Identity Crisis

ACLU

Contents

I. Introduction

State legislatures, motor vehicle departments, and companies that sell identity systems are gearing up to o er a new technology to the American people: digital driver's licenses stored in smartphones and used in place of the plastic identity cards that most Americans now carry.

Digital driver's licenses (often called "mobile driver's licenses" or mDLs) are often promoted as a straightforward digitization of our driver's licenses as they are currently used. And if mDLs are broadly adopted, they are likely to start that way.

expanded by proponents of a national identity system who understand that calling it such would never y politically.

It is in this context that digitization of identity would arrive. Digital driver's licenses may bring certain advantages for individuals, but they will also give institutions a major new tool by which individuals can be tied to the full documentary DMV identi cation and proo ng process required

But with the right kind of digital ID, you could attest to a Veri er that you are over 21 without sharing your date of birth or any other information. You could share your state but not your city, your city but not your ZIP code, your ZIP code but not your address, and so on.

Another advantage touted by mDL boosters is convenience. There's no guarantee people will nd mDLs more convenient given the ease of a physical card compared to ddling with a phone. Alabama, for example, has had a digital driver's license available to residents since 2015, but it remains rarely used even as mobile payments have skyrocketed. Nevertheless, it's certainly true that people are storing ever more information on their phones and it's possible that mDLs could prove popular if the option is more widely

THE C RRENT STATE OF PLA

The impetus for digital driver's licenses is coming from a variety of powerful institutions. The concept is being sold hard by an "identity-industrial complex" of corporate players, including the French companies Thales and Idemia and the Louisiana-based company Envoc.

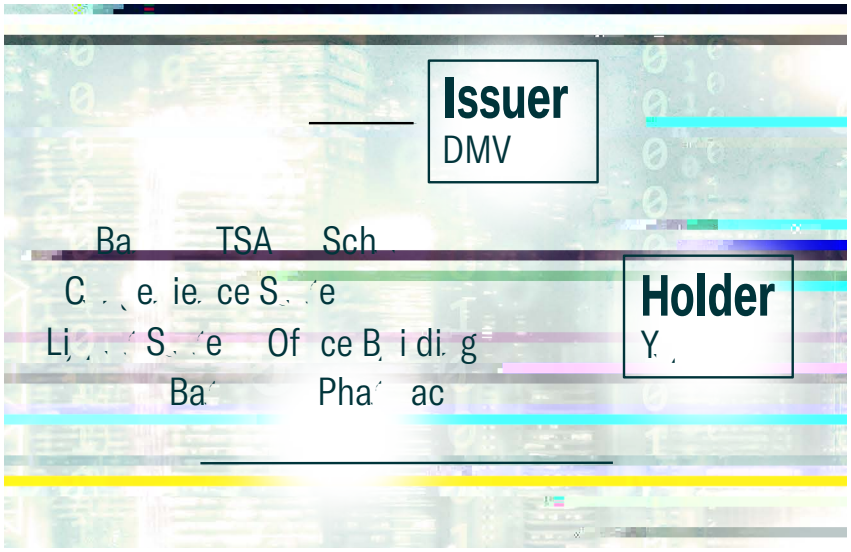
A number of state legislatures and DMVs have also begun moving toward mDLs. Louisiana, for example, enacted a law in 2016 that fully legalized digitized driver's licenses for tra c stops and has made a mobile ID app available to the public. The state's alcohol and tobacco and voter registration agencies have both begun accepting the app, which was jointly designed by the Louisiana State Police, Department of Public Safety and the O ce of Motor Vehicles and built by Envoc. According to the American Association of Motor Vehicles Administrators (AAMVA), Colorado, Delaware, and Oklahoma also have some form of digital driver's license, though, like Louisiana's, they are not yet compliant with a common standard and will need to be updated when such a standard is nalized. The states closest to issuing standards-compliant mDLs, according to AAMVA, are Iowa and Florida, which have announced contracts or plans with companies to create such a system. Other states have enacted enabling legislation, including Arizona, Arkansas, Illinois, Indiana, Maryland, Michigan, Tennessee, Utah, Virginia, and Wyoming. And a number of states—including Idaho, Maryland, Virginia, Utah, and Washington, D.C.—have worked with companies on mDL pilot programs.

The push for mDLs is also coming from the federal government. The National Institute of Standards and Technology (NIST) has, since the Obama administration, been working to create an online identity system, and nanced several of the state mDL pilots. The TSA is working on integrating mDL functionality into its airport security checkpoints. And in December 2020, Congress passed legislation modifying the Real ID Act to allow mDLs to qualify as compliant and giving DHS the power to regulate what that looks like. That means our nation's largest security agency can dictate the implementation of any mDL that is to be recognized by the federal government, which, realistically, means it has the power to shape the national standard—a power that DHS is already gearing up to exercise.

The movement toward mDLs has not yet gained wide traction within the states, however. A big reason is that such IDs must be interoperable—that is, recognized around the United States and abroad, as physical licenses are. That requires the creation of standards. Standards-making e orts for mDLs have been underway at both the national and international level and are nearing completion. Internationally, the International Organization for Standardization (ISO) is creating

II. Potential Threats to Privacy

The overarching privacy question is whether digital driver's licenses are being built to form a solid


Issuer
DMV
Holder
Y

Many of the interests pushing mDLs appear to see the linkable presentation problem as an issue of policy rather than technology. A recent white paper by the industry group Secure Technology Alliance (STA), for example, merely urges that Veri ers "do not report Holders' personally identifying information to any centralized service that compiles usage data, regardless of whether the data is obtained from o ine or online mDL interactions."

Digital IDs should not be built around an online system that gives an Issuer visibility into where and when a Holder is using their ID. But an mDL model statute created by AAMVA (and partly adopted by at least one state) requires construction of a "veri cation system" based on the online mode. The statute explicitly contemplates situations where a government agency "requires that an electronic credential or pro le be veri ed through the veri cation system." There is no requirement that that veri cation system be unlinkable. (AAMVA tells us that it is rethinking this model and "will be working on an update.")

DHS, meanwhile, said in an April 2021 document that it sees "data freshness"—minimizing the time that has passed since the data in an mDL was last veri ed—as a security bene t. Other security agencies and interests no doubt agree, and that will be an incentive to create mDLs that are based on an online model where constant connection guarantees such freshness.

Another incentive for DMVs (or the private companies that work for them) to build an online model for veri cation is to enable the collection of fees. DMVs have expressed reluctance to cover the costs of an mDL system that would mainly bene t businesses and other government agencies that verify ID. So, they are looking at revenue options. Among the possible models is a system in which Veri ers pay a fee to verify the IDs that they check—a model that would most likely require tracking of mDL presentations. In its model legislation, AAMVA suggests state legislatures authorize such fees.

In its mDL implementation guidelines for state DMVs, AAMVA points out that the online option allows tracking and encourages Issuers to carefully weigh its use against the privacy implications. Still, DMVs are free to adopt an online structure that allows them to track presentations while still being compliant with the ISO standard—and the possibility of charging fees will provide an incentive to exercise that option.

Policy protections are vital but may change or weaken over time. They need to be enacted on top of technological protections for privacy in any widely adopted digital identity system.

The architects of the emerging mDL system are largely representatives of government agencies and big companies, and they have focused on using the most advanced cryptographic techniques to advance the government's interest in preventing people from faking their IDs and to protect people from malicious hackers. But they have not so far made it a priority to protect people's

privacy against the kind of tracking by Issuers (or their contractors) that a switch to digital IDs would make possible.

. IDS THAT ` PHONE HOME

Even without a digital identity system designed so that Veri ers report back to Issuers every time an ID is presented, digital IDs may "phone home" to their Issuers for other purposes. The primary such purpose is revocation: the ability to remotely reach into a Holder's phone and revoke or update a license.[4] That's something that obviously can't be done with plastic licenses, and it's a big selling point for mDL boosters. But designing an mDL that regularly connects to the issuing DMV (outside of speci f c appointments initiated by the Holder) creates all kinds of privacy problems and shouldn't be done. It allows the Issuer to see your IP address, for example, from which it can infer your location—both potentially sensitive pieces of information. It also increases the opportunity for abuse.

And it's not necessary to create these privacy problems. First, it's not clear how instant remote revocation of a license would reduce the incidence of unlicensed driving, compared to simply notifying someone that their ID has been revoked. Either way, some people will drive even though they're not supposed to, and if (and only if) they are pulled over by a police o cer, they will be caught. Second, revocation of a digital license doesn't accomplish anything if the Holder also has a plastic license, because when their mDL is revoked, they can just present their physical card. In the case of police stops, o cers can check for license revocation when presented with a physical card just as easily as when presented with an mDL. And when it comes to non-driving contexts, there's no reason to render an mDL inoperative as a means of identi cation or age-proo ng just because

> Architects of the emerging mDL system are largely representatives of government agencies and big companies.

1

someone is no longer quali ed to drive. In fact, giving the government the power to instantly and remotely remove people's ability to identify themselves or verify anything about themselves is a recipe for abuse.[5] (As an ACLU investigation has shown, driver's license revocations are already used abusively around the country.)

The ability to do remote revocation is unnecessary and not worth the privacy tradeo s. And it is only relevant if our driver's licenses become digital-only—but, as we explain below, that shouldn't happen.

4. ERIFIER ID TRACKING

Another threat to privacy comes not from the Issuer (DMV) but from Veri ers. Even if data doesn't ow to the Issuer each time a person presents their ID, Veri ers could record and compile information about those presentations. For example, a consortium of bar owners could keep an electronic record every time you present your ID. They may not see when you present your driver's license to others, but they could know every time you show it to one of them (or to their corporate a liates or anyone else they make a data-sharing deal with) and gain a rich trove of data about a Holder's life. The digitization of IDs could make this much easier and more automatic than it is today.

The threat of Veri er linking of presentations can be addressed through the same cryptographic architectures for unlinkable identities that can protect Holders against tracking by Issuers. However, under current standards, the Veri er will receive a copy of the Holder's license photo in order to verify that the mDL actually belongs to the Holder. And those photos can be stored by the Veri er and used to link presentations—or for automated face recognition. That's a distinct privacy disadvantage of mDLs over physical licenses, where the Veri er looks at your photo but doesn't get a digital copy of it. The only solution to this problem under the photo-based system would be to ban the collection of photos in that way and/or to regulate the equipment used by Veri ers to prevent it fromeal w(sn (ll)(eal(rev)9(e)-4 (s th)-6(f p)8 (h)16 (o)10.9 (-18 (os can)((o)20 (w(-18 1 (11

the holder's security mechanism could be hacked–or abused, for example, by undercover police who have in ltrated the meeting of a political group they don't like. And it would only be useful with regard to incapacitated people if mDLs become a replacement for rather than an optional secondary copy of people's physical IDs.[6]

Finally, another part of having control over the data in one's mDL would be knowing exactly what is shared and when. That means that mDL apps should have thorough auditing functionality built in so that users can look at exactly what data leaves their phone. This is something that mDL architects appear to be building into the current system.

. S SCEPTIBILIT TO HACKERS

Security in the digital age is hard. The fact is, as security experts point out, that attacking digital systems is simply easier than defending them. We see this in the way that even the largest, most sophisticated and deep-pocketed companies and government agencies fall prey to malicious hackers. The essential insecurity of the digital world should not automatically be a reason not to make something digital, of course–and plastic licenses have their own vulnerabilities–but the

present themselves as you—not only in person, but potentially in the future, online. And the more everyone assumes that mDLs are secure, the more trust they will put in the imposter and the more damage that imposter could do to you.

Google and Apple are both working on modifying their phone operating systems to make identity apps like mDLs more secure and privacy protective. In some cases, they rely on secure cryptographic hardware that is built into some phones—but it's never certain how secure such complex systems are until they are released into the wild. In addition, not all phones have such hardware, and that leaves mDL apps vulnerable to known, un xable vulnerabilities in phone hardware, as well as whatever vulnerabilities exist in hardware and operating systems.[7]

what they are supposed to do and b) are as secure as the authorities claim they are. The problem is that many or all of the private companies that make the apps (such as Idemia, Thales, and Envoc) are likely to want to keep their code proprietary. That would mean that ID holders are running what is essentially secret government code on their phones and reduced to merely trusting in its operation and security. That is not acceptable—and even less so if people are legally or practically required to use mDLs.

It's important that the source code of these apps be transparent.

Second, open standards should be created for the "provisioning process"—the procedure by which DMVs (or other Issuers) load a Holder's mDL onto their device. An open standard for that process could allow anybody to create an mDL app that would interface with a DMV simply by complying with those standards. This would allow a variety of developers—including public-minded/nonpro t developers—to create competing mDL apps, giving consumers a choice in which app to use. If some states fail to require that all mDL apps reveal their source code, open

III. Potential Harmful Consequences of Digital Driver's Licenses

It's important that any digital ID system squarely address the seven immediate privacy threats discussed above. Only then will an mDL be built on a solid foundation that would allow Americans to feel comfortable using the technology.

Solving those privacy problems is necessary but not su cient. There are potential longer-term consequences and evolutionary paths that digital identities might take that would hurt privacy and other civil liberties interests in signi cant ways.

. E PANSION OF SAGE

It is not too early to start worrying about mission creep. Currently, mDLs are being framed narrowly as replacements for physical ID cards, to be deployed in tra c stops, alcohol purchases, TSA checkpoints, and the like. But, once entrenched in that role, mDLs are likely to expand into a far broader role in proving identity than driver's licenses play today.

Indeed, many of those involved in the development of mDLs envision just such an expansion. The global ISO working group is planning a second phase of standards-writing to enable the presentation of mDLs over the Internet; Google and Apple's operating system work in this area is also largely focused on building the capacity for online presentations. AAMVA declares that "new use cases brought about by the nature of an mDL can be expected. Online use is one example."

Much of the pressure for an ID that is usable over the internet, seems to be coming not from DMVs and AAMVA, however, but from corporate interests. As one anonymous participant in an AAMVA webinar put it, "The overwhelming interest among big relying parties is not [in live human ID presentations] but one where people can use their mDLs to support remote ID proo ng." AAMVA appears happy to accommodate that; as one executive with the association put it in the webinar, "We understand there's a thirst for trust and identity and proo ng when the people are not in the same room, and that the natural interest is going to take us down that path."

There is a real danger that

give ID information, the more palatable it is to ask for, or demand it." We have already seen this dynamic with the appearance of magnetic stripes and bar codes on our licenses; fully digital IDs will only accelerate that trend.[9]

Digital ID checks could be increasingly demanded not just by humans, but also by machines. This would likely supercharge Templeton's paradox, because automated "robot ID checks" will be cheaper, less time-consuming, and more scalable for verifiers. Why not ask people for their IDs left and right when you can just buy some cheap machine, sit back, and let the data pour in? Imagine, for example, a website that today requires you to turn on your webcam and take a photo of your driver's license for human verification to make an account. If you can instead just press a button that says "Send mDL," you are going to be asked to prove your identity a lot more often just because it's so easy.

These kinds of dynamics could lead us toward a "checkpoint society" where an increasingly dense net of identity check6 (o)17 (ing)-0ry

DMVs "are uniquely positioned to enroll citizens in an identi cation system," and that "other entities within jurisdictional governments have started to recognize this, and there are initiatives to leverage this setup by adding other privileges (e.g., hunting licenses or social entitlements) as attributes to the identity established by the issuing authority. It is envisioned that a mDL would be an ideal vehicle to support this."

A mobile driver's license would likely be seen as an "ideal vehicle" for far more. "The really powerful thing is that once we bind you to that credential and verify it," gushed Iowa's transportation director, Mark Lowe, "you can use it for hunting and shing licenses, weapons' permits, tax returns—all sorts of things." Some have already pushed to use the mDL standard for "vaccine passports." And many other ideas would no doubt ow; think of the information that could be valuable to various Veri ers:

- Complete vaccination records
- Pre-existing health conditions a paramedic should know about
- Other health data
- Dietary preferences
- Licenses and permits of all kinds
- Outstanding parking nes and other fees
- Sex o ender status
- Passage of—or failure to pass—a government background check for whitelist/blacklist programs like the TSA's PreCheck
- Status in various rewards programs
- Credit score

Some of this information might be useful for some people to have in a cryptographically secure, user-controlled, privacy-protected digital form. But the prospect that mDLs will become a vessel for so much sensitive information is another reason why any digital identity system we create must have an unimpeachable privacy foundation.

Of course, technology only gets us so far when it comes to protecting privacy. E(ab)m7y[on is ayn1D9 (e)1k Tm(m)i1-4 (s)-5 ( )]TJigt0.1 (y g)6 (Std32m)-18.9 (ec)w 1

discussion, use a Wi-Fi network, or purchase a product. Wherever companies or other parties have real-world power over people, those parties will be able to pressure people to give "voluntary permission" to share. And there's no guarantee that those demands for ID data will be limited to what is necessary, unless our country passes stronger legal privacy protections. Good technological privacy protections are vital, but they're not enough.

. MANDATOR DIGITAL ID

Another possible consequence of the introduction of mDLs is that they will gradually become mandatory. Currently, mDL boosters are saying that digital licenses will augment rather than replace physical IDs. "For the near future, it is envisioned that an mDL will be issued in addition to, and not in lieu of, the plastic license," as AAMVA puts it. "It is anticipated that, *f . . e. e be* , an mDL will be an option."[10] But, as the association also notes, there is a "generally held position by subject matter experts that we will in the not-too-distant future see physical credentials start to disappear and experience an ever-increasing electronic landscape when it comes to credentials."

Indeed, as we have seen, much of the architecture being built for mDLs (such as revocation) appears to be implicitly premised on them eventually replacing physical driver's licenses. And the fact that physical licenses can't be remotely revoked or updated and are easier to forge could cause mDLs to be viewed as more reliable by some Veri ers and cause those Veri ers to pressure people to use mDLs. In its mDL model legislation, AAMVA recommends that state legislatures declare that "In the case of a discrepancy between the physical and electronic credential, the electronic credential takes priority and is considered the more current information."

Another incentive for Veri ers to force people to use electronic licenses is that they want to use machines to quickly and automatically check people's credentials so they don't have to pay humans to do it.[11]

10

11

While use of mDLs might theoretically be "optional," in other words, it might become harder and harder to get by with just a physical ID. The United States has no constitutional authority to compel people to carry a phone, much less to install a speci c app on their phone, but that doesn't mean it won't become a practical requirement. Nowhere is it written that a person has to own a credit card—yet it's di cult to fully participate in modern life without one, and those who lack them su er signi cant disadvantages in establishing credit, renting a car, buying things online, or even, increasingly, buying food. It may become much the same with mDLs: First a few merchants or others start rewarding people for using mDLs. Then they start refusing to recognize plastic IDs outright. More and more follow, and eventually they become legally mandated.

Given the strong corporate interest, it could be the online uses of mDLs that lead this trend. It would not be surprising if, once mDLs that meet a national standard begin being issued, online ID demands proliferate practically overnight.

If mDLs become practically or legally mandatory, that would have several bad e ects:

a. F e Ma i ai i a i f Pe le W i S a es

First, a lot of people don't have smartphones, 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. People with disabilities are 20 percent less likely to own a smartphone, and many who are homeless also lack access. Some 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.

A ordable Internet connectivity may also pose a challenge to using an mDL app if it requires online checks. Pew estimates that 24 million Americans—including 30 percent of rural Americans—lack access to xed broadband service. Many lower-income smartphone users have limited data plans. Even for those who have access to a smartphone and a ordable broadband, technical ability and lack of support may pose a challenge. (This is another reason why mDLs should be designed to work only o ine.)

Broadband service will hopefully improve over time, and the penetration of smartphones is sure to rise. But much of the discourse around mDLs assumes a future with e a smartphone ownership. While smartphones bring many conveniences, it would be unwise to allow ourselves to become too dependent upon them.[12]

---

1 [illegible]

A legal requirement for mDLs would therefore be deeply problematic, and even a purely practical requirement for the IDs would further disadvantage marginalized communities.

b. Ha f ıP ecede f F ced A I s aıa ¸

Smartphones are personal computers. They belong to, should remain under the control of, and should act on behalf of their owners. Mandatory digital IDs would amount to a government demand that citizens install a particular piece of software on their personal phones—software that, as we have seen, may very well be opaque to those who are forced to install it.

That sets a terrible precedent. We don't want to see people's smartphones ll up with apps that serve the purpose not of empowering people, but of controlling them. We don't want our phones to turn into the functional equivalent of ankle bracelets. Giving consumers the option to install a duplicate, digital version of their driver's license for their own convenience is one thing; forcing them to install software that serves as an instant, remote, and revocable government lever over citizens is quite another.

We've already seen signs of this trend elsewhere. Some colleges and universities require their students and faculties to install tracking apps on their phones as part of the e ort to stem the spread of COVID-19. And the companies that make actual ankle bracelets are shifting to cell phones, imposing nightmarishly onerous requirements on parolees and others through tracking apps theyaoidquiremo ceall a du7 (n paro)12 (l(o)17 (n)12 (e)-4 (s t)-17.9 (o)8g[(o)

behind the wheel has been suspended. Digital license plates might change to show the ID of the person who is driving at any given time—helping the authorities identify drivers but eroding privacy. People convicted of driving under the in uence could be prohibited from using their IDs to buy alcohol.

There are endless such possibilities, most of which haven't been thought of yet, but these examples give us a glimpse of how far-reaching the implications of this technology could be.

c. Ne P ss'b'i'ies f Ab se

Digital enforcement also increases the potential scale and consequences of abuse. Imagine a ruthless governor or an abusive o cial like J. Edgar Hoover bent on destroying Black Lives Matter activists or other political opponents or activists challenging the status quo. What could someone like that do with badly designed mDLs that they couldn't do with plastic licenses? They could abusively revoke or alter the licenses of activists—individually or even en masse—rendering their IDs invalid with the ip of a switch. They could monitor deployments of licenses by people on watch lists (a group that in recent years has included nuns, anti-fracking activists, and peace activists), setting alarms when certain people present their IDs in certain locations or for certain purposes.

Due process rights might become harder in the context of digital enforcement as well. When you're standing at the DMV as part of a periodic scheduled application or update for a license and run into a problem, you can challenge, argue, and explain whatever bureaucratic quirks or anomalies—or abuses—might arise. But if your driver's license just gets deleted remotely, you may have no such opportunity, and the burden could fall on you to ght your way into the bureaucracy to get an explanation for the problem and then solve it.

d. Fa'i es f Tec

Smartphones fail. They are dropped, get run over by trucks, su er water damage, experience software corruption, get infected with malware, and, of course, lose battery power. Sometimes, they stop working properly—or die entirely—for no apparent reason. Within an mDL system, a Veri er's reader might not be able to connect to the Holder's device or authenticate the mDL after it does. Neither party may have the foggiest idea why the veri cation isn't working, and whether the problem lies with the Holder's phone or the Veri er's reader.

And it's not just smartphones that fail; so do entire computer systems. The world saw this in 2019, when the network of one of the nation's largest retailers, Target, went down, leaving customers with no way to buy anything in any of its stores except by cash. Entries in

databases—like your DMV records—also can get corrupted, hacked, or simply deleted. Like cash and the paper ballot, plastic IDs may seem primitive compared to a bright and shiny future world of digital-only transactions, but they are an important and robust safeguard against centralized failure.

In a context where mDLs are an optional accessory to mandatory physical licenses, AAMVA contemplates putting the onus for such failures in contexts such as tra c stops squarely in the hands of the ID Holder; where an mDL can't be read, "the mDL holder is treated as if it did not present a driver's license." Putting the onus on Holders could be justi ed if mDLs are viewed as an optional supplement for plastic licenses: If your phone fails while driving, you had better have your plastic license with you just as you do now, or that's on you. But if plastic licenses disappear, how would technology failures be handled? It can't be the case that if your device dies—or the police o cer's does—you go to jail.

In Britain, a whole political movement is demanding the right to physical rather than digital

IV. Questions About Process and Transparency in the Creation of mDLs

If our society is to embrace a digital identity architecture, we should do so in an educated, clear-eyed, open, and democratic fashion, not merely as the result of decisions by small handful of bureaucratic and corporate players.

Crucial decisions about our new potential identity infrastructure, for example, are being made by a working group within the ISO whose American members seem to consist primarily of representatives of corporations, AAMVA, and government agencies such as the Department of Homeland Security. The ISO is a private entity and hardly exhibits the transparency that an organization whose activities have such important public implications ought to have. The working group's membership list is not published, for example, and the ISO refused to share it with us. It's practically impossible for any interested party to join this secret committee; their deliberations are not open to the public; and their drafts and other work products are treated like classi ed documents. The draft ISO standard for mobile driver's licenses we were able to nd was not formally posted or shared by the ISO, and we have no idea how current it is. When published, their standards, including those governing mDLs that will guide the construction of every state digital driver's license in America, aren't accessible except by paying thousands of dollars for the copyrighted document. That might be acceptable for something like industrial machinery, but certainly not for standards with implications that go to the heart of the relationship between citizens and their government. There are also representatives of authoritarian countries in the ISO who would like to surveil ID holders instead of protect their privacy.

All this is in stark contrast to W3C, the developer of the "Veri able Credentials" standards, where the work is done through an open public process, participation is far more open, and meeting notes, recordings, and materials are accessible to all.

As driver's licenses have gained an increasingly signi cant role in American society, motor vehicle administrators are being thrust into a role far broader than their traditional one of administering the nuts and bolts of motor vehicle regulations. AAMVA is increasingly playing the role of a federal government agency, making decisions that will a ect American life nationally—yet, like the ISO, it is a private entity, not subject to the checks and balances that apply to government agencies. The Freedom of Information Act, for example, doesn't apply to AAMVA. The organization's sta were commendably helpful and open with us as we prepared this report, but as a legal matter, AAMVA is free from the transparency obligations that apply to civilian government agencies. Many of its key documents are not available to the public, and it claims copyright in the materials that it produces. In the past, it has removed controversial documents from its site and sent copyright takedown notices to critics who are monitoring its activities. That's not something that a federal agency can do. Nor is AAMVA subject to strictures like the Administrative Procedure Act, which imposes rules for how agencies enact new regulations—such as requiring that they be submitted for public comment, and that those comments be addressed, before the rules are nalized.

Because of the backhanded way IDs have developed in the United States, DMVs and companies are building a governance architecture that will be national in scope yet developed by a process not subject to democratic input and debate. This is not the way to proceed with societal decisions that promise to have enormous and long-term implications.

V. Recommendations

No police officer access to phones

Standards and technologies should be designed so that as a practical matter, Holders never need to relinquish control of their smartphone to any Veri er. When it comes to law enforcement, technology design should be reinforced through policies that prohibit "voluntary" requests—which are never truly voluntary coming from a police o cer—to hand over devices.

Unlinkable presentations

Standards and technologies should be designed so that the Issuer (or any of their agents or contractors) cannot know where or to whom a Holder is presenting their ID, and so that Veri ers cannot conspire with each other or with Issuers to compile records of presentations.

Granular control over data released

Standards and technologies should be designed so that Holders have complete control over what data is released from their IDs, including broad exibility to provide attestations of general categories into which a Holder ts, such as "over age 65" or "a resident of this city."

A standardized provisioning process

The process by which data from DMVs or other Issuers is loaded onto people's devices should be standardized so that anyone can write a compliant mDL app and Holders will have choices in which app they use.

Transparent source code

The code for mDL apps that people install on their phone should be transparent so that members of the public can be assured that it does only what it's supposed to do, and to increase its security.

IDs that don t “phone home

mDLs should not incorporate remote revocation capabilities and should be designed to operate

VI. Conclusion

Until relatively recently, identity checks did not feature as prominently in American life as they do today, and it's important to keep in mind that such checks are not a natural or inevitable part of life. Nor are they necessarily a re ection of the public interest. Many ID presentations, such as those in airports, banks, building lobbies, and elsewhere, though usually unquestioned, amount

fake IDs to buy beer. Nor is it worth doing so to ll some cracks in the administration of our motor vehicle licensing system.

Policymakers should seek objective data on just how important more-secure IDs are in terms of reducing fraud and other serious crimes. They should ask just how much of a di erence mDLs will make if they remain optional, and what the consequences will be if they're made mandatory. They