Mobile Driver's Licenses and the Costs To Privacy, Safety, and Security

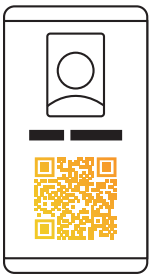
RESOURCE DEVELOPED BY:

Surveillance Resistance Lab

National Immigration Law Center

I. Mobile Driver's License (mDL) 101

What are Mobile Driver's Licenses?



- A digital or mobile driver's license (mDL) is a version of a driver's license that is stored on a smartphone, similar to how a credit card is stored on a mobile wallet.
- States and corporations are rapidly developing mDLs across the country, with little public awareness of their risks. As of December 2023, dozens of states are researching, testing, or implementing mDLs.

Why Should We Be Concerned?

- The mDL could easily become a primary tool for government and corporate surveillance because smartphones already are. We take our smartphones everywhere and use them to store vast amounts of personal information. Smartphones also collect massive amounts of data about our daily lives, often without our knowledge, and report that to corporations.
- With mDLs, our phones would become our IDs. Police and companies like Apple, Google, IDEMIA, and GET Group, whose business models are built around capturing massive amounts of data, have a mutual interest in increasing our data trails and reliance on our smartphones. Adding more sensitive personal information—like when and where we use our driver's licenses—increases the risk of surveillance and abuse.

We need to ask urgently: What are the interests behind mDLs? Who benefits? Which communities will become less safe?

Learn more in Section III: Who is Behind the Push for mDLs?

What are the potential risks and impacts of wider mobile driver's license use?

- DHS and ICE use of mDL information to identify and track anyone who they consider a national security threat, including immigrants
- Police will have easier physical access to our phones because of mDLs
- Surveillance by government agencies and corporations
- Tracking by "Verifiers" every time and place you use your mDL
- Increased corporate profits from a government-required mDL app, leading to the continued privatization of essential government services
- Decreased protections after hard-fought "Driver's Licenses for All" victories
- Greater risk of cyberattack

Learn more in Section II: Potential Risks and Impacts of mDLs.

How Do Mobile Driver's Licenses Work?

Three parties are involved in the mDL ecosystem:

An **Issuer**: typically, the state Department of Motor Vehicles (DMV) (or its corporate contractor), which issues and stores mDL information in a central place, similar to data on physical licenses;

A **Holder**: the individual license holder; and

A **Verifier**: the official or person who checks the mDL and verifies information (name, age, address, etc.), such as a police officer, TSA agent, or liquor store clerk.

Information from the mDL is communicated through a digital verification system called public key cryptography, in which a pair of digital "keys" are used to verify mDL information. Three interactions take place:

1. ISSUER

The ***Issuer*** first provides the mDL to the individual *Holder* (making it available on the person's smartphone) and uses a unique ***private*** key to digitally sign the mDL as authentic.

2. HOLDER

When asked to provide their driver's license or ID, the ***Holder*** shows their smartphone to the Verifier (either physically in person, or using their mDL online).

3. VERIFIER

The ***Verifier*** then uses a mDL reader to scan the mDL, verify the license with its *public* key, and retrieve specific data.

The Verifier can retrieve data directly from the Holder's smartphone or from the Issuer directly via a server.

Where could mDLs be used?

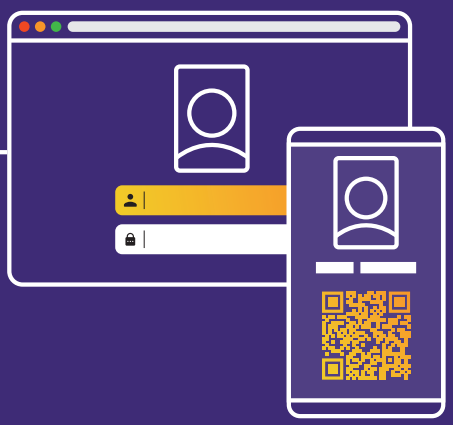
States and corporations are pushing for mDLs to be used in a broad range of situations to check people's identities and other key information about them. This includes:

In-person:

- Showing your driver's license to police (like in a traffic stop)
- Traveling through an airport or international border
- Proving your identity to a hotel, bank, or store
- Buying alcohol or other age-restricted products

Online:

- Verifying your identity with particular websites, like a bank or online retailer
- Verifying people's age to access social media platforms, porn sites, and other age-restricted content



II. Potential Risks and Impacts of Mobile Driver's Licenses

Check out Section I: Mobile Driver's License 101 to learn about what mDLs are and how they work.

Mobile driver's licenses (mDLs) increase the potential for government and corporate monitoring, control, and denial of basic resources.

1 **DHS and ICE Use of mDL Information to Identify and Track Anyone They Consider a National Security Threat—including Immigrants:**

Congress authorized the Department of Homeland Security (DHS) to regulate mDLs that are used for federal purposes, which gives DHS a key role in setting up the default mDL infrastructures and data sharing practices across the country. Generating massive amounts of information, mDL programs and data will make it easier for DHS to target all drivers, especially immigrants and other groups characterized by DHS as a "national security threat". Learn more in Section III: Who is Behind the Push for Mobile Driver's Licenese?

2 **Police will have easier physical access to our phones because of mDLs:**

Residents showing their mobile driver's license to police may be required or coerced into physically handing over their smartphone. This could give local police, ICE, or U.S. Customs and Border Protection (CBP) access to people's smartphones and information, without a warrant or true consent. Police could not only view driver's license information, but also use that license verification process to unlawfully extract more data and personal information. This is not new; police already physically extract data from cellphones using mobile device forensic tools—often without a warrant—and use remote tracking tools to search location data on over 250 million devices. mDLs further increase the risk of police misconduct and surveillance.

3 **Surveillance by Government Agencies and Corporations:**

Mobile software is often built with a "phone home" function, where the app contacts the developer automatically, without user consent or awareness, to complete a task, update information, or share an app or smartphone's status or location. This could have multiple consequences. First, "phoning home" can compromise a user's privacy by sharing the mDL Holder's data and information with the DMV or private vendors, such as the app developer. Second, "phoning home" could be used to alter or even revoke driver's license privileges without a holder's awareness.

4 **Tracking Every Time and Place You Use Your mDL:**

Every time a person presents their mDL to access a resource or prove their identity, the Verifier could potentially record and track this information. This means that any time someone goes to a liquor store, bank, airport, and other locations where IDs are required, the Verifier could log their visit, creating a long record of personal information, movements, activities, and behaviors. Depending on the software or program used for the mDL, the phone itself might also create a similar tracking log and compile additional "metadata," such as information about the person's smartphone and wifi network access. Tracking could lead to "function creep" as law enforcement and other government agencies may seek to access these massive datasets, as was the case in Australia when the country introduced a digital health and welfare Access Card.

5 Increased Corporate Profits From a Government-Required App, Leading to the Continued Privatization of Essential Government Services:

An mDL is essentially a government document that we will all be encouraged and incentivized to download on our smartphones. But to hold this digitized document, people would be required to use a corporate digital wallet or similar technology. Digital wallets such as Apple Wallet are designed to extract large amounts of consumer data which the corporation can then use and/or sell. A public, open source digital wallet could be designed, but states are choosing to rely on corporations instead. Vital government functions and services, like the issuance and administration of government IDs, should remain public and free of corporate control. Holding an essential government document should not drive the volume of corporate data extracted from smartphone users.

6 Decreased Protections After Hard-Fought "Driver's Licenses for All" Victories:

Across the country, communities have fought for years to expand access to driver's licenses for all residents, while protecting people from government surveillance and limiting local entanglement in federal immigration policing activities. mDLs could threaten these hard-won gains. People stopped by police, ICE, and CBP could be compelled to hand over their phone to show their driver's license, potentially giving police unwanted and unlawful access to the rest of the content of people's smartphones. Also, the large databases storing sensitive mDL data could potentially be accessed by ICE, CBP, and DHS to bypass privacy laws and other protective policies for immigrants.

7 Greater Risk of Cyberattacks:

All digital files can be hacked into and compromised. mDLs are no exception. By digitizing driver's licenses and storing sensitive information in centralized databases, the government is needlessly placing our identities in harm's way. In early 2023, a cyberattack compromised the personal information of everyone with a driver's license in Louisiana, including those with mDLs. Hackers could not only access our data but also steal our identities.

What do we do about these risks? Check out Section IV: What Can I Do about Mobile Driver's License in My State?

For more information on the broader risks of digital IDs, check out the Surveillance Resistance Lab's Digital ID Community FAQs.

III. Who is Behind the Push for Mobile Driver's Licenses?

Check out Section I: Mobile Driver's License 101 to learn about what mDLs are and how they work.

What is the Role of DHS in the Shift to Mobile Driver's Licenses?

Through its regulatory authority and various corporate partnerships, the U.S. Department of Homeland Security (DHS) has been setting up the default infrastructure to push for greater mDL use across the country, and to influence the implementation of state mDL programs.

DHS control or even influence over state mDL programs could have alarming consequences for immigrant drivers.

- **Federal immigration authorities *already use* driver information from state DMVs to identify, track, and target immigrants for detention and deportation, relying especially on address and vehicle information.**

  DHS agencies, specifically U.S. Immigration and Customs Enforcement (ICE), obtain this information in various ways, including by contracting with data brokers such as LexisNexis that buy, share, and resell DMV data. A shift from physical licenses to mDLs creates more opportunities for data about our daily lives to be created and collected. DHS' role in creating mDL infrastructure increases the likelihood that the department will have access to this data and push to make it interoperable with other databases. As outlined in Section II, *potentially every use of mDLs can be tracked*, including location information.

- **Although DHS has focused on developing mDLs that are valid for federal purposes (such as boarding a plane or entering a federal building), we are beginning to see the emergence of non-REAL ID mDLs that are available to various state residents regardless of immigration status.**

  As has been the case with physical licenses, any mDL standards and technologies that DHS adopts for REAL ID purposes will influence the machinery that the states use to set up non-REAL mDL programs. This includes how data collection and sharing processes are set up, what apps, including digital wallets, are used, which types of mDL readers become standardized, and which companies gain further dominance over this technology.

DHS' Mobile Driver's License Authority

Through the REAL ID Act of 2005, DHS requires states to meet specific requirements in order for their driver's licenses to be acceptable for certain federal purposes such as boarding a plane (referred to as a "REAL ID license"). Undocumented immigrants are not eligible for REAL ID licenses, but states can issue non-REAL ID licenses to residents regardless of their immigration status.

The REAL ID Modernization Act, passed in 2020, granted DHS authority to regulate mDLs for federal purposes. In April 2021, DHS published a "Request for Information", revealing its plans to set-up a national mDL standard that allows for "interoperability" (compatibility and information-sharing between various mDL systems).

In August 2023, DHS's Transportation Security Administration (TSA) posted a proposed rule setting minimum requirements for state-issued mDLs to be accepted for REAL ID purposes. Immigrants' rights advocates have raised concerns that TSA is prematurely rushing to influence state mDLs based on a false sense of urgency, in spite of acknowledging that it is still too early to set mDL standards. In its haste, the agency is sweeping aside important civil liberties and privacy interests, prematurely locking states into underdeveloped standards, and further privatizing an essential government service.

Who Are the Corporate and Other Key Players?

Corporations have been pivotal to the development of mDLs. These companies stand to profit from lucrative government contracts and the incentivized use of their technologies, such as mobile wallets and other mDL mobile applications. Corporate partnership with the federal government, in particular, exponentially increases profitability and the likelihood that a few companies will monopolize the field of mDL technology in the United States, including the development of state mDL programs.

DHS has already taken several steps to build private-public partnerships around wider mDL adoption. Starting in early 2022, TSA partnered with several for-profit companies to test the acceptance of mDLs at select TSA PreCheck checkpoints, with 25 participating airports to date.

The following companies play a role in the development or support of key mDL pilot programs that are connected to DHS activity or oversight:

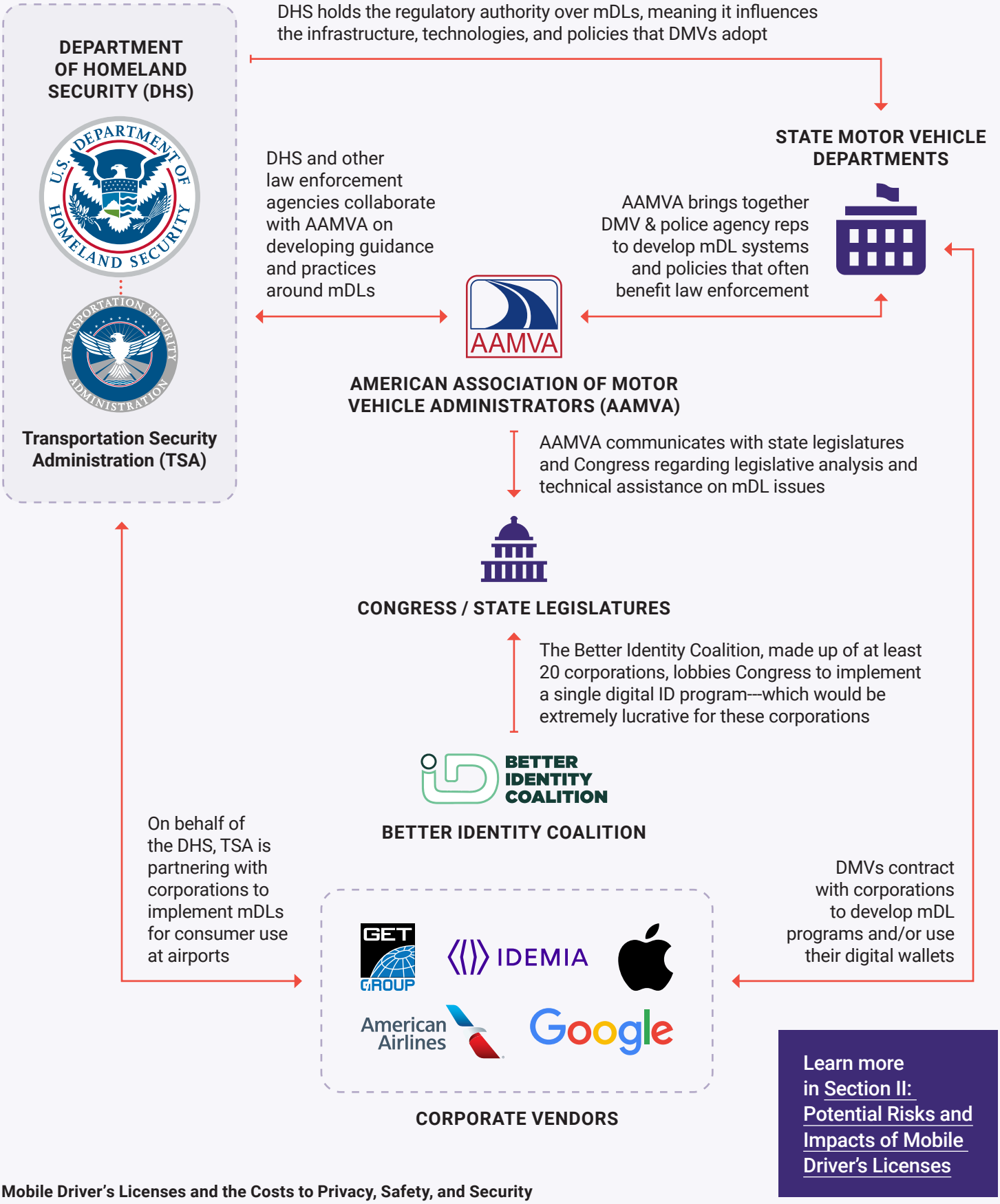
- ***Apple*** announced a mDL pilot in 2021 that, to date, allows driver's licenses and IDs from Arizona, Colorado, Georgia, and Maryland to be stored on Apple Wallet, and used on iPhones and Apple Watches at participating TSA checkpoints. Apple plans to expand its mDL pilot to several other states in the coming years.
- ***Google*** launched a program that allows Maryland mDLs to be added to Android phones via Google Wallet and used at participating TSA checkpoints.
- ***IDEMIA*** contracted with TSA to supply mDL readers to the government for Apple's mDL pilot, allowing mDLs stored in Apple Wallet to be verified at TSA checkpoints; and separately, developed proprietary mDLs for Arizona, Delaware, Oklahoma, Mississippi, Missouri, and Iowa.
- ***GET Group*** announced partnership with TSA to begin accepting Utah mDLs at participating TSA checkpoints via the Get Mobile app.
- ***American Airlines*** announced a proprietary digital ID for American Airline customers, called the "American Airlines Mobile ID," to be used in lieu of a physical license or ID, at participating TSA checkpoints.

Industry Coalitions

Many of these companies are involved in various coalitions and private, or quasi-private, groups that have been instrumental in building out the machinery for mDL use and adoption including:

- The ***American Association of Motor Vehicle Administrators (AAMVA)*** is a nonprofit, nongovernmental organization representing state and local officials such as transportation, DMV, and police officials "who administer and enforce motor vehicle laws." AAMVA developed and controls the State-to-State Verification Service, an information exchange system that includes a central database containing personal information about drivers, including the last five digits of their Social Security numbers and whether they have a REAL ID license. AAMVA has developed resources on mDLs for its members like model mDL legislation, implementation guidelines, training videos, and white papers to push for wide adoption and use of mDLs in the United States;
- The ***Better ID Coalition*** is a group of companies that are lobbying for a universally-accepted digital ID. The coalition includes data brokers, like Equifax and Transunion; banks, like JPMorgan Chase and Discover; and others like IDEMIA and CVS. These companies stand to profit from the opportunity to collect massive amounts of data from users once a universal digital ID is adopted.

mDL Key Players



Learn more in Section II: Potential Risks and Impacts of Mobile Driver's Licenses

IV. What Can I Do About Mobile Driver's Licenses in My State?

Check out Section I: Mobile Driver's License 101 to learn about what mDLs are and how they work.

Concerned about the growth and risks of mobile driver's licenses (mDLs) where you live? Check out this guide for suggested action steps to gather information, reduce the risks, and advocate for protective policies.

1 Get a Status Update

Find out if your state is planning to implement mDLs. Here are a few ways to get information:

- **Check our list of active mDL programs with information by state and corporate vendor.** We add to this frequently, and rely on people like you across the country for updated information about their states—so please contact us if you have information that's not on this list!
- **Check AAMVA's map of mDL implementation** for the US and Canada. (We do not know how this is updated, so recommend that you verify information with your state officials.)
- **Look for announcements, media coverage, draft legislation, and testimonies from state officials**, including your state DMV, Governor's office, and budget hearings.
- **Search for contracts with your state DMV** for mobile driver's license development, equipment, or even facial recognition systems. Search for the vendors listed in Section III: Who is Behind the Push for Mobile Driver's Licenses?.
- **Review state lobbying records** to see if any of these companies have met with state officials about mDLs or digital IDs.

2 Ask Questions

The introduction of mDLs in your state poses serious concerns and challenges that need to be addressed. Check out potential questions to ask state elected officials and DMV representatives, ideally before a mDL is piloted.

3 Advocate for Protective Policies

Build or activate existing coalitions with local and state advocates and communities who could be disproportionately affected by mDL implementation, especially immigrants, unhoused people, formerly incarcerated people, youth, LGBTQ+ people, and others involved in Driver's License for All fights.

Advocate for policies and legislation that do not reinforce the reliance on smartphones and prioritize data protection and residents' security over profit and trackability. This could be banning the development of mDLs, or alternatively, advocating for policies that:

- Prohibit corporate capture of mDL data
- Prioritize data minimization and deletion
- Prevent tracking of mDL use and interactions
- Prohibit sharing of mDL data with federal, state, and local government agencies, including law enforcement and commercial entities
- Prevent mDLs from becoming mandatory or incentivized over physical licenses
- Prohibit the REAL ID verification system from facilitating the use or sharing of driver's license information for immigration enforcement purposes (i.e. no sharing with federal, state, local government agencies; law enforcement; commercial entities or other persons)

4 Learn More

Check out the resources below to learn more about mDLs' technical infrastructure, the role of DHS, and how mDLs fit into larger concerns about data sharing of driver's license information.

Privacy and equity risks of mDLs

- *Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom*, ACLU, available at: www.aclu.org/report/identity-crisis-what-digital-drivers-licenses-could-mean-privacy-equity-and-freedom

How state driver's license data is already used for tracking

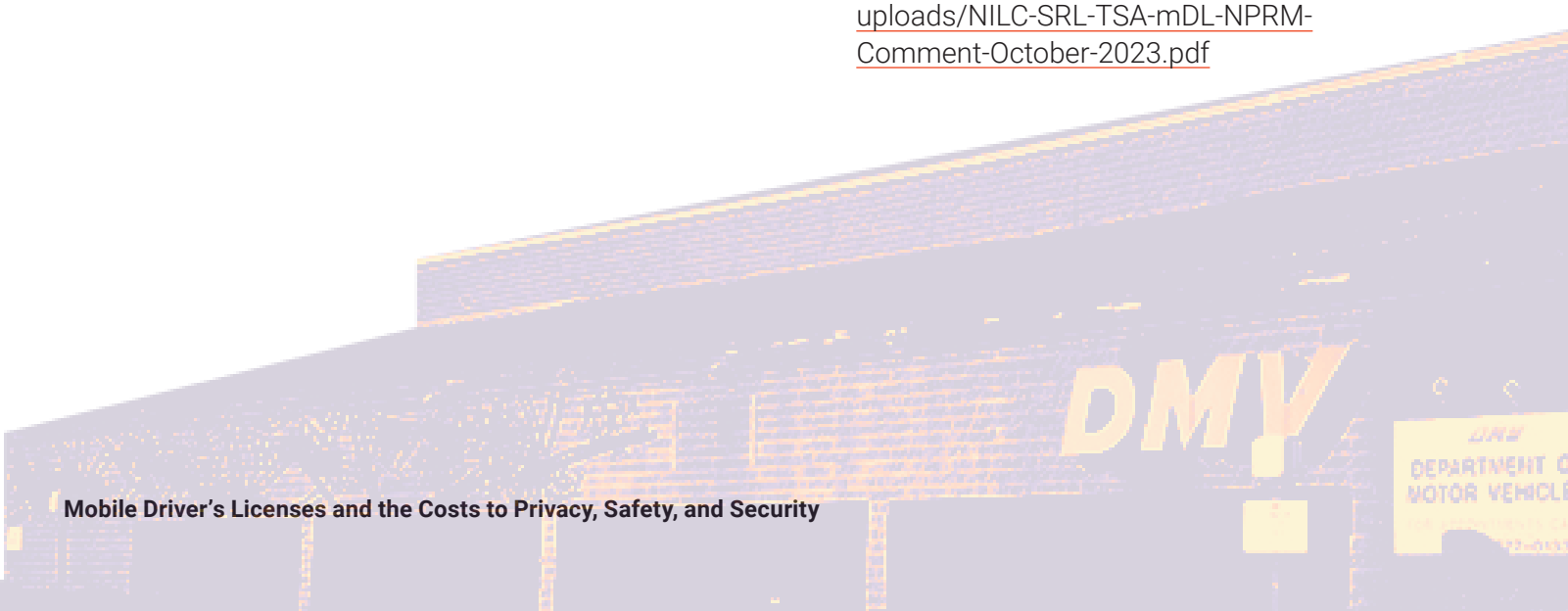
- *State Driver's License Data: Breaking Down Data- Sharing and Recommendations for Data Privacy*, Just Futures Law, available at: www.justfutureslaw.org/driversprivacy
- *American Dragnet Data-Driven Deportation in the 21st Century*, Georgetown Center on Privacy and Technology available at: americandragnet.org
- *Immigration Enforcement–related Information Sharing and Privacy Protection*, NILC, available at: www.nilc.org/issues/immigration-enforcement/imm-enforcement-info-sharing-and-privacy-protection

Smartphone tracking

- *New documents reveal 'huge' scale of US government's cell phone location data tracking*, TechCrunch, available at: techcrunch.com/2022/07/18/homeland-security-cell-phone-tracking

Understanding the role of DHS in driver's license issues, including mDLs

- *The REAL ID Act: Questions and Answers*, NILC, available at: www.nilc.org/wp-content/uploads/2015/11/REAL-ID-Act-Q-and-A.pdf
- NILC et al. Comments on DHS' Request for Information on "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Mobile Driver's Licenses", available at: www.regulations.gov/comment/DHS-2020-0028-0041
- NILC & SRL Comments on DHS and TSA Notice of Proposed Rulemaking on "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Waiver for Mobile Driver's Licenses," available at https://surveillanceresistancelab.org/wp-content/uploads/NILC-SRL-TSA-mDL-NPRM-Comment-October-2023.pdf



Questions to Ask State Officials

General

1. What has been the planning, design, and development phase? Have you reached out to and consulted with privacy and encryption experts, civil rights and liberties advocates, and impacted communities? How will you engage with the public in the development and before roll-out?
2. What gives the DMV statutory authority to implement a mDL? Does the DMV plan to issue any new regulations to facilitate the mDL program? When will notice be published?
3. What devices will the mDL be compatible with? Will there be a separate app or software that mDL users will need to install, and who is developing that?
4. Will both standard and REAL ID licenses be available as mDLs, or only the latter?
5. For mDLs that are REAL ID compliant, what is the process for obtaining approval from DHS so that the program meets federal requirements?

Vendors and Other Entities

1. Who is the vendor developing the state mDL? Are there other involved entities?
2. Has the state audited vendor practices, particularly regarding data collection, sharing, and minimization, and will you publish the results?
3. Congress gave DHS the authority to develop the interoperability standards for mDLs. How has DHS been involved in the development of the state mDL program?
4. Has the state partnered or been in consultation with DMV agencies from other states or with any federal agencies on this?
5. Has the state interacted with AAMVA (the American Association of Motor Vehicle Administrators) or other non-governmental entities during this process, and if so, wat was their role?
6. What role is the DMV playing in the development of the mDL readers that will be used by verifiers when the program is implemented?

Privacy, Data Protection, and Disparate Impacts

1. What are the privacy protections? What technical and legal safeguards will you put in place to protect people's data and their interactions?
2. What are the policies and protections that will prevent ICE, CBP, and DHS access to your state's DMV records?
3. How has the state considered the disparate impact of this technology on immigrant communities, formerly incarcerated people, unhoused people, youth or seniors without access to driver's licenses, people with disabilities, and other protected classes?
4. Aside from convenience, will mDL holders enjoy any benefits that physical cardholders do not? How will you prevent discrimination or barriers that prevent access to services for physical cardholders?
5. What data sharing policies will be implemented, especially with law enforcement agencies? Have you had discussions with any police departments or otherwise given thought to how mDLs will be presented/inspected in law enforcement interactions, such as traffic stops?
6. What data minimization and privacy-preserving measures are you implementing to ensure mDLs won't result in a massive, centralized tracking system?

SURVEILLANCE RESISTANCE LAB

surveillanceresistancelab.org
@S_ResistanceLab
@surveillanceresistancelab

The Surveillance Resistance Lab is a think and act tank focused on state and corporate surveillance as one of the greatest threats to migrant justice, racial equity, economic justice, and democracy. We challenge how surveillance at the nexus of state and corporate power not only threatens privacy, but seriously erodes fundamental rights leading to heightened oppression and repression. To counter this threat, the Surveillance Resistance Lab engages in investigative research, campaign incubation, advocacy, and organizing. We are committed to movement building to fight for accountability and government divestment from technologies that expand systems of control and punishment (as well as suppress dissent and difference) in public spaces, schools, workplaces, and at and across borders.

NILC NATIONAL IMMIGRATION LAW CENTER

nilc.org
@nilc
@nilc

The National Immigration Law Center (NILC) is one of the leading organizations in the U.S. exclusively dedicated to defending and advancing the rights of immigrants with low income. At NILC, we believe that all people who live in the U.S. should have the opportunity to achieve their full potential. Over the years, we've been at the forefront of many of the country's greatest challenges when it comes to immigration issues, and we play a major leadership role in addressing the real-life impact of policies that affect the ability of low-income immigrants to prosper and thrive.

Our organizations would like to thank the following for their contributions to this report:

Writers: Alli Finn, Chiraayu Gosrani, Ed Vogel, Sarah Kim Pak, Tanya Broder

Reviewers: Christine Sauve, Jay Stanley, Mizue Aizeki

Illustrations and Design: Objectively

December 2023