NYCLU
ACLU of New York

SURVEILLANCE
RESISTANCE LAB

January 8, 2024

Dear Commissioner Mark Schroeder,

As the New York Civil Liberties Union and the Surveillance Resistance Lab, we write to raise urgent concerns regarding the New York State Department of Motor Vehicles' plan to implement a pilot program for mobile driver's licenses (mDLs) in the near future. Any mDL program drastically changes what it means for New Yorkers to have a state-issued ID and exposes them to numerous risks inherent to mDL and digital identification systems. We demand that this important policy development be properly put before New Yorkers for investigation, public debate, and a full balancing of benefits and costs of a mDL program, and to implement comprehensive protections to further people's privacy and equity.

The DMV referenced its plans to introduce mDLs in New York State at the 2023 legislative budget hearings, without a clear timeline, any public debate, or engagement with New Yorkers, and has entered into two contracts with a vendor, IDEMIA, for that purpose. The DMV's minimal disclosures have not acknowledged the potential risks associated with mDL's architecture or the role of DHS behind mDL infrastructure.[1] Without public debate or discernable legal and technical safeguards, the introduction of mDLs—a largely untested technology and unprecedented data collection program in New York State—has the potential to undermine democratic systems, infringe on personal privacy, compromise equity and civil liberties, and exacerbate mistrust among communities wary of using DMV services.

We ask that the DMV immediately pause its plans for an mDL pilot. Mobile driver's licenses can cause significant harm to residents. The perceived need for any program should be debated in public forums and include plans for technical and legal safeguards, including comprehensive privacy protections. We have included an attached list of policy recommendations in Appendix A of this letter, as well as additional resources on the risks of mDLs in Appendix B.

Digitizing any identification system requires particular scrutiny and immense care, based on the harms we have seen across the country and beyond. Digital identification systems generate a massive dataset of peoples' information, behaviors, whereabouts, and movements that physical licenses do not. In New York City, 65 community groups and advocacy organizations opposed a corporate plan to digitize the City's municipal ID card by adding a smart chip, which would have undermined the program's critical data-sharing protections.[2] In South Korea, the digitization of the national ID system led to 80 percent of the population having their personal information, including SSN equivalent, stolen in data breaches.[3] In

[1] "Comments on the U.S. Department of Homeland Security, Minimum Standards for Driver's Licenses Acceptable by Federal Agencies for Official Purposes; Waiver for Mobile Driver's Licenses, Docket No. TSA–2023–0002," National Immigration Law Center and Surveillance Resistance Lab, October 16, 2023, https://surveillanceresistancelab.org/wp-content/uploads/NILC-SRL-TSA-mDL-NPRM-Comment-October-2023.pdf.

[2] "8 Reasons Why NYC Council Should Reject IDNYC 'Smart Chip' Plan and Preserve IDNYC as a Secure Identification Program," Immigrant Defense Project, Make the Road New York, New Economy Project, New York Civil Liberties Union, and New York Immigration Coalition, December 9, 2019, https://www.immigrantdefenseproject.org/wp-content/uploads/12-9-19-Protect-IDNYC-Memo-from-Groups.pdf.

[3] "South Korean ID system to be rebuilt from scratch," BBC News, October 14, 2014, https://www.bbc.com/news/technology-29617196.

2021, the Irish government had to roll back its implementation of the Public Services Card[4]—a digital ID program that was initially voluntary but then became mandatory for all social welfare benefits recipients—after a two-year investigation exposed its collection of unlawful data[5] and a 2020 UN evaluation found that the program discriminated against marginalized groups.[6]

Key Concerns: If not implemented with the highest level of care, mDLs can be disastrous for privacy, equity, and democracy. While the concerns are many, we highlight here four risks inherent to the infrastructure and architecture of mDLs, focusing on those which are particularly relevant to the New York State mDL pilot program:

1. **Impact on the Green Light Law:** Concerns about tracking and law enforcement access are particularly salient for immigrant drivers who became eligible for driver's licenses following the passage of the state's Green Light law. Communities across New York State fought for years to expand driver's license access for all residents, improving traffic safety and access to employment, education, and healthcare, while simultaneously limiting local entanglement in federal immigration policing. People who have acquired driver's licenses in this time, including those vulnerable to government surveillance and immigration enforcement, did not sign up for a mobile tracking program. While the program is currently voluntary, we have repeatedly seen digital identification systems become privileged or mandatory within the US and beyond, as in Ireland's public benefits system.

2. **Centralized Tracking and Data Sharing:** Every time a person presents their mDL to access a resource or prove their identity, the inherent architecture of mDL systems allows the DMV and/or a verifying party[7] to potentially record and track this information. This can create additional centralized repositories of information that track when and how a person's ID is used, creating a digital record of a person's travel itinerary, alcohol and other purchases, and medical visits, among other things. The use of mDLs could also drastically increase mandatory identity verification, especially online, creating unprecedented state and corporate access to the public's online activity.

[4] Jack Horgan-Jones, "Irish State told to delete 'unlawful' data on 3.2m citizens," *The Irish Times,* August 16, 2019, https://www.irishtimes.com/news/ireland/irish-news/irish-state-told-to-delete-unlawful-data-on-3-2m-citizens-1.3987606; Frank Hersey, "Irish biometric public services access card not to be mandatory," Biometric Update, December 20, 201, www.biometricupdate.com/202112/irish-biometric-public-services-access-card-not-to-be-mandatory.

[5] Horgan-Jones, "Irish State told to delete 'unlawful' data on 3.2m citizens."

[6] "Ireland's Public Services Card discriminates against the marginalised, warns UN rights expert," United Nations Office of the High Commissioner of Human Rights, April 21, 2010, https://www.ohchr.org/en/press-releases/2020/04/irelands-public-services-card-discriminates-against-marginalised-warns-un?LangID=E&NewsID=25811.

[7] A "verifying party" or "verifier" refers to the official, person, or entity who checks the mDL and verifies information (name, age, address, etc.), such as a police officer, TSA agent, or liquor store clerk. The "issuer," typically the state Department of Motor Vehicles or a vendor, issues and stores mDL information in a centralized location, similar to data on physical licenses. The "holder" refers to the individual license holder. "Mobile Driver's Licenses and the Costs to Privacy, Equity, and Security," Surveillance Resistance Lab, December 2023, https://surveillanceresistancelab.org/wp-content/uploads/Mobile-Drivers-Licenses-and-the-Costs-to-Privacy-Safety-Security-2023.pdf.

Depending on their configuration, an mDL could allow the DMV—as well as third-party companies that verify user's mDLs and local, state, and federal law enforcement agencies—to access a history of a license holder's location and behavior information, and track them over time. Depending on the software used, a license holder's device may also create a similar tracking log as well as metadata about the person's device and network access. Without protection and regulation, there would then be no restriction on the use, processing, sharing, or selling of mDL holder's information, transactions, or other data to third parties or for other purposes.

3. **Law Enforcement Access to Mobile Devices:** The New York State DMV implementation of mDLs raises concerns about how they will be physically shared with and viewed by law enforcement. During routine encounters with police, an mDL holder may be pressured into handing over their smartphone in a way that police later argue is consent for purposes of a seizure. mDLs also introduce a means for police to forcibly interrupt someone recording a police interaction. This dynamic is a particular concern for communities of color and immigrant communities, who already experience escalations of violence and other abuses of police authority.

4. **Threats to Equity and a Right to Inclusion:** In the longer term, mDLs have deep implications for social inequity. Even if mDLs are voluntary and do not replace traditional plastic IDs at the outset, it is not difficult to imagine a future where mDLs become the norm, or are eventually required or highly privileged (and where the future infrastructure for physical identities are underserviced), as has happened with other digital identification systems.[8] Some vendors might choose to exclusively accept mDLs for proof of identity or access to services, in the same way that some businesses have stopped accepting cash as payment. This can lead to marginalization of people who do not own smartphones—who tend to be lower-income, older, living in rural communities, or have a high school education or less[9]—as well as people who may instead use older smartphones, poorly-functioning devices, or smartphones that lack the requisite hardware features, latest software updates, and necessary connectivity capabilities. mDLs could pave the way for tiered services and longer wait times for physical license holders. It is not too early to begin thinking about these possible consequences and how they could be avoided.

As the DMV has thus far disclosed very little information about the planned mDL pilot program, it is impossible to know whether these concerns are being addressed or even considered. Advocates, including the undersigned, have outlined the many harms of mDLs and digital identification systems, and noted that any mitigating recommendations are not a substitute for informed and deliberate public debate. We remain deeply concerned about the forthcoming rollout of the mDL pilot in New York State and related harm to New Yorkers and urgently ask you to pause these plans. We look forward to hearing from you.

Sincerely,
New York Civil Liberties Union
Surveillance Resistance Lab

[8] "Ireland's Public Services Card discriminates against the marginalized, warns UN rights expert," United Nations Office of the High Commissioner of Human Rights.

[9] "Mobile Fact Sheet," Pew Research Center, April 7, 2021, https://www.pewresearch.org/internet/factsheet/mobile.

NYCLU
ACLU of New York

SURVEILLANCE RESISTANCE LAB

Appendix A: Mobile Driver’s Licenses Policy Recommendations

New York Civil Liberties Union and the Surveillance Resistance Lab

In December 2022, the New York State Department of Motor Vehicles (DMV) entered into a three-year $1,750,000 contract with IDEMIA to create a Mobile Driver’s Licenses (mDL) system.[10] However, the DMV has not publicly provided any information or details about the program and New Yorkers, nor their representatives, have been given the opportunity to weigh in. This program will have far-reaching ramifications for New Yorkers across the state—undermining democracy, entrenching injustice, eroding privacy rights, and threatening our civil rights and liberties.[11]

This important policy development deserves at minimum to be properly put before New Yorkers for investigation, open public debate, and a full balancing of benefits and costs of a mDL program. The DMV should not lock New Yorkers into costly contracts with proprietary technology vendors that often limit public engagement, oversight, and accountability—as experienced in the past with one of NYC’s digital procurement systems,[12] New York State’s unemployment benefits system,[13] NYPD surveillance systems,[14] and state welfare systems across the United States.[15]

The New York Civil Liberties Union (NYCLU) and the Surveillance Resistance Lab strongly urge New York State not to move forward with any mDL pilot because the following key principles have not been adhered to:

- *Democratic Processes*. Impacted people need to have a seat at the table from the start. Communities most affected, including under-resourced communities, marginalized communities including undocumented New Yorkers and those receiving public assistance must be represented and meaningfully involved. Consult with experts in digital identification, cryptography and cyber-security, open-source technology, immigrant rights, civil rights, and accessibility.

[10] See, e.g., Contract C001009, IDEMIA IDENTITY & SECURITY USA LLC, $1,750,000.00, Open Book New York - Office of the State Comptroller, https://wwe2.osc.state.ny.us/transparency/contracts/contracttransactions.cfm?Contract=0000000000000000000109566.

[11] “Mobile Driver’s Licenses and the Costs to Privacy, Equity, and Security,” Surveillance Resistance Lab.

[12] Anna Sanders, “City tech agency was overcharged for $47M procurement system, watchdog says,” *New York Daily News*, June 2, 2019, https://www.nydailynews.com/2019/06/02/city-tech-agency-was-overcharged-for-47m-procurement-system-watchdog-says/.

[13] Rebecca Heilweill, “AI Has Locked New Yorkers Out of Unemployment Benefits,” *New York Focus,* June 16, 2023, https://nysfocus.com/2023/06/16/id-me-facial-recognition-unemployment-new-york;
“NYCLU, ACLU Sue New York State Department of Labor for Withholding Records on Automated Identity-Verification Tools,” New York Civil Liberties Union,” June 16, 2023, https://www.nyclu.org/en/press-releases/nyclu-aclu-sue-new-york-state-department-labor-withholding-records-automated-identity.

[14] Emily Hockett and Michael Price, “Palantir Contract Dispute Exposes NYPD’s Lack of Transparency,” The Brennan Center, July 20, 2017, https://www.brennancenter.org/our-work/analysis-opinion/palantir-contract-dispute-exposes-nypds-lack-transparency.

[15] Miriam Jones, “Nobody Wins in Indiana vs. IBM Lawsuit, Judge Says,” *GovTech*, July 19, 2019, https://www.govtech.com/health/nobody-wins-in-indiana-vs-ibm-lawsuit-judge-says.html; Eva Constantarus et. al., “Inside the Suspicion Machine,” *The Intercept,* March 6, 2023, https://www.wired.com/story/welfare-state-algorithms/.

- *Equitable Tech*. Ensure technologies serve people and communities in need, not companies' shareholders.
- *Ban Discriminatory Technologies*. Enact bans on technologies that show discriminatory impact or threaten people's fundamental rights. Rigorous research has documented the risks of biometric technologies, interoperable data sharing systems, and digital ID systems, all of which are fundamental to the design of any mDL program and thus must be approached with extreme caution.[16]

Minimum mDL Policies:
We have heard from multiple lobbyists and vendors about their approaches to mDLs that promote privacy. These fall far short and do not consider the unique and inherent dangers of mDL and digital ID programs. Any digital identification program, including but not limited to mDLs, must be entirely voluntary, require full opt-in consent from participants, offer participants granular control over their data, eliminate risks of data capture and sharing, and ensure the strongest protections for our data, privacy, and civil liberties – guaranteed both by legal and technical safeguards. Transparent and auditable open standards are the only meaningful path to ensure trust and security.

We outline below the minimum policies that would be needed to mitigate—but not eliminate—harms of mDL programs on New York residents. This alone is not enough; public debate is urgently needed to more fully understand these documented risks and full balancing of costs and benefits of any mDL program.

Program Foundation:

- *Voluntary Programs and Opt-In Consent*. Legislation and/or regulation should explicitly forbid any party, including the mDL issuer and verifiers, from requiring an mDL for any purpose or transaction. Any digital ID program must be fully voluntary and require opt-in consent. The use of digital IDs should never become mandatory, required, or incentivized to access certain services, and must never provide additional benefits or preferential treatment.
- *No Law Enforcement Access or Other Verifier Access to Phones*. Systems should be designed such that ID owners never need to hand over their device to a verifier. Legislation should explicitly forbid all parties from asking if they can physically take possession of or search someone's phone, when the holder presents their mDL.
- *No Preferential Treatment.* Using an mDL should not allow for preferential treatment and efforts should be made to ensure utilizing a physical driver's license does not result in second-class services or longer wait times. This should be formally institutionalized in law and/or regulation, to prevent future changes.
- *Restrictions on ID Demands*. The system should not create additional ID checks or identity verification where none was needed before. One approach to this is to require registration of verifying parties (including both government agencies and private companies) with the DMV or state, clearly outlining and limiting what uses of verification are allowed, ensuring that the mDL holder receives clear and complete information about the verifier's request before every transaction, and explicit

[16] Patrick Grother et. al., "National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (NISTIR 8280)," December 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf; "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," National Institute of Standards and Technology, December 19, 2019, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software .

penalties or liabilities for verifiers that violate these policies—including those that ask for more information than is warranted.

- *Open Source and Open Standards*. Require and adopt open-source technologies for all aspects of any digital ID program, including the mDL itself and mobile wallets used to access the mDL, as well as open standards. Ideally, this would include the creation or use of an open-source mobile wallet, rather than a proprietary, vendor-run option. Open-source technologies and open standards are essential in order to avoid proprietary solutions, vendor lock-in, and long-term dependencies. Adopt initiatives like "Public Money, Public Code,"[17] which requires publicly financed software developed for public use to share its source code in such a way that it can be used without restriction, modified, and redistributed with or without modifications at no cost.[18] Standard, interoperable protocols are also more secure and better tested.

Data Protection:

- *Granular Control Over Data Released*. The system should be designed to limit the creation of records of where and when an ID was presented, regardless of the type of use, and especially records of unique identifiers that can be associated with the holder. In addition, the system must be designed to give people comprehensive controls over which points of their data are released to verifiers and provide holders with the opportunity to locally retain specific records, so they can look back and see which verifying law enforcement officer or vendor accessed their ID, including when and what information. In accordance with the strictest data minimization principles, data disclosed to verifiers should be broad categories wherever possible (e.g., over 21; over 65; NYC resident), rather than specifics (e.g., the person's exact date of birth, the person's exact address).
- *Unlinkable Presentations.* In addition, when non-identifiable data is produced by the mDL system or interactions about the ID holder, the scheme should prevent any specific transaction from being linked to previous and future verifications involving the same ID.
- *No Sharing, Sale, or Exploitation of Data.* No data should be shared with any party besides the requester. This includes sharing and sale of data by the issuing party (DMV), contracted vendors, requester/verifier, and any third parties. All sharing of data with local, state, federal, and other law enforcement agencies should also be prohibited without a warrant. This includes aggregate and de-identified data, some types of which can easily be disaggregated and de-anonymized.
- *Data Deletion.* All data should be deleted once its purpose is fulfilled, meaning that any data collected during a transaction or interaction must be deleted immediately after the transaction or interaction is complete. Data should also be able to be immediately and easily deleted at the request of the data subject.
- *Encryption and Security Standards*. The system must be built with the strongest possible encryption and security standards. This should include a regular process of auditing and updating standards, supported by an annual budget to ensure this occurs.

Review and Accountability:

- *Auditing and Reviewing Mechanisms*. All systems should be subject to independent, transparent, and regular review to ensure – and to assure the public – that such technologies are being used

[17] "Public Money, Public Code," Free Software Foundation Europe, accessed December 15, 2023, https://publiccode.eu/en/.

[18] "What is Free Software?" Free Software Foundation Europe, accessed December 15, 2023, https://fsfe.org/freesoftware/.

appropriately, requirements are being followed, and implementers are treating personal information with the care required.

- *Accountability Mechanism:* Transparency and auditing alone do not ensure accountability. Enforcement mechanisms must be in place to identify and hold verifiers and issuers accountable, and more broadly protect the rights of mDL holders. This includes ensuring that users have access to the courts and are not bound by the state to an arbitration clause or government contractor defenses.

Without the necessary protections, mDLs will supercharge surveillance and create or reinforce barriers and harms for people. Any steps towards a digital identity system must center equity and privacy protections from the very beginning – and for this it matters who sits at the table and what values undergird the endeavor.

Appendix B: Additional Resources

Here are additional resources on the risks of mobile driver's license programs, digital ID systems, and state driver's license information sharing.

Overall risks of mDL programs:

- Mobile Driver's Licenses and the Costs to Privacy, Safety, and Security, Surveillance Resistance Lab and the National Immigration Law Center, 2023
- Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom, ACLU, 2021

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
- *American Dragnet Data-Driven Deportation in the 21st Century*, Georgetown Center on Privacy and Technology, 2022
- *Immigration Enforcement–related Information Sharing and Privacy Protection*, National Immigration Law Center, 2022

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

- 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," Surveillance Resistance Lab and the National Immigration Law Center, 2023
- *The REAL ID Act: Questions and Answers*, National Immigration Law Center, 2021
- 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", National Immigration Law Center, 2021