a world where digital IDs are commonplace is to 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 set by the Issuer. The provisioning process by which data from DMVs or other issuers is loaded onto people's devices should be standardized so that anyone meeting the standards can write a mDL app and holders will have choices in which wallet they use. In addition, wallet providers should be barred from collecting any data about their users' presentations.

Language Recommendation:

> *(X) A Digital Driver's License or other Digital ID shall adhere to open standards for wallets and the processes of provisioning and presentation. Those standards may prescribe communications and security measures but must be published, not restricted by patents or other intellectual property ownership, and as a practical matter allow any compliant entity to create a wallet in which holders may store their digital license.*
>
> *(X) An individual shall have a right to carry a digital ID in any wallet of their choice that complies with widely accepted standards for security.*

6. Verifier Accountability

The ISO standard is focused on helping Verifiers securely authenticate Holders, but does nothing to help Holders authenticate Verifiers. How do you know who is asking for your data, and whether they have a right to do so? This is likely to be especially difficult in any online presentations, which lack the physical-world context that does much of that work offline. And what happens if, for example, a liquor store asks for not only your date of birth but also your full name, address, and other information? Under our recommendations the law would allow them no more than a yes/no authentication that the Holder is over 21.

In order to enable accountability for those who inappropriately request digital ID or misuse digital ID data, there must be technical mechanisms in place for citizens to authenticate and record where their ID has been accessed and used. Holders should have full visibility into what

data fields are being requested by a Verifier, control over what is actually sent, and a log (under their exlusive control) of what they have shared.

Language Recommendation:

(1) A Digital Driver's License or other Digital ID shall include standard technical and administrative measures that Verifiers must use to identify and authenticate themselves to a user's digital wallet.

(2) *All digital wallets containing a [STATE NAME] Digital ID shall display to a Holder what data is being requested by a Verifier, the Verifier's identity, and allow the Holder to select what data is and is not transmitted to the Verifier.*

(3) *Such wallets shall also keep a log of each requesting Verifier, what data was requested, and what data was transmitted to that verifier, if any. That log shall be available exclusively to the Holder, who shall be able to delete any or all of it at will.*

7. Reporting requirements

When the legislature requires the inclusion of privacy preserving technology and other protections in a Digital ID system, how is it and the public to know whether the system that is actually built will properly incorporate those protections? In February 2024, the European Parliament enacted digital ID legislation that included many privacy protections. The European Commission, charged with carrying out that law, published a proposed architecture for that system, but experts quickly pointed out that that architecture failed to live up to the law's requirements. State implementers of a Digital ID system should, like the EU, publish a proposed technical architecture for such a system, and seek feedback from experts and other interested members of the public, before implementing it.

How we issue, provision and present digital IDs are fundamental questions of public infrastructure. These decisions involve both technical details and important questions of privacy, accessibility, and other tradeoffs. These questions should not be delegated to closed door agreements, contracts with private vendors or inaccessible processes. Instead, the system should be designed with public input and review, and with the technical expertise of open standard-setting bodies and experts that work in this area.

Language Recommendation:

(1) Prior to deploying a program for issuing a Digital Driver's License or other Digital ID system, or before making any substantive change to such a Digital Driver's License or other Digital ID, the the agency responsible for creating that system shall transmit to the legislature and make public a report on the proposed privacy and accessibility characteristics of that system. It shall include:

- *a) a technical description of how the proposed system complies with the requirements of this Act;*
- *b) a description of any tradeoffs that were made regarding privacy and accessibility.*

(2) The agency shall accept public comment on the proposed system for a minimum of 90 days, consider the relevant matter presented, and then issue a new report explaining the basis and purpose of the decisions made.

8. Don't build in a remote government "kill switch" to disable people's IDs

A plastic license is updated only every 10 years or so, yet many proponents of digital driver's licenses want to give the government the power to revoke them at any time. If digital IDs become necessary for certain interactions online, that gives government the power to revoke a person's ability to participate in those transactions, perhaps with little or no due process. If our worst fears about online identity demands come true, that could paralyze people's ability to engage online without the blessing of the state.

Common approaches for revocation also require either the holder or the verifier to contact the issuer during presentation to check on the revocation status of a credential. This sort of check essentially amounts to "phoning home," and that creates new and unnecessary opportunities for data collection and tracking.

This capability is unnecessary. The only party that truly needs an up-to-the-minute check on whether someone's driving privileges have been revoked is a police officer, and they can contact the DMV to check on the validity of a digital license just as they will continue do when presented with a physical one. Other elements of a license, such as DOB, cannot change over time and do not expire. And while some other elements such as address might change over time, their ability to be updated is not vital and should be up to the holder to initiate, either electronically or in-person at a department of motor vehicles office. A digital ID system should not incorporate remote revocation capabilities and should be designed to operate offline only, except when a Holder wants to set up a remote "appointment" for a specific task such as an update or renewal.

Language Recommendation:

> *A Digital Driver's License or other Digital ID may not permit the Issuer to initiate contact with the wallet for any purpose including revocation or updates. It may allow but not require Holders' wallets to contact or exchange data with the Issuer for those purposes.*

9. and 10. A "right to paper" and restrictions on ID demands

There are many reasons a person might not have a digital driver's license or other digital ID: Many people do not possess smartphones, have access to reliable internet access, or have the technological savvy to participate in a digital identity system. People may worry about the reliability of devices that can lose battery power or just die for no apparent reason. Or they may simply prefer physical documents because they are less malleable, less prone to technical difficulties, and less susceptible to centralized manipulation and control. Therefore it is important that people have a right to obtain and use a physical identity document instead of or in addition to a digital ID. The use of digital IDs should never become mandatory as a legal or practical matter. Policies should bar those engaged in commerce or other regulated activities from refusing to accept physical IDs on an equal basis. An exception would be the inherent advantages of doing business online; an online wine store, for example, would not be expected to ship an order just as quickly for someone who cannot prove their age online.

The digitization of IDs can make it easier for a person to provide ID in some circumstances — but that means it also can make it easier for stores and websites to *ask* a person to provide ID (something they will be economically incentivized to do). As a result, we are likely to see an avalanche of identity demands, especially online, once a website can simply say "click here to send us your ID." That will facilitate tracking and other privacy invasions, and also intensify the equity implications of the technology as those without access to technology or the savvy to use it will increasingly be excluded from resources. Legislatures should limit ID demands outside of specified circumstances, such as the purchase of age-restricted items.

Language Recommendation:

A commercial entity may not:

(1) Condition the offer or use of a good or service on the presentation of a digital or physical driver's license or other government identity document.

(a) Exceptions

(i) Transactions where presentation of proof of identification, age, residency, or other characteristics is required by state or federal law or regulation.

(ii) In financial services where the purpose of an ID request is to ensure that funds, financial instruments, or personally identifiable financial data are not accessed by unauthorized parties.

(iii) In medical services where the purpose is to ensure that goods, services, or personally identifiable medical data are not provided to unauthorized parties.

(2) Charge different prices or rates for goods or services to, provide preferential treatment or a different level of quality of a good or service to, or condition access or entry for, any individual who exercises or elects not to exercise the individual's rights under this subtitle, or who presents a physical as opposed to digital identity document, except as reasonably necessary for conducting a transaction online or through other remote means, taking into consideration available technology.

(3) Where a private entity requires presentation of an ID, they may not require or request presentation of more than the minimum data necessary to determine that a transaction meets legal requirements, including requiring more than a binary "yes/no" attribute authorization for age or other qualifications.

(X) An agency of the state or a political subdivision thereof:

(1) May not condition the offer of an in-person good or service on the presentation of a digital driver's license or other government-issued digital ID.

(2) May not offer a different level of quality of an in-person good or service to any individual who presents a digital or physical form of identification.

11. Restrictions on data use

Where demands for identity or other information are permitted, a digital driver's license makes it much easier to collect, store, and share the data that is on people's licenses. Some states (such as New Jersey) already regulate the collection and use of digital data that is incorporated into driver's license bar codes.

The introduction of a digital form of identification should be accompanied by protections to counterbalance the greater privacy invasions that digital IDs enable. It is also important that wallet providers not monitor the activities of those who hold state driver's licenses or digital IDs, and the state should not allow those who do to participate in the state's digital ID system.

Language Recommendation:

(1) Verifiers and agents or contractors for a governmental Issuer may not collect, retain, share, or use information from a state-issued identity document for longer than what is strictly necessary for the purpose for which that information was presented.

(2) No provider of digital wallets or of verification tools operating in [state or political subdivision] shall access, collect, retain, share, or use identifiable data about the Holder's ID or its use, except as required by state or federal law.

12. Enforcement

Consistent and strong enforcement of civil laws generally requires a private right of action in addition to enforcement by state attorneys general.

Language Recommendation:

(1) An individual alleging a violation of this Act may bring a civil action against the offending entity in a court of competent jurisdiction. A prevailing plaintiff may recover for each violation:

(a) Against an entity that negligently violates a provision of this Act, liquidated damages of $2,500 or actual damages, whichever is greater;

(b) Against an entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;

(c) Reasonable attorneys' fees and costs; and

(d) Other relief, including an injunction or declaration, as the court may deem appropriate.

(2) *For purposes of recovery of damages by an individual under this Act, a repeated violation of this Act by the same party affecting the same individual for the identical use of a digital ID as in a prior violation does not constitute a separate and distinct violation of this Act.*

(3) *The Attorney General of [STATE NAME] may bring an action against a non-governmental entity who violates any provisions of this Act, and shall be entitled to seek*

any forms of relief and remedies available to private plaintiffs, including the collection of damages as a civil penalty.