Comment on:

U.S. Department of Homeland Security, Request for Information on "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Mobile Driver's Licenses,'' Docket Number DHS–2020–0028

SUBMITTED BY THE NATIONAL IMMIGRATION LAW CENTER AND THE UNDERSIGNED ORGANIZATIONS

The Department of Homeland Security ("DHS") seeks comments on its "request for information" ("RFI") "to inform an upcoming rulemaking that would address security standards and requirements for the issuance of mobile or digital driver's licenses to enable Federal agencies to accept these credentials for official purposes as defined in the REAL ID Act and regulation."[1] The National Immigration Law Center (NILC) and the undersigned organizations submit the following comments regarding the need to protect the privacy of drivers' information in mobile driver's license (mDLs) regulations in response to DHS' "Questions for Commenters" Nos. 2, 3, 6, 8, 11, and 15.[2]

Established in 1979, NILC is one of the leading organizations in the U.S. exclusively dedicated to defending and advancing the rights and opportunities of low-income immigrants and their families. For many years, NILC has published articles, provided technical assistance, and litigated on issues pertaining to driver's licenses, the REAL ID Act, and immigration enforcement.

INTRODUCTION

The RFI describes DHS' envisioned model for mDL issuance, usage, and acceptance by federal agencies for official purposes. An mDL, as defined in the RFI, is "a digital representation of the information on a state-issued physical DL/ID, and is stored on, or accessed via, a mobile device."[3] DHS' mDL model requires three players—the mobile device user (i.e. mDL holder or licensed driver), the Department of Motor Vehicles ("DMV") or state equivalent that "would be responsible for issuing an mDL" onto the mobile device, and the verifying federal agency that is empowered to retrieve and verify mDL data for identification and other official federal purposes.[4] An mDL uses cryptographic technology to securely transfer a driver's mDL information to a verifying party (such as a Transportation Security Administration agent or U.S. Immigrations and Customs Enforcement officer) via offline and online data transfer modes,[5] described further below, in lieu of presenting a physical driver's license card.

This shift raises serious privacy concerns and implications for citizens and immigrants. In particular, the RFI does not seek consideration of several key protections that are necessary to ensure drivers' data

[1] Request for Comment of Request for Information, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Mobile Driver's Licenses, Office of Strategy, Policy and Plans, Department of Homeland Security (DHS), Docket No. DHS–2020–0028, 86 Fed. Reg. 20320-26 (Apr. 19, 2021), https://www.govinfo.gov/content/pkg/FR-2021-04-19/pdf/2021-07957.pdf, [hereinafter "RFI"].
[2] *Id.* at 20325-26.
[3] *Id.* at 20322.
[4] *Id.* at 20323.
[5] *Id.* at 20326.

privacy as well as their physical and digital safety, including transparency and accountability measures, safeguards against impermissible information-sharing (such as for immigration enforcement or other unintended purposes), and protections against discrimination or other harm that is likely to occur in the mDL context.

THE RFI SETS THE STAGE FOR A NATIONAL IDENTIFICATION SYSTEM THAT PRESUMES DATA-SHARING, INTEROPERABILITY, AND ONGOING COMMUNICATION BETWEEN DMVs AND FEDERAL AGENCIES

The RFI invites the public and interested stakeholders to provide comments that would "*help inform* a potential rulemaking" and "*facilitate development* of the regulation" setting minimum technical requirements and security standards for the issuance of mDLs compliant with the REAL ID Act.[6] But the RFI is not simply a benign request for information to help guide DHS in an ostensibly nascent rule development stage. It reveals that DHS is much further along in the development of a national mDL standard.

In fact, the RFI sets the stage for the endgame: a national identification system that presumes data-sharing, interoperability, and ongoing communication between mDL devices, state DMVs and federal agencies, including DHS. The RFI includes "DHS's envisioned reference implementation and interoperability model" for mDLs that "would require DMVs . . . to conform to criteria" that DHS is responsible for establishing.[7] This gives DHS an encroaching role over the administration and design of state driver's license programs and pushes states closer to a future in which mDLs become the norm.

ANY REGULATION OF mDLS FOR REAL ID PURPOSES MUST PROTECT THE PRIVACY OF DRIVERS' INFORMATION AND PROVIDE FOR TRANSPARENCY AND ACCOUNTABILITY

- REGULATIONS MUST PROTECT THE PRIVACY OF STATE DRIVER'S LICENSE INFORMATION

Creeping incrementalism is the hallmark of federal regulation of state driver's licenses. Without any hearings or debate, Congress passed the REAL ID Act as part of the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief in 2005 (HR 1268). Under the REAL ID Act, driver's licenses and state IDs that do not meet the act's requirements will not be accepted for specifically defined "official" federal purposes.[8] Neither the Act nor regulations implementing it contemplated the issuance of mDLs.[9]

[6] *Id.* at 20321 (emphasis added).
[7] *Id.* at 20323.
[8] Improved Security for Drivers' Licenses and Personal Identification Cards, Title II of the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, https://www.dhs.gov/xlibrary/assets/real-id-act-text.pdf [hereinafter "REAL ID Act"]. The current deadline for individuals to present REAL ID-compliant driver's license or identification cards at airport security checkpoints for domestic air travel is May 3, 2023, *see* DHS Press Release, https://www.dhs.gov/real-id/news/2021/04/27/dhs-announces-extension-real-id-full-enforcement-deadline.
[9] *See, e.g.*, REAL ID Act, § 208(b) (listing the features on driver's licenses and identification cards that must be included on driver's licenses and identification cards).

The Act gives DHS a prominent role in state driver's license issuance: states that seek certification of their licenses as compliant with REAL ID must meet a wide range of requirements.[10] These include requiring license applicants to prove (and state agencies to verify) their U.S. citizenship or immigration status, as well as many other benchmarks, including the physical appearance of licenses and the information that must be included on them.

In 2020, Congress passed the REAL ID Modernization Act as part of the Consolidated Appropriations Act of 2021.[11] It re-defines driver's licenses and identification cards to include those "stored or accessed via electronic means, such as mobile or digital driver's licenses [or identification cards], which have been issued in accordance with regulations prescribed by the Secretary.'' The Act also authorizes acceptance of application information through electronic transmission methods.

The REAL ID Act and its regulations do not include provisions that protect the privacy of driver's license information. The REAL ID Modernization Act does not include meaningful privacy protections for mDLs and does not set standards for how an mDL should be issued, criteria for the DHS Secretary to develop privacy protections, or limits on outsourcing the development or management of the verification system.

Despite its frequent reference to "privacy", the RFI focuses on "security standards and requirements for the issuance of mobile or digital driver's licenses to enable Federal agencies to accept these credentials for official purposes as defined in the REAL ID Act and regulation."[12]

The absence of privacy protections is of critical concern to drivers who have licenses that are not REAL ID-compliant and who fear that information provided to DMVs will be used by DHS agencies for immigration enforcement.

- REGULATIONS MUST INCLUDE TRANSPARENCY AND ACCOUNTABILITY MEASURES AND PREVENT OUTSOURCING TO UNACCOUNTABLE ENTITIES

The RFI requests "comments on how DHS should choose the correct standard(s) for mDLs, and on the appropriate baseline standard(s) that DHS should impose,"[13] but the industry standards that the RFI relies on are shrouded in secrecy. For example, the RFI refers repeatedly to Implementation Guidelines prepared by the American Association of Motor Vehicle Administrators (AAMVA). AAMVA is a "nonprofit organization …[that] represents the state, provincial, and territorial officials in the United States and Canada who administer and enforce motor vehicle laws."[14] But AAMVA Guidelines are only available to AAMVA members.

[10] *See Full Compliance Certification Checklist*, American Association of Motor Vehicle Administrators (AAMVA) (Oct. 9, 2012), www.aamva.org/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=3069&libID=3055.
[11] The REAL ID Modernization Act, Title X, Div. U of the Consolidated Appropriations Act, 2021, Public Law 116-260 (Dec. 27, 2020), https://www.congress.gov/bill/116th-congress/house-bill/133/text (hereinafter, "REAL ID Modernization Act").
[12] RFI at 20320.
[13] *Id.* at 20325.
[14] *About AAMVA*, AAMVA, https://www.aamva.org/about-aamva/#GeneralInformation (last visited May 27, 2021).

Moreover, the RFI makes no reference to the work that AAMVA clearly has initiated regarding the development of mDLs.[15] AAMVA has developed model mDL legislation which similarly is not available to the public.[16] In addition, AAMVA's role "to test technologies, establish basic governance rules and policies, and create an operating framework to discover the path to a full DTS [mobile Digital Trust Service]" is also unmentioned in the RFI.[17]

Deference to AAMVA in regulating or managing mDLs presents risks for non-citizens because their information may be shared with federal agencies in the absence of safeguards or limits. For example, AAMVA developed and controls the system implementing REAL ID's requirement that states have access to driver's license databases of other states.[18] Under that State-to-State system, information about whether an individual has a REAL ID compliant license or identification card may be transmitted to other states and is maintained in an AAMVA database.[19] Since AAMVA is not a federal agency, it may not be subject to the Freedom of Information Act (FOIA) , or the Administrative Procedure Act. Deferring to an outside entity such as AAMVA for development and management of a mDL verification system would undermine public oversight and accountability.

The RFI repeatedly references the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draft standards, indicating its intent to adapt them for DMVs in the United States.[20] But the ISO/IEC standards are currently under development, and are not final, preventing meaningful comment on their application to the RFI. Additionally, like AAMVA, the ISO is an external entity and closed group that is comprised of and supported by private corporations as well as non-governmental organizations.

The RFI neither asks for nor discusses measures to ensure accountability and oversight or how any limits in potential future regulations would be enforced. And DHS' repeated exemption of databases and records systems from Privacy Act requirements pertaining to the accuracy of information, the ability to obtain access to and correct records, or the availability of judicial review[21] further suggests that DHS intends to operate its envisioned mDL system outside of regulatory requirements and without public oversight.

---

[15] *See, e.g.*, *AAMVA Plans for an mDL Digital Trust Service*, AAMVA, https://images.magnetmail.net/images/clients/AAMVA//attach/subfolder/mDLDTSsummary052021.pdf (last visited May 27, 201).

[16] *See mDL Resources / Documentation*, AAMVA, https://www.aamva.org/mDL-Resources/ (last visited May 27, 2021).

[17] *AAMVA Plans for an mDL Digital Trust Service*, *supra* note 15.

[18] *See* REAL ID Act § 208(d)(12); *State-to-State (S2S) Verification Services*, AAMVA, https://www.aamva.org/State-to-State/ (last visited May 27, 2021). The State-to-State system currently determines whether a person has only one driver's license and only one REAL ID-compliant document.

[19] AAMVA's publicly available information does not disclose that its central databases contain information about whether the individual has a REAL ID-compliant or non-compliant license. *See State-to-State FAQs*, AAMVA, https://www.aamva.org/pubs2sfaqs-general/.

[20] RFI at 20322-23, 20325.

[21] *See, e.g.*, Notice of Proposed Rulemaking on the Implementation of Exemptions; U.S. Department of Homeland Security/Immigration and Customs Enforcement–018 Analytical Records System of Records https://www.govinfo.gov/content/pkg/FR-2021-03-22/pdf/2021-05643.pdf.

During DHS' June 30, 2021 public meeting on the RFI,[22] DHS officials demonstrated a lack of transparency into the mDL rulemaking process. Contrary to email communications, DHS did not offer substantive information or respond to comments made during the meeting.[23]

REGULATIONS MUST SAFEGUARD mDL DATA AND DRIVERS' PERSONAL INFORMATION BY FAVORING OFFLINE OVER ONLINE VERIFICATION

Under DHS' envisioned mDL model, a federal agency may retrieve mDL data from either an mDL holder's mobile device (offline data transfer) *or* directly from the DMV (online data transfer). Under the offline mode, mDL data would be transferred without a live connection to the internet. The offline mode would allow the verifying party to authenticate the mDL data on a driver's phone and confirm that the data was in fact issued by a particular DMV, without actually notifying the DMV of the driver's identity.[24] In the offline mode, the DMV is not involved in the actual transaction during which a mDL holder presents their license to a verifying party.

In contrast, the online mode "would require establishing a secure network connection between a Federal agency and a DMV" in which a "federal agency would receive mDL Data directly from a DMV instead of from a mobile device."[25] Under the online mode, a federal agent or officer attempt to verify a person's identity would alert the DMV when an mDL is being used and what data is being shared.

A direct and instantaneous online connection between a federal agency and DMV raises significant privacy concerns. DHS should not include the online data transfer mode in the design of its mDL standards and technologies. Rather, for the reasons stated below, mDL data transfers and identity verifications must be permitted only under the offline mode.

- REGULATIONS MUST ENSURE THAT mDL VERIFICATION DOES NOT CREATE A CENTRALIZED TRACKING SYSTEM OR CENTRAL DATABASE OF DRIVERS' PERSONAL INFORMATION

[22] Public Meeting and Extension of Comment Period on Request for Information: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Mobile Driver's Licenses, Office of Strategy, Policy and Plans, Department of Homeland Security (DHS), Docket No. DHS–2020–0028, 86 Fed. Reg. 31987 (June 16, 2021) ("DHS will hold a virtual public meeting on June 30, 2021, to answer questions regarding the RFI and to provide an additional forum for comments . . . ").

[23] E-mail from DHS Meeting Support (June 23, 2021, 09:10 PST) (on file with author).

[24] RFI at 20324 ("A Federal agency confirms the integrity of the mDL data by obtaining the DMV's public key to verify the digital signature."). Specifically, the offline mode uses the asymmetric cryptographic technique of the public key infrastructure (PKI). Under the PKI, when a DMV places a mDL on a driver's phone, it digitally signs that file using a *private* digital key, which is held and only held by the DMV. When a verifying party requests mDL information, they verify the authenticity of the mDL by using a corresponding *public key*, which confirms that the mDL was digitally signed with the DMV's private key (and therefore unaltered and original). See *Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom* (ACLU, 2021), https://www.aclu.org/sites/default/files/field_document/20210517-digitallicense.pdf (hereinafter ACLU Identity Crisis report).

[25] *Id.* at 20324. Under the online mode, a mDL holder's device would not actually hold any driver's license data. Rather, the mDL holder's mobile device would first pass a digital token to the verifying party, which would then use the token to retrieve mDL data, over the internet, from the DMV. See ACLU Identity Crisis report, *supra*, ft. 21.

No central federal government database of driver's license information currently exists. However, DHS' envisioned online data transfer mode under the RFI would make it much easier for DHS or another federal agency to create such a database. Online connections of this nature could make it possible to track frequency, time, and even location (via IP address) of an mDL every time it is used.[26] Beyond simultaneous tracking, it is unclear (and the RFI does not ask for views about) whether the verification processes provide an opportunity for other personal information to be stored, including whether the individual has a REAL ID-compliant license; whether information about where an individual has presented an mDL as identification becomes part of state DMV databases; and whether any of that information could be made available to commercial entities that sell driver's license information to ICE or CBP.

This type of centralized tracking system as well as the storage of driver's license information in a central government database would constitute a significant and profound invasion of privacy and would increase the risks of governmental abuse, including the potential for DMVs to collaborate with federal agencies to compile or monitor mDL usage data. This is a critical issue for non-citizens who fear that their driver's license information will be available for immigration enforcement purposes. The real possibility of information-sharing creates barriers for non-citizen drivers to obtain a license and impedes access to daily activities that require identification.

- <u>REGULATIONS MUST ENSURE THAT PERSONAL INFORMATION IS NOT SHARED FOR IMMIGRATION ENFORCEMENT PURPOSES</u>

For years, agencies such as DHS have relied on information in DMV databases for enforcement purposes.[27] Although it is not mentioned in the RFI, it is unclear whether the online connection would make non-REAL ID compliant licenses subject to verification. An online network connection between DHS and DMVs could increase the likelihood that DHS will use the connection for purposes other than those contemplated by the REAL ID Act (proving identity for official federal purposes).

The RFI focuses on verification of identity for REAL ID purposes, but any information system inevitably could be used for purposes that remain unexplored in and unconstrained by the RFI, such as immigration enforcement. For these reasons and the reasons stated above, DHS must not include the online mode in the design of its mDL standards and technologies.

- <u>REGULATIONS MUST EQUIP DRIVERS WITH THE ABILITY TO MAINTAIN MAXIMUM CONTROL OVER INFORMATION SHARED THROUGH A VERIFICATION SYSTEM</u>

The RFI does not seek views about protections against access to other information contained on an mDL. The REAL ID Modernization Act provides that "t]he presentation of digital information from a mobile or digital driver's license or identification card to an official of a Federal agency for an official purpose may not be construed to grant consent for such Federal agency to seize the electronic device on which the license or card is stored or to examine any other information contained on such device."[28] But the absence of presumed consent is not the same as a prohibition on a demand for the information

[26] ACLU Identity Crisis report, *supra*, ft. 21.
[27] *Untangling the Immigration Enforcement Web,* NILC (Sept. 2017), http://www.nilc.org/untangling-immigration-enforcement-web/.
[28] REAL ID Modernization Act § 1001(b)(3).

or intimidation to induce consent.[29] Nor would the Modernization Act's limitation regarding consent apply to non-federal agencies or commercial entities.

Instead of considering affirmative protections, the RFI simply asserts that mDL holders will have the ability "to control what data fields are released to a Federal agency"[30] and release of information will be limited to "the data necessary for the purpose the transaction (e.g., identity verification), while blocking the [federal] Agency's ability to view any other mDL data (e.g., organ donor status)."[31] However, this overstates the amount of control mDL holders will have over their mDL data and other personal information.

First, mDL holders will have only the degree of control over their data that their state DMV allows to be built into the mDL app or software.[32] For example, one mDL app developer might collapse multiple biographic data points like height, weight, hair color, and eye color into a single data field labeled as "physical biographic data" while another developer could separate each of those data points into discrete fields. The former approach would allow for far less user control over data than the latter.

Second, in order for mDL holders to have meaningful control over their data, they must know how their data is being shared throughout the mDL machinery and when this happens.[33] Control therefore should include a clear and accessible accounting of what mDL data is being shared and when. The RFI fails to include considerations for auditing functions to be built into mDL apps and/or software that would enable mDL holders to easily access and view any data that has been released, when, and to whom.

Finally, real-world dynamics of power, control, and coercion that many government agencies and their officers embody will affect mDL holders' ability to exercise control over their data. These dynamics are particularly significant for immigrants and people of color, who may feel fearful, distrustful, and disempowered when engaging with government actors, especially police and immigration authorities.[34] A demand by an ICE agent or TSA officer to see one's license, in practical terms, feels like a mandate that must be obeyed, rather than a situation where a mDL holder would feel empowered to choose which data fields to release.

- <u>REGULATIONS MUST LIMIT OTHER ONLINE CONNECTIONS OUTSIDE OF THE VERIFICATION CONTEXT</u>

Beyond the identification verification context, DHS envisions regular connections between a driver's mobile device and the DMV for purposes ranging from *provisioning* a license (i.e. "the process where a DMV would authorize the secure storage of mDL Data onto a mobile device, enable the device to receive the data from a DMV, and transmit the data to the device")[35] to updating *data freshness* (i.e.

[29] *See generally* Roseanna Sommers & Vanessa K. Bohns, *The Voluntariness of Voluntary Consent*, 128 Yale L.J. 1962 (2019), https://www.yalelawjournal.org/pdf/SommersBohns_w4cmjkwe.pdf (discussing the limits of the voluntariness of consent inquiry as consistently underestimating the pressure to comply).
[30] RFI at 20321, n.7.
[31] *Id.* at 20324.
[32] ACLU Identity Crisis report, *supra*, ft. 21.
[33] *Id.*
[34] See e.g., David Becerra et al., *Policing Immigrants: Fear of Deportations and Perceptions of Law Enforcement and Criminal Justice*, https://repository.asu.edu/items/51880; Sommers & Bohns, *supra* note 29, at 1967-68.
[35] RFI at 20323.

"the synchronization of mDL data stored on a mobile device to data in a DMV's database, within a specified time period").[36] Although the RFI suggests the need for more frequent data freshness synchronizations—and consequently and presumably, more frequent online connections between a driver's device and the DMV—as stated above, DHS must design its mDL system to operate offline only. A limited exception could allow the mDL holder to set up a remote appointment, during which an online connection is established *and* expires, to complete a specific and discrete task such as provisioning, syncing data, or license renewal.

REGULATIONS MUST PROTECT AGAINST DISCRIMINATION IN THE USE OF PHYSICAL DRIVER'S LICENSES, PREVENT DISPARITIES IN ACCESS, AND COUNTERACT RACIALIZED POLICING

DHS' pressure on states to create mDLs through a national mDL standard will increase the likelihood that mDLs will become the default, or more problematically, mandatory. AAMVA explains that the "generally held position by subject matter experts [is] 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."[37] The RFI's ask for "quantifiable cost-savings from being able to use a REAL ID-compliant mDL rather than a REAL ID-compliant physical driver's license or identification card" confirms that DHS is contemplating such a future.[38]

This push for mDLs will exacerbate the digital divide between privileged and marginalized communities. Smartphone ownership, though increasingly common, varies most notably across age and income: nearly 40% of people over the age of 65 do not own a smartphone,[39] nor do three-in-ten adults with a household income below $30,000 a year.[40] In addition, while smartphone ownership is necessary under the mDL schema, it is not sufficient. Stable and affordable internet connectivity may be required, depending on the design of the particular mDL (e.g., to facilitate online data transfers and online verifications). According to the Pew Research Center, many lower-income, Black, and Hispanic smartphone owners encounter constraints such as data caps and other barriers to long-term access, including canceled or cut off services, twice as often as White users.[41] As of February 2021, 80% of white Americans are estimated to have fixed broadband service, compared to 71% of Black Americans and 65% of Hispanic Americans. Lower-income households also experience barriers to high-speed internet at disproportionate rates. The prevalent disparities in smartphone and internet access are additional unaccounted-for considerations that militate in favor of an offline-only mDL standard.

Consequently, people who lack the technology required to support an mDL could have less access to any projected or actual benefits that are or become associated with mDLs, such as shorter wait times for

---

[36] *Id.* at 20322.
[37] *Mobile Driver License (mDL) Frequently Asked Questions for Law Enforcement*, AAMVA, at 1 (Question 4), https://www.aamva.org/mDLFAQs/.
[38] RFI at 20321.
[39] *See Mobile Fact Sheet*, Pew Research Center (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/.
[40] *See Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption*, Pew Research Center (May 7, 2019), https://www.pewresearch.org/fact-tank/2019/05/07/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/.
[41] *Smartphones Help Blacks, Hispanics Bridge Some – but not all – Digital Gaps with Whites*, Pew Research Center (Aug. 20, 2019), https://www.pewresearch.org/fact-tank/2019/08/20/smartphones-help-blacks-hispanics-bridge-some-but-not-all-digital-gaps-with-whites/.

processing DMV applications and renewals; expedited identification checks at airports or federal facilities; or purported security enhancements of driver data. The rise of a ubiquitous mDL standard that is acceptable for federal purposes could inadvertently create a reflexive presumption that a physical driver's license is not compliant with the REAL-ID Act's requirements. This could lead to further disenfranchisement of drivers who lack the technology and hardware to support mDLs and therefore rely on a physical driver's license.

Many immigrants have expressed concern that driver's licenses that are not REAL ID compliant ("non-REAL ID licenses") would be used as evidence of their immigration status by rogue police officers or federal immigration agents.[42] This was the case in Vermont where DMV employees, who were fixated on the perceived immigration status of non-REAL ID license holders, collaborated with federal immigration agents to share information and target Latinx drivers with non-REAL ID licenses.[43] Moreover, immigrants and people of color—especially Black immigrants — already experience more risk and vulnerability when they are stopped by or encounter the police.[44] Across the nation, local police departments funnel thousands of individuals into the immigration detention and deportation system every year through a web of largely opaque mechanisms that link federal immigration enforcement and local police operations.[45] Police officers are more likely to stop Black and Latinx individuals; and when stopped, Black and Latinx individuals are more than twice as likely to experience the threat or actual use of force.[46] During field police interactions, in which critical decisions are made in seconds, with the backdrop of implicit bias and police misconduct, the addition of cellphones can be lethal.[47] The RFI and DHS' envisioned mDL model does not account for these real harms.

It is therefore essential that upcoming rulemaking on mDLs include the protection of physical driver's licenses and the implementation of an offline-only mode to help address disparities in access and consequences linked to biased immigration enforcement and local policing.

CONCLUSION

[42] *See How California Driver's License Records Are Shared with the Department of Homeland Security*, NILC (Dec. 2018), https://www.nilc.org/issues/immigration-enforcement/how-calif-dl-records-shared-with-dhs/.
[43] *See* Ellie French, *Migrant Justice Settles with DMV to Halt Information Sharing with ICE*, VT Digger (Jan. 15, 2020), https://vtdigger.org/2020/01/15/migrant-justice-settles-with-dmv-to-halt-information-sharing-with-ice/.
[44] *See* NYU Immigrant Rts. Clinic & Black Alliance for Just Immigration, *The State of Black Immigrants, Part II: Black Immigrants in the Mass Criminalization System* 20, https://www.immigrationresearch.org/system/files/sobi-fullreport-jan22.pdf.
[45] *See* NILC, *How ICE Uses Local Criminal Justice Systems to Funnel People Into the Detention and Deportation System* (Mar. 2014), https://www.nilc.org/issues/immigration-enforcement/localjusticeandice/; Immigrant Legal Resource Center, *National Map of Local Entanglement with ICE* (Nov. 13, 2019), https://www.ilrc.org/local-enforcement-map.
[46] *See, e.g.*, Elizabeth Davis et al., *Contacts Between Police and the Public, 2015* 8, 16-17 (Oct. 2018), https://www.bjs.gov/content/pub/pdf/cpp15.pdf.
[47] In March 2020, following a traffic stop for a minor violation, Donnie Saunders, at 47 years old, was killed by a police officer who mistook Saunders' cellphone for a weapon. *See* Trone Down, *The Deadly Consequences of Carrying a Cell Phone While Black,* VICE (Mar. 4, 2021), https://www.vice.com/en/article/5dp87a/cops-keep-shooting-black-men-with-cell-phones-assuming-theyre-guns. Both tragic and tragically commonplace, Flint Farmer (29 years old – killed June 2011), Stephon Clarke (22 years old – killed March 2018), and Andre Hill (47 years old – killed December 2020) have also all been killed by police for holding a cellphone. *Id.*

DHS must not abrogate the right of states to regulate and administer their driver's license programs or discriminate against drivers who wish to maintain a physical driver's license. As the federalization of state driver's licenses proceeds, DHS must consider and account for privacy, physical harms, and potential discriminatory impact of its mDL schema.

Sincerely,

National Immigration Law Center
Arkansas United
CASA
Florida Policy Institute
New Jersey Alliance for Immigrant Justice
Colorado Immigrant Rights Coalition
Just Futures Law
Legal Aid Justice Center
NAKASEC VA
CAIR Georgia
Women Watch Afrika, Inc.
Massachusetts Immigrant and Refugee Advocacy Coalition
Asian American's Advancing Justice - Atlanta
Dignidad Inmigrante en Athens