Digital ID State Legislative Recommendations

Version 2.0
November 2026

Introduction

When states consider adopting digital driver's licenses (sometimes also known as mobile driver's licenses or mDLs), they often view this adoption as a relatively minor step that merely creates a digital form of a traditional plastic license. This couldn't be further from the truth; a digital ID exposes regular people to far more risk of harm than a plastic one. If implemented without rigorous restrictions and substantial avenues for recourse, digital IDs will open a Pandora's Box of privacy, equity, and security issues so severe that these systems may stop resembling driver's licenses at all. In fact, we have identified more similarities between problematic implementations of so-called "digital IDs" and electronic ankle monitors.

The ACLU produced an in-depth report on digital driver's licenses in 2021, where you can find more detail about our concerns. 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 may enshrine giant technology companies as monopolistic, voyeuristic middlemen every time Americans need to prove things about themselves. That will be even more true if such an ID system 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 convenience store? Scan your ID. Want to browse a clothing store, buy a cup of coffee, or 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' everyday activities, and polls show Americans are very uncomfortable with it. But that tracking still has gaps where privacy exists. A digital ID could make it inescapable.

And in such a world, what happens to the surprisingly high number of Americans (disproportionately elderly, disabled, and rural people, and people of color) who don't have smart devices, or to the people who lack the technical facility to use them? What happens when someone's phone dies at a traffic stop—will they go to jail?

Some of these problems, though not all, can be addressed. 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 the state motor vehicles department? Generally, the answer is no—that architectural decision is also a *values* decision and may be too important to leave up to implementation.

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. If the EU can implement digital ID without damaging essential freedoms, Americans should not have to settle for less.

Summary of recommendations

Our 14 specific recommendations are listed below, followed by proposed legislative language for each item along with an explanation of each item and its importance.

1. No police officer access to phones
2. No phone home mechanism
3. Sensible controls over data sharing
4. Unlinkability by verifiers
5. Ensuring holder freedom
    a. Open wallets
    b. Private wallets
    c. Transparent source code
    d. A standardized provisioning process
6. Verifier accountability
7. Reporting requirements
8. No remote "kill switch" allowing the government to disable people's IDs
9. A "right to paper"
10. Restrictions on ID demands
11. Duty of loyalty
12. Restrictions on data use and access
13. Enforcement
14. Liability and reporting requirements for breaches and leaks

Recommendations

Definitions

"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.

"Device" shall mean any piece of equipment or possession that holds or has access to a person's Digital ID.

"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 ID" shall mean any digital document, file, or other instrument issued to any individual 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 wallet" or "Wallet" shall mean an application accessed on a 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.

"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.

"Issuer" shall mean the state or political subdivision that issues a Digital Driver's License or other Digital ID, or 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.

"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.

"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.

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

"Selective disclosure" shall mean the disclosure of only the data fields from a Digital Driver's License 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.

"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.

"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, and any agent, contractor, employee, or partner, performing such a check on behalf of a relying party.

1. No police officer access to phones

Because of the large amount of personal data most people hold on their devices today, it is important to ensure that, when a person presents their Digital ID, police officers or other verifiers do not end up gaining access to other data in that device. Standards and technologies must be designed so that holders never need to relinquish control of their phone, laptop, or other device 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 be3tter when a Verifier has physical access to a Device during the verification process. No law enforcement officer, nor their agent, shall, in the course of their duties, take physical possession of a Person's personal digital Device, or access or direct another Person to access, a Device for purposes of verifying an identity. No law enforcement officer, nor their agent, shall, in the course of their duties, have the opportunity to access or direct another Person to access a Device beyond what is necessary for Presentation. To the extent an officer or their agent does take physical possession of a Person's personal digital Device for purposes of verifying an identity, such physical possession shall not be deemed to be voluntary relinquishment of the Device for any other purpose.

2. No phone home mechanism

One way a digital ID can differ from physical ID is that, depending on how it's designed, it can enable the issuers of the digital ID to track where, when, and to whom any holder shows their ID. This tracking can reveal very private and sensitive information about the digital ID holder—where they bought supplies for a political rally, what medical services they used online, whether

they attend Narcotics Anonymous meetings, and where (and when) they went to church, for example. 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, supporting, implementing, or integrated with a Digital Driver's License or other Digital ID system utilized by [State or a political subdivision] shall disclose any data regarding a Presentation or other use of a Digital Driver's License or other Digital ID to the Issuer or any other party, other than to the Verifier during a Presentation.

3. Sensible controls over data sharing

One of the privacy advantages that a well-implemented digital ID system could have over physical ones is that they can provide "selective disclosure." That means that a holder can reveal some fields of personal information—their date of birth or zip code, for example—without revealing anything else. Digital IDs can also allow for "attribute authentication," in which qualities of a field are shared without the holder having to reveal the underlying data in that field. For example, a holder can prove that they are over 21 without revealing their date of birth or exact age, or that the holder is a local resident without revealing their address. To offer any realistic privacy protections for its constituents, any state making the move to digital should incorporate these privacy protections into its digital ID system and allow for any form of authentication capability that wallet providers build in response to market demand.

Language Recommendation:

A Digital Driver's License or other Digital ID system adopted in [State or political subdivision] shall provide for any form of Selective Disclosure, and allow for any reasonable form of Attribute Authentication capability.

4. Unlinkability by verifiers

We don't want digital IDs to become an inescapable, omnipresent unique identifier—a "supercookie" that allows websites and stores to constantly watch 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 against such tracking include single-use credentials (in which the department of motor vehicles or other issuer provides a digital "stack" of unique IDs, each of

which is used with a different verifier) or cryptographic techniques such as anonymous credentials which let a holder repeatedly prove they have an attribute like age or residency without sharing a unique, linkable identifier). To prevent digital IDs from becoming "universal ankle monitors", states should prevent verifier linkability. 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 adopted in [State or political subdivision] shall include techniques and methodologies that prevent multiple Presentations of data, including non-unique data (selected fields and attribute authentications), by a Holder from being connected, linked, related, or combined in any way that would allow the tracking of an individual's location, choices, behavior, or other conclusions or trends over time by one or more Verifiers, or through collusion or cooperation between an Issuer and a Verifier.

5. Ensuring holder freedom: 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 that 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.

At the same time, people should not be forced to run government code on their personal devices. The best way to ensure freedom of choice for ID holders 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 compliance standards set by the Issuer. Without meaningful pro-competition regulation, the wallet marketplace is likely to default to a handful of companies, thereby making most consumers more vulnerable to hacking and surveillance. The provisioning process by which data from departments of motor vehicles (DMVs) or other issuers is loaded onto people's devices should be standardized so that anyone meeting the standards can write a digital ID app, and holders should have real choices around which wallet they use.

Language Recommendation:

(1) A Digital Driver's License or other Digital ID adopted in [State or political subdivision] shall adhere to open standards for Wallets and the processes of provisioning and Presentation. Those standards may prescribe communications standards 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.

(2) 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.

(3) No entity that offers a Wallet hosting a Digital Driver's License or other Digital ID from [State or political subdivision] may exclude or otherwise disadvantage other Wallets from any application marketplace or operating system that it owns or maintains, except in the case of a failure to adhere to standards mandated under paragraph [1] or in the case of provable and reasonable security or privacy concerns, nor use its market power to the advantage of its own Wallet offering.

(4) Any user agreement necessary for the use of any component of a Wallet utilized in [State or political subdivision] must be written in clear, concise, and plain language.

6. Verifier accountability

The ISO standard is focused on helping verifiers securely authenticate holders, but it 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. Another question is what happens if, for example, a liquor store asks for not only proof that you're of age but also your precise date of birth and your full name and address? Under our recommendations, the law would allow them no more than a yes/no authentication that the Holder is over 21.

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 of what they have shared (under their exclusive control, meaning that it is either only stored locally on the Holder's device or stored in the cloud using end-to-end-encryption) if they are to protect themselves from fraudulent or suspicious requests. This must be balanced, however, with methods to protect the holder's data from unreasonable searches and breaches. This can be achieved through data minimization protocols like timed deletion defaults (e.g. a 48-hour deletion protocol that the holder can choose to extend or shut off), category-based preservation or deletion controls, two-factor protection, second-layer password requirements, and blocking or restriction functionality.

Language Recommendation:

(1) A Digital Driver's License or other Digital ID adopted in [State or political subdivision] 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 or political subdivision] 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.

(4) By default, requests shall be deleted from the log after 48 hours. Wallets in [State or political subdivision] shall provide controls for the Holder to change or eliminate this deletion policy.

(5) Wallets in [State or political subdivision] shall, to the extent possible without violating any other statute or rule, provide Holders with the capacity to restrict, hide or prevent future requests from Verifiers and to report particular Verifiers.

7. Reporting requirements

When the legislature requires the inclusion of privacy preserving technology and other protections in a Digital ID system, how are the government, legislature, regulators 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 similarly publish a proposed technical architecture for such a system and seek feedback from experts and the public before implementing it.

The mechanism for issuing, provisioning, and presenting digital IDs is a fundamental public infrastructure. The choice of mechanism involves both technical details and important questions of privacy, accessibility, and other tradeoffs—questions that 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 rely on the technical expertise of open standard-setting bodies and topic experts.

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, in [State or political subdivision] the entity or individual responsible for creating or changing that system shall transmit to the legislature and make public a report on the

proposed privacy and accessibility characteristics of, and changes to, 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.

(c) In the case of a substantive change, an accurate quantitative evaluation of relevant privacy metrics and figures including;

(i) The number of IDs in the system

(ii) The number of individuals whose IDs are in the system

(iii) Information on any privacy incidents or breaches from the previous 2 years, including the number of incidents organized by type and severity, entity, region, number of impacted IDs, percentage of incidents where root cause has been identified and corrective action taken, number and percentage of incidents notified to Holders, number and percentage of incidents reported within 12 hours, number of IDs revoked, removed, or destroyed, the number of new IDs created, and any other up-to-date and relevant privacy metric the entity, [regulator], or [legislature] deems necessary.

(2) The entity 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.

(3) [Insert reference to State's existing governing law for advisory committees.] The entity shall assemble an advisory committee of privacy experts or advocates, data security experts or advocates, and other relevant independent experts or advocates. The membership of this advisory committee shall be made available to the public. Members of the advisory committee shall be allowed to anonymously disclose meaningful privacy concerns to the Legislature or the [State] Attorney General and may not be removed from their position, exposed for their disclosure, or otherwise retaliated against for this disclosure by any government or other entity.

8. No remote "kill switch" allowing the government 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 or commonplace for online and in-person access to healthcare, food, utilities, education, information, and services, governments (and potentially hackers or foreign adversaries) gain the power to revoke a person's ability to participate in those transactions, with little or no due process.

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," (the dangerous tracking capability discussed above in section two).

This new capability for data collection and tracking is unnecessary and dangerous. 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 to do when presented with a physical one. Other elements of a license, such as date of birth, cannot change over time and do not expire. And while other elements such as address might change over time, their need to be continuously updated is not vital and should be up to the Holder to initiate, either electronically or in-person at a DMV 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 required periodic renewal.

Language Recommendation:

A Digital Driver's License or other Digital ID system in [State or political subdivision] may not permit the Issuer to initiate contact with the Wallet for any purpose including revocation or update. It may allow, but not require, 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 version of a driver's license or non-driver 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 changeable, 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 – and that the government provide easily accessible means of obtaining them. 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 as a physical wine store could.

The digitization of IDs can make it easier for a person to provide ID in some circumstances—but that means it can also make it easier for stores and websites to *ask* a person to provide ID (something they will be economically incentivized to do given the dollar value of real-time location data and other personal information). 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 intensify the negative 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 to specific circumstances, such as the purchase of age-restricted items.

Language Recommendation:

(9) An entity operating in [State or political subdivision] may not:

(1) Condition the offer, quality, or use of a good or service on the Presentation of a digital or physical driver's license or other government ID, except in the case of:

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

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

(iii) Medical services where the purpose is to ensure that goods, services, or personally identifiable 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 entry, or exit for; any individual or entity who does or does not exercise the rights under this subtitle, or who presents a physical ID, except as reasonably necessary for conducting a transaction online or through other remote means, taking into consideration available technology, and if they should do so, must prepare reports twice annually, and maintain these reports for inspection by [regulator, or an individual bringing an enforcement action], on each implementation, containing:

(i) The purpose of the Verification in this context;

(ii) The specific differences in good, service, treatment, quality, access, entry, and/or exit.

(ii) A specific justification for the exception.

(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 attribute authorization for age or other qualifications.

(10) An agency of [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. Duty of loyalty

A duty of loyalty obligates government agencies, private actors, and anyone else collecting or processing digital ID data to act in the best interests of people whose data is exposed. This duty has been supported by a number of prominent legal scholars as one of the best ways to protect individual privacy. It comes from the ancient concept of "fiduciary duty," which has been part of American and common law for centuries, and requires doctors, lawyers, guardians, managers of trusts, and certain others to act in the best interests of their client—including in how such parties share information. Applying that concept to the key players in a digital ID ecosystem has significant advantages for policymakers. It is broad enough that it can't be evaded or gamed by bad actors and is adaptable and resilient in the face of technological change—provided, of course, there are sufficiently strong enforcement provisions (see section 12). A duty of loyalty has been enacted into law in Utah and is under consideration in other states.

Language Recommendation:

(1) Duty of loyalty.
The Issuer, digital Wallet providers, and Verifiers, [and other participants in the digital ID ecosystem, such as a relying party or digital guardian], shall refrain from practices or activities related to the processing of an individual's identity attributes from a digital identity that:

(a) Conflict with the best interests of an individual;

(b) Take advantage of or otherwise exploit an individual.

(c) Result in a disproportionate risk to an individual.

(d) Are to an individual's detriment; or

(e) Cause harm to an individual.

12. Restrictions on data use and access

Where demands for identity or other information are permitted, a digital driver's license increases the danger that issuers, verifiers, and wallet providers will 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 downstream privacy invasions that digital IDs enable. It is also important that wallet providers not be allowed to monitor the activities of those who hold state driver's licenses or digital IDs.

Language Recommendation:

(1) Neither Verifiers or Issuers, nor their agents, employees, affiliates, consultants, representatives, or contractors in [State or political subdivision] may collect, retain, share, donate, license, provide access to, expose, or use information from a state-issued identity document for longer than or beyond what is strictly necessary for the purpose for which that information was presented.

(2) *No provider of digital Wallets or of verification tools, nor any agent, employee, affiliate, consultant, representative, or contractor, operating in [State or political subdivision] shall access, preview, collect, retain, share, donate, license, provide access to, expose, or use data about the Holder's ID or its use, except as required by state or federal law.*

13. Enforcement

Consistent and strong enforcement of civil laws generally requires a private right of action in addition to enforcement by state regulators. Digital ID systems will affect so many individuals, and engage with so much data, that it will not be possible to enforce good practices without the ability of individuals to bring independent legal enforcement action.

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) 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.

(3) Any non-governmental entity who violates any provision of this Act in [State or political subdivision] shall share, through an accessible and sufficiently visible place and method, a disclosure of any violation and any action against the entity including a title, full text or working link to full text of a settlement or order, plain language explanation of all violations, and publicly disclosable settlement terms in any application, website, marketing materials, terms of use, or other user or consumer agreement. Any violating entity must also share within a time period determined by [the regulating organization / Attorney General], through an accessible and sufficiently visible place and method, this disclosure in a time, place, and manner such that a potential Holder can choose not to use a service provided by the entity, if otherwise possible, in any application, website, marketing materials, terms of use, or other user or consumer agreement.

(4) Any non-governmental entity who violates any provision of this act in [State or political subdivision] will be subject to monitoring and shall submit monthly summaries to [the regulating organization / Attorney General] for at least a period of 24 months detailing compliance with any previously violated statutes including:
(a) Randomized, anonymized sampling of the entity's activity logs, if applicable, that does not include any unique identifiers
(b) Relevant source code
(c) Change logs for relevant source code
(d) Progress updates on changes being made for compliance with settlement terms or previously violated statutes

(5) *Any non-governmental entity who violates any provision of this act in [State or political subdivision] will publish monthly summaries that shall be available to the public with an accessible and visible place and method for at least a period of 24 months detailing compliance with any previously violated statutes including:*
(a) A plain language explanation of all violations.
(b) *Progress updates on changes being made for compliance with settlement terms or previously violated statutes.*

14. Liability and reporting requirements for breaches and leaks

Establishing a digital ID system considerably increases the risk of breaches and the harm such breaches could cause. While physical IDs can be stolen individually, the data consolidation and

pipeline standardization caused by digital ID adoption mean that the long-running trend of government and private databases being breached and leaked may inevitably expose tens of millions of government IDs and allow bad actors to efficiently weaponize this information. While every state has security breach notification requirements that would apply to digital IDs, digital ID exposure would cause harm that exceeds most other possible breaches in breadth and impact. Additionally, those affected by a breach often face substantial hurdles in receiving any meaningful compensation for the harm they encounter. States should therefore implement fair liability standards, strong reporting requirements, and private rights of action specific to digital ID systems. In addition, it may be helpful for the state Attorney General or regulating organization to provide guidance to agencies and businesses engaging with digital ID services who are unfamiliar with their breach compliance responsibilities.

Language Recommendation:

(1) Any person who is injured by improper, illegitimate, unlawful, or nonconsensual access to their digital ID data or information, or nonencrypted and nonredacted information that would permit access to their digital ID data or information may bring a civil action against the entity who owned, licensed, maintained, possessed, controlled, or shared the data or information, and violated the duty to implement and maintain reasonably security procedures and practices appropriate to the nature of the information. A prevailing plaintiff may recover for each violation, against an entity that violates a provision of this Section:

(a) Liquidated damages of $2,500 or actual damages, whichever is greater;

(b) Reasonable attorneys' fees and costs; and

(c) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth. Other relief, including an injunction or declaration, as the court may deem appropriate.

(2) [In addition to compliance with existing notice requirements,] any [term or definition the state uses for a breach violator] must also share, through a clear, conspicuous, accessible, plain-language, and comprehensible method, without the use of any obfuscatory, manipulative, deceptive, or steering patterns, a disclosure of following information, in a time, place, and manner such that a Holder or potential Holder can choose not to use a service provided by the entity if otherwise possible in any application, website, marketing materials, terms of use, or other user or consumer agreement, as soon as practicable and without unreasonable delay following awareness of a breach.

(a) [Any content that may have been specified in the subdivision's existing breach notification law]

(b) The breach date or range;
(c) A description of compromised information and potential harms that can come of this breach;
(d) A summary of the Holder's rights following this breach;
(e) Contact information for the entity and [the regulating organization / Attorney General.]

(3) [In addition to compliance with existing law about notification of the regulating organization / Attorney General,] any non-governmental [term or definition the state uses for a breach violator] shall submit summaries to [the regulating organization / Attorney General] for at least a period of 24 months detailing improvements to identified failure points, identified vulnerabilities, compliance with settlement terms, and compliance with previously violated statutes, on a cadence determined by [the regulating organization / Attorney General], beginning as soon as practicable and without unreasonable delay, such as:
(a) Randomized, anonymized sampling of the entity's activity logs, if applicable, that does not include any unique identifiers;
(b) Relevant source code;
(c) Change logs for relevant source code;
(d) Progress updates on changes being made for compliance with settlement terms, previously violated statutes, identified failure points, or identified vulnerabilities.

(4) Any non-governmental entity who allows or enables improper, illegitimate, unlawful, or nonconsensual access, or other breach or leak, of digital ID data will publish periodical summaries, on a cadence determined by [the regulating organization / Attorney General], that shall be available to the public with an accessible and visible place and method for at least a period of 24 months detailing compliance with settlement terms, and compliance with previously violated statutes including:
a. A plain language explanation of all violations;
b. Progress updates on changes being made for compliance with settlement terms, previously violated statutes, identified failure points, or identified vulnerabilities.

--
For questions or input, please contact Jay Stanley (jstanley [at] aclu [dot] org) or Varun Gadh (vgadh [at] aclu [dot] org).