



Identity Crisis

What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom

ACLU

Contents

I. Introduction.....	3
The Evolving Role of IDs in American Life	4
How Digital ID Systems Work	5
Possible Advantages.....	6
The Current State of Play	8
II. Potential Threats to Privacy.....	10
1. Police Access to People’s Phones.....	10
2. Centralized ID Tracking.....	12
3. IDs That “Phone Home”	15
4. Verifier ID Tracking.....	16
5. Lack of Personal Control Over ID Data	17
6. Susceptibility to Hackers	18
7. Forced App Installation	19
III. Potential Harmful Consequences of Digital Driver’s Licenses.....	21
1. Expansion of Usage.....	21
2. Expansion of Information Contained	23
3. Mandatory Digital IDs.....	25
IV. Questions About Process and Transparency	30
V. Recommendations.....	32
VI. Conclusion.....	34

I. Introduction

State legislatures, motor vehicle departments, and companies that sell identity systems are gearing up to offer 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.

But this technology is likely to have ramifications that quickly extend far beyond a simple replacement of plastic IDs by phones. Identifying people is sometimes necessary, but but it's also an exercise in power. That means that we need to take great care in how we build identity systems—especially when digital technology enters the mix.

By making it more convenient to show ID and thus easier to ask for it, mDLs will inevitably make demands for ID more frequent in American life. They may also lead to the routine use of automated or "robot" ID checks carried out not by humans but by machines. Depending on how a digital ID is designed, it could also allow centralized tracking of all ID checks, and raise other privacy issues. We might even see demands for driver's license checks become widespread online. This would enormously expand the tracking information such ID checks could create and, in the worst case, make it nearly impossible to engage in online activities that aren't tied to our verified, real-world identities. Longer-term, if digital IDs replace physical documents entirely, that could have significant implications for equity and fairness in American life.

A move to digital identity "cards" is not a straightforward translation; important things are lost and gained in the switch. New possibilities open up, some potentially good and some not. A digital system could enhance user privacy and control if done right—but it could also become an infrastructure for invading privacy and increasing the leverage and control of government agencies and companies over individuals. In this paper, we will look at how mDLs are currently shaping up and the issues that they raise for privacy, equality, and other civil liberties.

A move to digital
identity cards is not
a straightforward
translation.

THE EVOLVING ROLE OF IDs IN AMERICAN LIFE

Mobile driver's licenses would arrive at a time when the role of identity and identity checks in American life has already been expanding. Until relatively recently, identity checks did not feature as prominently as they do today. Before an accidental plane [crash](#) in 1999, you didn't need to show an ID to fly, for example, and if you had an airline ticket you couldn't use, you could sell it to someone else. After 9/11, the [highly questionable](#) notion took hold that terrorist attacks could be thwarted by tightening up the standards for issuance of IDs. At the same time, conservative antipathy toward immigrants led many people who were normally skeptical of government mandates and the creeping bureaucratic regimentation of American life to embrace the expansion of identity systems. The post-9/11 effort to make driver's licenses more secure was bungled by the congressional leadership of the time, who rammed through the poorly designed Real ID Act of 2005. That bill, which was passed with no hearings, debate, or testimony from state department of motor vehicles (DMV) officials or other experts and was attached at the last minute to must-pass emergency legislation, imposed a cumbersome and unnecessary system of identity and citizenship proofing on state DMVs.

Digital driver's licenses
will give institutions
a major new tool by
which individuals can be
inescapably tracked.

In the years since, identity checks have increased in more and more places, from [building lobbies](#) to [banks](#), [voting booths](#), [doctor's offices](#), and [employers](#). The TSA began building an enormous, [misguided](#) security infrastructure on the quicksand of identity-based security—trying to protect aviation by gathering information about people and pretending to know who is most likely to launch the next attack—an approach that also opens the door to bias and targeting. And identity checks are on course to further accelerate in the coming years as the Department of Homeland Security (DHS) pushes to fully enforce the ill-

conceived Real ID Act over resistance by the states, and as facial recognition-based [machines](#) for automatically verifying the authenticity of physical ID cards enter the market.

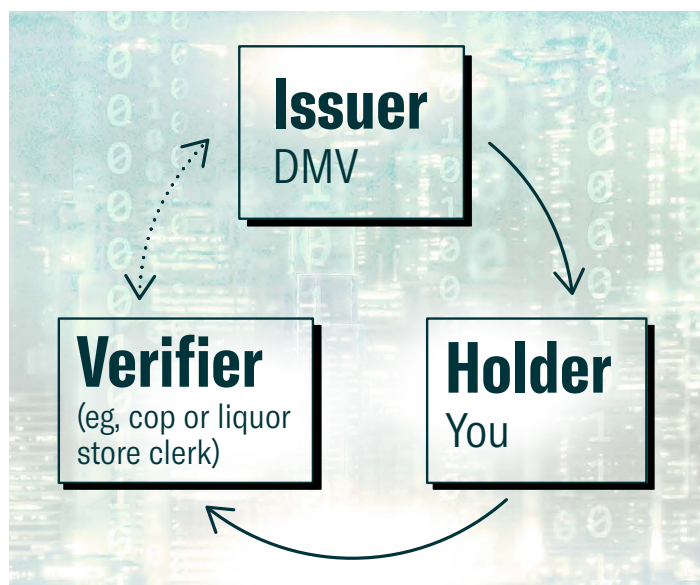
Americans across the political spectrum have long resisted the idea of a national identity card, and Congress would probably never pass any measure labeled as such. But the nation is backing into such a system through state bureaucracies originally set up for a limited purpose: to certify who is competent to drive a car on the public roads. This backdoor ID system has been exploited and

expanded by proponents of a national identity system who understand that calling it such would never fly 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 identification and proofing process required by the post-9/11 Real ID Act—and thus be inescapably tracked.

HOW DIGITAL ID SYSTEMS WORK

To understand some of the potential privacy issues raised by mDLs, it's important to understand the structure of digital identity systems. In their simplest form, they include three parties: an identity Issuer (for mDLs, that would be the state's DMV, but it can be any party wanting to issue a credential, including a bank, library, gym, etc.), an identity Holder (such as you), and an identity Verifier (such as a liquor store clerk or a police officer who has pulled you over on the highway).



Digital credentials like mDLs rely on modern cryptography to produce files that—even though they consist of nothing but ones and zeros stored on your phone—cannot be tampered with by you or anyone else without detection. Such a feature is necessary, or it would be easy for the Holder (or others, including malicious hackers or apps) to open the digital driver's license file on their phone and change anything or everything about it. This system works through what is known as [public key cryptography](#), in which files are signed

and verified with a linked pair of digital codes or “keys”—one that is public and one that's kept private. When an Issuer (such as the DMV) places a digital credential (such as an mDL) on your phone, it digitally signs that file using its *private* digital key, which only it possesses. Then, when a police officer or other Verifier looks at that file, they verify it using a corresponding *public* key distributed by the DMV. That public key can only verify signatures that have been made with the

corresponding private key, so if the signature is valid, the police officer knows with ironclad mathematical certainty that the file was signed with the DMV's private key, and that not a single bit has been changed.

The presentation of an mDL is envisioned as working in one of two ways: offline or online. The offline version would work like this: When you walk up to a cash register to buy alcohol, get pulled over by a police officer, or otherwise need to show ID, the clerk or officer uses an mDL reader app or device to request certain data from your ID. You see the request on your phone and choose whether to approve it. Any data that you agree to release to the Verifier gets sent to them along with your photo, which they use to make sure that you are the actual owner of the mDL that you're presenting. The Verifier's device then checks the digital signature on your mDL against the DMV's public key to make sure that it's a valid digital license that hasn't been tampered with.

Under the online method, your phone would not actually hold your driver's license data. Instead, your phone would send an identifying digital token to the Verifier, who would then send that token over the internet to the DMV. The DMV would confirm its authenticity and then send the Verifier the data that you have given permission to share. As we discuss below, online verification raises significant privacy problems.

POSSIBLE ADVANTAGES

A digital driver's license could bring a number of advantages that should be weighed in considerations of the technology.

One of those advantages is that, if done right, the technology could actually improve the privacy of ID holders in some respects, by giving them the power to decide exactly what information they share with a Verifier—and to share no more than is necessary for a transaction. With a physical driver's license, for example, if you want to prove to a bartender that you're old enough to be served, you have to hand over a card that lets the bartender see your full date of birth as well as all the other information printed on your ID, from your name and address to weight, [gender](#), and organ donor status. Some [bars scan](#) patrons' driver's licenses, collecting and retaining all the data from the IDs' bar codes for marketing or other [purposes](#). In our experience, some retailers, such as Target, abuse this system to collect their customers' full date of birth, refusing to sell them alcohol unless they give not only the year but also the month and day of their birth, no matter how old a customer appears to be.

But with the right kind of digital ID, you could attest to a Verifier 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 find mDLs more convenient given the ease of a physical card compared to fiddling 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 publicized. Allowing people to prove their identity remotely could also open up new conveniences and efficiencies.

If done right, the technology could actually improve the privacy of Holders in some respects.

Digitization would also make stealing, altering, or forging driver's licenses exceedingly difficult if not impossible; it would probably require theft of the cryptographic private keys held by the DMV or other Issuer. For institutions that want to know who you are with a high level of certainty, mDLs provide a significant advantage.

At the same time, while it may be true that a shift toward digital could bring enough convenience or other advantages that it ultimately proves successful, Americans should not leap to embrace that change on an assumption that it will be neutral and harmless. As with some other technologies like voting systems—where digital-only is not just inferior but potentially disastrous, and is being phased out in most places—digital IDs can bring distinct disadvantages over old-school hard copies, and those need to be thought through carefully. In particular, if we are to accept a digital ID system, we need to make sure it remains voluntary and has the strongest possible privacy protections. Although the state of privacy online and off is already pitiful in many ways, there is plenty of room for a poorly constructed digital identity system to make things worse and leave us looking back on today's world with a feeling of loss over the freedom, anonymity, and lack of regimentation we once had.

THE CURRENT STATE OF PLAY

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 traffic 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 Office 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 finalized. 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 [financed](#) 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 efforts 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

DHS can dictate the implementation of any mDL that is to be recognized by the federal government

[a standard for mDLs](#), and within the United States, AAMVA is working to help state DMVs implement mDLs that are compliant with ISO's standard. Meanwhile, Google and Apple, the duopoly that makes the operating systems for nearly all smartphones, are working to make those operating systems function well with an mDL system.

More broadly, aside from these institutional architects of the emerging mDL system, the move toward mDLs stems from a general sense that digital versions of our identity cards are inevitable. That sense has fueled the emergence of an entire identity community that

has been working on the problems of online identity and authorization for many years. That community is animated by a belief that it's not realistic to expect that in 50 years everyone will still be sharing meaningful documents only in face-to-face meetings using pieces of paper. Some within the identity community have embraced centralized, proprietary systems, while another camp is animated by a vision of "self-sovereign identity" that is decentralized, open source, privacy-preserving, and empowering of individuals. That movement has created a number of proposed systems, including an open standard created by the World Wide Web Consortium (W3C) called [Verifiable Credentials](#) (VCs). Like most efforts in this area—including mDLs—the VC concept is still being refined. Unlike mDLs, with their narrow focus on the centralized digitization of one form of identity (driver's licenses), broader concepts like VCs would create a framework that would allow any party—from government agencies to your employer to your local coffee shop—to issue digital credentials.

But as we will see, despite their purportedly narrower focus, mDL proponents are simultaneously thinking big.

II. Potential Threats to Privacy

The overarching privacy question is whether digital driver's licenses are being built to form a solid foundation for the much broader uses to which they may eventually be put. Getting privacy right in the mDL architecture is important for digital driver's licenses themselves, but it becomes even more important if they end up being used in a hundred other ways. The nation's DMVs put credentials in the pockets and purses of most Americans, an enormous power that could overwhelm efforts to create more decentralized ID systems.

Although the global ISO standards and AAMVA's work are quite advanced, participants in this ecosystem tell us that the work is not complete. Most of the players we spoke with recognized that privacy is an important value, and they told us that further work may substantially affect mDLs from a privacy standpoint. Currently, and for some time into the future, many of the details of how mDLs will work will be determined by a secret committee in the ISO standards-setting process, along with AAMVA, smartphone companies, individual state DMVs, and the companies those DMVs hire to design mDL apps.

At the same time, some states are already rushing to prepare for the creation of ISO-compliant mDLs, and some participants in the ecosystem expect that the first compliant state systems will be unveiled in the next year or so. Once states begin to roll out interoperable identity systems, it will become significantly harder to address any privacy problems that may arise at the technology level. Those issues should be addressed now.

We see seven immediate potential privacy problems with digital driver's licenses. Some of these are being addressed in current standards and plans—but others are not. In addition to these immediate concerns, there are a number of other, longer-term potential implications of and problems with mDLs. Here, we start with the immediate privacy issues and then discuss the broader issues.

1. POLICE ACCESS TO PEOPLE'S PHONES

The most immediate and obvious danger of transferring our driver's licenses from physical plastic cards to our phones would arise if we were required to hand our phones over to a police officer. That would be a total nonstarter for any mDL system given how much personal information our phones hold.

Fortunately, current mDL architects appear to recognize that having Holders hand their phones over to police officers (or other ID verifiers) is unacceptable and are designing a system that would not require Holders' phones to leave their hands. Instead, Holders would show a QR code on their phone screen to the officer or other verifier, or transmit the ID wirelessly to the Verifier.

Nevertheless, it's important to understand the context in which this technology will land. Despite a crystal-clear Supreme Court [requirement](#) that police obtain a warrant for smartphone searches, questionable "consent-based" police searches of people's cell phones happen [thousands of times a day](#). A police officer's request—"mind if I look at your phone?"—may make a search "voluntary" in the eyes of the law, but few searches based on such police requests are truly voluntary. That is especially true for members of poor and marginalized communities. And while people may think an officer is just planning to flip quickly through their phone, many are surprised when an officer then walks away with it. When your phone is taken from you—especially if it's taken out of your sight—you have no idea what is being done with it. An officer may have indeed just looked through it, but they may also have used forensic tools—which [have become widespread](#) within law enforcement—to copy the phone's [entire contents](#). If your cellphone is taken, police could even install spyware or make other changes to it.¹

Some [states](#) have enacted statutes declaring that presentation of an mDL "shall not serve as consent or authorization" for Verifiers to "search, view or access any other data or application on the mobile device." While it's helpful to clarify that using an mDL "may not be construed as consent" for an officer to search a phone, that kind of language, which is also [contained](#) in the federal bill enacted in late 2020, is weak. It doesn't categorically bar officers from exploiting the presence of cell phones in the digital verification process to achieve an abusive, so-called "consensual" phone search. Police officers must be expressly prohibited by statute from seeking consent for phone searches during mDL verifications.

Given rampant questionable police searches of mobile devices, statutory protections against such searches—already needed—will become even more vital if people's smartphones are to become a central and routine part of interactions with law enforcement.

¹ In addition, access to a person's phone can reveal to the police not just the data on the phone itself, but also, frequently, additional reams of data that are stored in the cloud, as apps on the phone provide a gateway to that online data.

2. CENTRALIZED ID TRACKING

Another significant question about a digital identity system is whether it would make centralized tracking possible. When someone visually inspects your plastic driver's license, no record of that inspection is automatically generated, retained, or shared with the DMV. But with a shift from plastic to digital identities, such tracking becomes possible. No system of electronic identity that permits that kind of tracking should be supported.

For mDLs, such tracking would mean the DMV would learn that “police officer X checked driver's license holder Z's ID on this date at this time.” Having information on police traffic stops flowing to the DMV may not seem like an enormous invasion of privacy, but remember that driver's licenses have become all-purpose identity documents in American life. This means that tomorrow, information could be gathered by DMVs about every bar, club, casino, office lobby, bank, pharmacy,

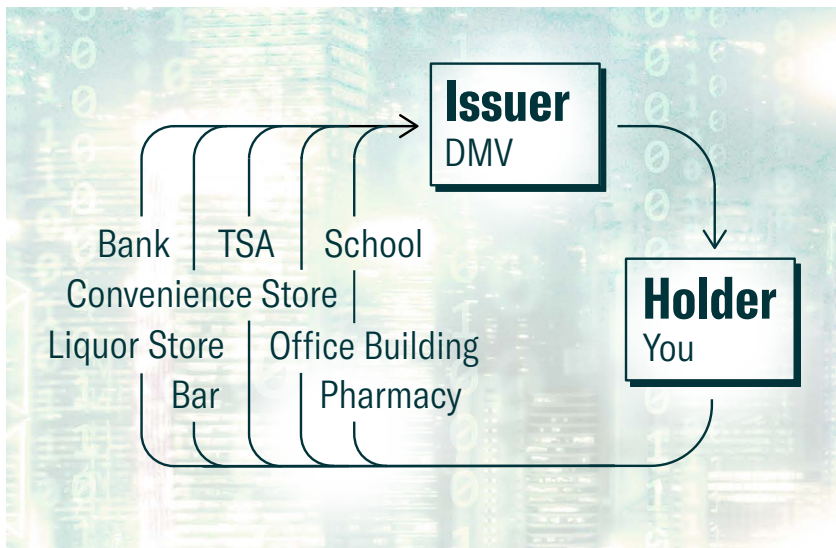
Questionable police searches of people's cell phones happen thousands of times a day.

doctor's office, and airport that you visit; every convenience store beer purchase, equipment rental, or hotel check-in; any applications for social services; and any other circumstance in which you may be asked to show an ID. The record of an ID presentation at a marijuana store that is legal in your state could be viewed quite differently by the federal government. And that list could grow exponentially; if a digital identity system starts being used for online transactions, it could include every website you visit.

In addition, if the police in your town have a memorandum of understanding (MOU) with your state's DMV—and almost all of them do—that could give the police access to whatever the DMV can see. Where a DMV chooses to outsource its verification functions, that data might also flow to private contractors—companies that would have a constant incentive to make money off our personal information.² DMVs themselves have long [sold access](#) to personal information as a revenue source.

.....

2 There is another group of companies that could also conceivably gather information: The ISO standard suggests as an option that Issuers hand off key distribution functions to third parties who will hold and verify the cryptographic keys that are used to verify the authenticity of a Holder's mDL. AAMVA is working on making that happen for American DMVs through what they call “Digital Trust Service” providers. If Verifiers carry out a real-time check of public keys with the Digital Trust Service, as opposed to, for example, preloading them, that service could gather data about such checks.



Fortunately, there are [fancy cryptographic techniques](#) that can solve this problem. They can allow a Verifier to mathematically confirm that a token was issued by a particular Issuer without the Issuer knowing to which Holder that credential was issued. In other words, a police officer’s device would ask the DMV, “Did you issue this person’s credential and

is it valid?” and the DMV could reply, “Yes that’s one of our tokens—but we have no way of telling you to which user we issued it.”

Such “unlinkable presentations” are an absolute requirement for any digital identity scheme. Digital IDs need to be designed on a technological level to prevent the Issuer from gaining a bird’s-eye view into a Holder’s transactions. Given that such techniques already exist, there’s absolutely no reason why they should not be incorporated into a digital identity system *before* it becomes operational. The more likely a system is to expand in the uses to which it is put, the more important implementing such protection from the outset becomes.

Unfortunately, in the current mDL system, which allows for online verification as an option, this protection is not being baked in. Using the online mode—which many mDL architects speak of as the default—a Holder can send a token to a Verifier that contains no information but lets the Verifier request information about the Holder directly from the DMV or other Issuer. And, as the ISO notes in its standard,

The issuing authority is present in each transaction in the on-line solution; therefore, the issuing authority knows when an mDL is used and what data is shared. If tracking is a concern, the issuing authority is advised to implement mitigating strategies to ensure the mDL and the mDL Holder are not tracked.³

.....

3 AAMVA points out that the ISO standard for the online mode (which the ISO calls “server retrieval”) does not include a field in the data sent from the Verifier to the Issuer that identifies the Verifier—just the identity of the Holder and the fields they have agreed to share. But they will see the Verifier’s IP address, which could be used to identify them. In addition, to establish the connection between the Issuer and the Verifier’s ID reader, they will use something called “TLS client authentication,” which easily and strongly identifies the reader to the Issuer. And if Verifiers were to be charged a fee for using the verification service, as has been suggested, the need to identify them would be even stronger. Rather than relying on good policies and trust in DMVs, tracking must be made technologically impossible in any identity verification system that is widely adopted.

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 Verifiers “do not report Holders’ personally identifying information to any centralized service that compiles usage data, regardless of whether the data is obtained from offline 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 “verification system” based on the online mode. The statute explicitly contemplates situations where a government agency “requires that an electronic credential or profile be verified through the verification system.” There is no requirement that that verification 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 verified—as a security benefit. 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 verification is to enable the collection of fees. DMVs have expressed reluctance to cover the costs of an mDL system that would mainly benefit businesses and other government agencies that verify ID. So, they are looking at revenue options. Among the possible models is a system in which Verifiers 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.

3. IDS THAT “PHONE HOME”

Even without a digital identity system designed so that Verifiers 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 specific 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 officer, 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, officers 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 identification or age-proofing just because

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

.....

4 An alternative to a revocation system is to provide short-term expirations that have to be remotely renewed regularly to keep a license valid. Those two systems are largely functionally equivalent.

someone is no longer qualified 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 tradeoffs. And it is only relevant if our driver’s licenses become digital-only—but, as we explain below, that shouldn’t happen.

4. VERIFIER ID TRACKING

Another threat to privacy comes not from the Issuer (DMV) but from Verifiers. Even if data doesn’t flow to the Issuer each time a person presents their ID, Verifiers 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 affiliates 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 Verifier 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 Verifier 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 Verifier and used to link presentations—or for automated face recognition. That’s a distinct privacy disadvantage of mDLs over physical licenses, where the Verifier 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 Verifiers to prevent it from saving copies of photos (not an easy task as a cryptographic matter, let alone an administrative one).

.....

5 In some states, police officers are authorized in some circumstances to seize and/or destroy driver’s licenses, rendering their holders not only unable to legally drive but also taking away the primary ID that most Americans use in a variety of contexts—including, in some states, voting. Remote access would allow an mDL in such circumstances to be demoted to a non-driver ID, but that is not sufficient reason to build such access. Instead, this practice should be ended. In a police stop, an officer can check to see if a driver’s license has been suspended or revoked, so there is no need to seize a license.

AAMVA says that “work is in progress that would alleviate the need for a Holder to share his/her portrait image.” That work is part of a second stage in the ISO standards practice aimed at allowing ID presentations over the internet. It would most likely involve using a fingerprint or other biometric identifier to allow Holders to authenticate themselves to their own phones as part of presenting their mDLs.

A robust privacy-protective system should also protect the privacy of Verifiers. In some circumstances, such privacy won’t matter—such as a police officer checking a motorist’s driver’s license—but in others, it could, especially if the data contained on mDLs and the uses to which they are put expand in unanticipated directions. An individual buying a used item off Craigslist, for example, may want to see the seller’s ID in case of problems, but may not necessarily want a record of the interaction sent to the government.

5. LACK OF PERSONAL CONTROL OVER ID DATA

A potential advantage of digital IDs is that if done right, they could improve the privacy of ID Holders by giving them the power to decide exactly what information they share with a Verifier—and to share no more than is necessary for a transaction.

The current mDL standards do contemplate this kind of selective disclosure, which is a good thing. For example, the standards will allow a Verifier to attest that they are over 21 without sharing their date of birth. ID holders may want to use their digital IDs to share other pieces of information in a similarly limited fashion, such as the ability to reveal whether they are the resident of a certain city or ZIP code without revealing their street address. We can’t anticipate all of the permutations of data minimization that holders may want—especially if mDLs begin to hold more forms of data, in which case user control will become even more important.

But Holders will only have whatever degree of control their Issuer allows to be built into the app, and—especially if the categories of data held in mDLs expand—it’s not clear whether those organizations will have any incentive to actively, responsively, and continually build in the privacy options that people need, or to judge what those needs might be.

Another threat to Holders’ control over what data is accessed is a proposal under discussion that would allow law enforcement officers to virtually “seize” the ID of a person without their permission, such as when they’re incapacitated. That would mean building a mechanism to allow law enforcement to read a person’s ID without their permission or control. Such a backdoor into

Holders will only have whatever degree of control their DMV allows to be built into the app.

the holder's security mechanism could be hacked—or abused, for example, by undercover police who have infiltrated 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.

6. SUSCEPTIBILITY 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 consequences of successful cyberattacks do need to be carefully considered: not only how serious the effects of an incursion could be, but who will bear the burden of an attack. All too often, we have seen that [companies don't spend](#) the money to protect their digital assets because when they're attacked it's their customers, not themselves, who suffer the consequences.

The direct alteration or forging of cryptographically signed mDL tokens would be difficult if not impossible, but the apps that hold them could still be vulnerable. An intruder could hack an mDL app to access the app's data or other data on your phone or copy your mDL token, allowing them to

⁶ Some proposals under consideration would ameliorate that problem by requiring that an officer take physical possession of a phone and plug a special certified reader into it. In the case of an incapacitated person with no physical ID, that would be better, but the creation of such a backdoor still raises concerns about hacking and abuse.

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, unfixable vulnerabilities](#) in phone hardware, as well as whatever *unknown* vulnerabilities exist in hardware and operating systems.⁷

And of course there are always other weak points. mDL boosters tout the ability to easily and remotely transfer a digital license when the holder’s phone is lost, replaced, or broken. This would require that the holder and their new device be properly authenticated, which is susceptible to fraud and trickery, and that the mDL on the old device be properly revoked, which is not necessarily an easy task for the reasons we discussed above.

7. FORCED APP INSTALLATION

Another privacy issue arises from the fact that a digital driver’s license system could require people to install what is essentially government software on their phones. Although many or all of the ID apps are likely to be built by private contractors, those companies will still be building their software for, and with the approval of, DMVs.

We don’t want to government to say, “You need to install this software on your phone.” But even if mDLs are fully optional, there are important steps that can be taken to give people confidence in the app they may want to install on their phone.

First, it’s important that the source code of these apps, which will be carrying out an essential public function, be transparent, so that experts (or any member of the public so inclined) can scrutinize them to confirm their operation and security. This will help assure people that the apps a) only do

.....

7 In addition, the security problems posed by digital authentication—especially internet or other remote authentication—may drive an increasing loss of control by consumers over their own devices. Because remote Verifiers will want assurance that you are not using someone else’s phone or other device, you would have to authenticate yourself to your own phone. That means there would have to be areas of the phone that are under the control of ID Verifiers instead of you, the owner of the phone. This would be another step toward making our phones devices built not to empower us but to control us.

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/nonprofit 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 standards for the provisioning process would also help give

consumers the ability to choose an open-source application they can trust. And, in the worst case, if mDLs were to become legally or practically mandated, an open standard would save us from a situation in which we’re forced to install a particular government app on our phones.

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 sufficient. There are potential longer-term consequences and evolutionary paths that digital identities might take that would hurt privacy and other civil liberties interests in significant ways.

1. EXPANSION OF USAGE

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 traffic 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 proofing." 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 proofing 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 once a standard is in place, people may start having to identify themselves everywhere online.

The fact is, corporate America likes to identify people. Among the motivations for this “thirst” to do so is cybersecurity. In security circles, there has long been talk about creating a “driver’s license for the internet” that everyone would have to use when they go online—meaning not a driver’s license that *can be used* on the Internet, but one that is *required to use* the Internet. The problem, of course, is that the former could easily morph into the latter. In the past, top executives at [Facebook](#), Google, and [Microsoft](#) have suggested ending online

anonymity. In 2010, for example, Google CEO Eric Schmidt [said](#) that the only way to manage online security problems “is true transparency and no anonymity.... it is too dangerous for there not to be some way to identify you.”

There is a real danger that once a standard is in place, people may start having to identify themselves everywhere online. Other interests that could drive that include:

- **Marketing:** “We want to be sure we know who you are so we can collect reliable personal data for online advertising and so that data is worth more.”
- **Enforcement:** “We need to make sure you aren’t someone we’ve previously banned due to violations of our terms of service.”
- **Age verification:** “For our legal due diligence, we need to know you’re over 13 or we can’t market to you.”⁸

And, of course, versions of those same motivations may operate offline as well, increasing real-world tracking in the same way.

If mDLs don’t make it more convenient to prove one’s identity, they’re not likely to succeed unless people are forced to use them. If they do make it more convenient to show ID, they will make demands for ID more frequent. In 2007, online pioneer Brad Templeton [dubbed](#) this the “Paradox of Identity Management”: “If you make something easy to do, it will be done more often....The easier it is to give somebody ID information, the more often it will be done. And the easier it is to

.....

8 The Children’s Online Privacy Protection Act bars the online collection of personal information from children under 13 without parental permission.

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 checkpoints and access controls is woven throughout American life. It could become impossible to go anywhere or do anything online without proving your identity. That would mean a significant loss of privacy. Anonymous speech has been an important American tradition since the nation’s founding (the Federalist Papers and many pro-revolutionary pamphlets were written anonymously) and brings many benefits, including the ability to do everything from freely associate and exchange ideas to seek support online for conditions and experiences that many find shameful to speak truth to power.

This potential for a drastic expansion in demands for identification makes it vital that any digital identity system created in the United States be built with the most bullet-proof privacy protections possible at the technological level. It’s also why it’s important that policymakers put strong privacy protections into mDL-enabling legislation, such as limits on commercial demands for ID.

2. EXPANSION OF INFORMATION CONTAINED

In addition to an expansion of the circumstances in which people are asked to prove their identity, we may also see an expansion of the data that is held in these digital IDs. AAMVA [points out](#) that

.....

⁹ We have seen ease-of-scaling lead to overuse in other surveillance contexts as well, such as cell phone location tracking, face recognition, and communications eavesdropping.

DMVs “are uniquely positioned to enroll citizens in an identification 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 fishing 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 flow; think of the information that could be valuable to various Verifiers:

- 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 fines and other fees
- Sex offender 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. Even if mDLs are designed for maximal Holder control over what data gets released, the Holder will still only have so much control. When a police officer demands to see your license as you’re driving, you will have to say yes. But you may also have to say “yes” to demands for data if you want to get a job, see a doctor, open a bank account, enter a shop, participate in an online

There’s no guarantee
that demands for ID
data will be limited to
what is necessary.

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.

3. MANDATORY DIGITAL IDs

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, *for the time being*, 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 Verifiers and cause those Verifiers 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 Verifiers 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 Emphasis added.

11 The TSA has introduced “Credential Authentication Technology” (CAT) machines to automatically check the validity of travelers’ IDs, and as of this writing, it is currently experimenting with using face recognition to also automatically verify that the ID belongs to the person presenting it. It is possible—indeed likely—that such machines could proliferate outside the airport to spare humans from checking IDs. But they are likely to be less reliable and more expensive than the systems that would be needed to automatically check mDLs.

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 specific 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 difficult to fully participate in modern life without one, and those who lack them suffer significant 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 effects:

a. Further Marginalization of People Without Smartphones

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.

Affordable 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 fixed broadband service. Many lower-income smartphone users have limited data plans. Even for those who have access to a smartphone and affordable broadband, [technical ability and lack of support](#) may pose a challenge. (This is another reason why mDLs should be designed to work only offline.)

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 *universal* smartphone ownership. While smartphones bring many conveniences, it would be unwise to allow ourselves to become too dependent upon them.¹²

.....

¹² In this, they are much like cashless payments—often convenient but not something we ever want to allow to [entirely supplant cash](#) as an option.

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. Harmful Precedent for Forced App Installation

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 fill 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 effort 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 they're required to install on phones they're required to carry.

There is no end to the range of bureaucratic enforcement measures, petty and grand, that could conceivably be enforced through a mandatory mDL app on people's cellphones. The desire of DMVs to tighten control over their bureaucratic domain should be seen in this context—driver's license expiration or revocation is just the tip of the iceberg. Because driver's licenses also serve as general-purpose identity cards in the United States, DMVs just happen to be in position to become the first to use modern identity technology to tighten control. But by creating a digital identity platform on which much else can be built, they could make it possible for every other bureaucracy to do the same. We may reach a point where every little municipal fee, fine, dues payment, uncompleted bureaucratic form, and overdue library book results in direct and inescapable enforcement actions taken through apps on people's phones.

The worst-case scenario is that people become prisoners of their own phones as various government agencies use compulsory app installation rules to turn them into enforcement devices for all kinds of legal and administrative rules. Radio-enabled digital IDs could be connected to vehicles and cars programmed not to start if the license of the person who gets

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 influence 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. New Possibilities for Abuse

Digital enforcement also increases the potential scale and consequences of abuse. Imagine a ruthless governor or an abusive official 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 flip 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 fight your way into the bureaucracy to get an explanation for the problem and then solve it.

d. Failures of Technology

Smartphones fail. They are dropped, get run over by trucks, suffer 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 Verifier'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 verification isn't working, and whether the problem lies with the Holder's phone or the Verifier'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 traffic 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 justified 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 officer's does—you go to jail.

In Britain, a whole political [movement](#) is [demanding](#) the right to physical rather than digital documents. European Union citizens who immigrated to the UK before the passage of Brexit, having established lives and families in that country, are being offered a special immigration status as the UK exits the EU. The UK government proposed to certify that status in a digital-only form, but the EU citizens are [loudly objecting](#). Among other things, confidence in digital-only methods was undercut by the UK's tragic "[Windrush Scandal](#)," in which unknown numbers of people who had legally immigrated to Britain between 1948 and 1970 from British colonies in the Caribbean were wrongly deported from the country where they'd been living for decades when they couldn't prove they were legal residents. And one reason they couldn't prove their legal status was that the Home Office had [lost](#) or [destroyed](#) their records.

While digital IDs have some advantages for Holders, such as selective data disclosure, a physical document is concrete, can't be quickly or easily modified, and stays under the control of the person who possesses it. In some circumstances, these are important advantages.

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 classified documents. The draft ISO standard for mobile driver's licenses we were able to find 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 "Verifiable 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.

Then there's the work being done within the U.S. states. While our transparent and democratically elected state legislatures are, in theory, the ultimate deciders regarding state driver's licenses, as a practical matter, that's not always true. The federal government imposed strict regulations on those licenses through the Real ID Act. And DMVs, like all agencies, have a lot of discretion and power themselves. Much of the work implementing Real ID has been performed by AAMVA, a Washington, D.C., association that most Americans have never heard of.

As driver's licenses have gained an increasingly significant 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 affect 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 staff 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 finalized.

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 Verifier. 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 officer—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 Verifiers 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 flexibility to provide attestations of general categories into which a Holder fits, 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 offline only, except when a Holder wants to set up a remote "appointment" for a specific task such as an update or renewal.

A "right to paper"

People should have a right to obtain and use a paper or other 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 be enacted in mDL-implementing legislation or elsewhere to bar those engaged in commerce or other regulated activities from refusing to accept physical IDs on an equal basis.

Restrictions on ID demands

Legislatures should consider enacting laws that limit ID demands in commercial contexts outside of specified circumstances, such as the purchase of age-restricted items.

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 reflection of the public interest. Many ID presentations, such as those in [airports](#), [banks](#), building [lobbies](#), and elsewhere, though usually unquestioned, amount to little more than theater and do nothing to enhance security at the cost of creating surveillance infrastructures that erode people's privacy.

There is no question that identifying people is sometimes a social need. But because of the way we have backed into the identity system we have today, we are not having the explicit political conversations and debates about our identity systems that we ought to be having. This raises the danger that a relatively small cadre of corporations and specialized government bureaucracies will build a new infrastructure for their own economic and administrative purposes, regardless of the larger implications. It raises the danger that there will be no balanced assessment of the costs and benefits of such a system and that we will adopt systems that do not strike the right balance between the needs for identification, security, and convenience and Americans' well-founded aversion to government and corporate surveillance and regimentation.

State legislators and
other policymakers
should ask hard
questions before leaping
to institute digital
driver's licenses

State legislators and other policymakers should ask hard questions before leaping to institute digital driver's licenses in their state. Is there a problem that we need to solve, for which mDLs are the solution? Are the side effects of that solution worth creating? Mobile driver's licenses would likely make it harder to alter or forge driver's licenses once they are issued. But how important is that project? There are undoubtedly occasions when people's ability to obtain and use fake IDs have serious consequences. But how common are those situations? How bad are their consequences? And how much will this measure help avert those situations, how much will it cost, and what side effects might it have?

It is not worth building a national identity infrastructure that will ratchet up the tracking of Americans and eviscerate online anonymity simply to reduce the scourge of college students using

fake IDs to buy beer. Nor is it worth doing so to fill 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 difference mDLs will make if they remain optional, and what the consequences will be if they're made mandatory. They should ask broad, far-sighted questions about the likely future evolution of such a system. If the goal is a broader system that can cover a variety of authentication needs, they should ask if this is the right vehicle. And if they decide to allow digital identity systems to move forward, they should insist that they be built with the strongest possible technological and legal privacy protections.

In the end, a digital identity system could prove just and worthwhile, if it is done right. But such an outcome is far from guaranteed, and much work will have to be done to implement a digital identity system that improves individuals' privacy rather than eroding it and is built not to enclose individuals but to empower them.