ACLU Pennsylvania

MEMORANDUM

TO: The Pennsylvania House Transportation Committee

FROM: Elizabeth Randol, Legislative Director, ACLU of Pennsylvania

DATE: June 23, 2024

RE: OPPOSITION TO HB 2428 P.N. 3342 (NEILSON)

Bill summary: HB 2428 (PN 3342) would amend Title 75 to allow the Department of Transportation to issue electronic driver's licenses and identification cards. It would establish a verification system to confirm the authenticity and validity of these electronic credentials and set requirements for carrying and exhibiting physical and electronic driver's licenses. It would also provide certain protections and limitations related to the use of electronic devices to display these credentials.

On behalf of over 100,000 members and supporters of the ACLU of Pennsylvania, I respectfully urge you to oppose House Bill 2428.

The ACLU does not object to the concept or creation of electronic driver's licenses (or mobile driver's licenses—"mDLs"). There are many benefits to an electronically available license or ID. However, as with any kind of new technology, privacy concerns are paramount and extreme caution and diligence should accompany any new or expanded ability for the government to identify and/or track you—especially when the new technology anticipates interaction with law enforcement.

The ACLU-PA opposes HB 2428 less for what the bill does, but what it ***fails to include or anticipate***. The ACLU's 2021 report, Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom, outlines 7 potential privacy threats that should be addressed by any legislation enabling the creation of mDLs. Two of the most critical threats are highlighted below.

HB 2428 needs stronger limitations on police searches of cell phones.

HB 2428: Under §1511(c), HB 2428 includes some important guardrails against police access to the contents of a person's phone when presenting their mDL to law enforcement for identification purposes. This section would (1) not require a person to surrender their device to police when asked for identification; (2) only permit police to view a person's mDL profile (and no other data); and (3) if police "inadvertently" review data beyond the mDL profile, it would prohibit that information from being used in any civil or criminal trial.

- **Concern:** While this language will protect against some abuse, it should be much stronger. In 2018, the U.S. Supreme Court ruled, in no uncertain terms, that police must obtain a warrant for smartphone searches (see the ACLU's case, *Carpenter v. United States*). And yet, 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. 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.

- **Recommendation: Police must be expressly prohibited by statute from seeking consent for phone searches during mDL verifications.**

HB 2428 must prohibit centralized ID tracking.

HB 2428: §1510(p) would require the DMV to (1) create a verification system that would (2) allow a user to consent to a verification request by any verifier (e.g., a government agency or private entity) via the DMV's verification system and (3) allow the DMV, through an agreement, to permit other government agencies to use the DMV's verification system to verify its own users. In other words, the DMV will become the central repository and hub for all mDL verifications. *Critically, HB 2428 includes no requirement that the verification system be unlinkable*.

- **Concern:** Under HB 2428, every time you present your ID to any verifier, that data is shared with and dependent upon the DMV's verification system. When someone visually inspects your physical license, no record of that inspection is automatically generated, retained, or shared with the DMV. But with a shift from physical to digital identities, such tracking becomes possible. For mDLs, 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, doctor's office, and airport that you visit; every convenience store beer purchase, equipment rental, or hotel check-in; any applications for social services; purchase of legal marijuana, and any other circumstance in which you may be asked to show an ID. In addition, any local police department that has a memorandum of understanding with the DMV (most of them do) would give each of those departments access to everything the DMV can see.
- **Recommendation: "Unlinkable presentations" are an absolute requirement for any digital identity scheme.** In other words, HB 2428 should explicitly prohibit the DMV (or any of their agents or contractors) from collecting or tracking where or to whom a user presents their ID. This would also prevent verifiers from colluding with other verifiers (or with the DMV) to compile records of ID presentations associated with individual users.

If the bill were to include these, and other, vital privacy safeguards, HB 2428 could offer all the benefits of an electronic license system without leaving Pennsylvanians vulnerable to warrantless police searches and a powerful, centralized government surveillance and tracking system.

For these reasons, we urge you to oppose House Bill 2428.