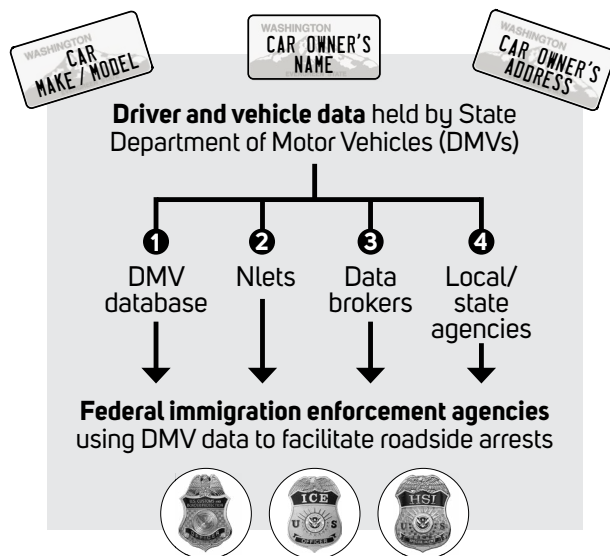


Summary

Across the country, traffic stops have become an increasingly frequent, visible, and violent means of immigration enforcement by ICE/CBP/DHS. In many cases, these arrests are directly or indirectly facilitated by state Departments of Motor Vehicles (DMV), through the sharing of driver and vehicle data in a process known as the DMV-to-DHS pipeline. The report, “Stopping the DMV-to-DHS Pipeline,” reviews those pathways and examines the experiences of four states—Maryland, Minnesota, New York, and Washington—all of whom have passed state laws to curtail the DMV-to-DHS pipeline, and yet, all of whom, to different extents, continue to experience vehicular immigration arrests.

What is the DMV-to-DHS pipeline?



The DMV-to-DHS pipeline shows the four main pathways through which state-held driver and vehicle data is shared with federal immigration agencies:

DMV database: Many states allow external parties direct access to their DMV data. In some states, ICE and CBP are among those with direct access.

Nlets: ICE/CBP uses Nlets, a national law enforcement data-sharing system that DMVs share data with, to identify people by querying the license plates of cars they see and retrieving information such as name and address of the car's owner.

Data brokers: Many states generate revenue by selling DMV data to data brokers, who in turn sell the data to others, including ICE/CBP.

Local/state agencies: State or local law enforcement or agencies with access to DMV data could search the data on ICE/CBP's behalf.

Driver and vehicle data protection laws

In states that have passed laws allowing noncitizens to obtain drivers' licenses, DMVs collect and hold data that can be used to identify and locate noncitizen drivers. Many of those states have made commitments to secure immigrants' DMV data from use for immigration enforcement purposes, however none have managed to shut off the DMV-to-DHS data pipeline completely.

Are the laws working?

This report compares the efforts of four states—Maryland, Minnesota, New York, and Washington—and examines whether their laws are upheld in practice by analyzing records that show how information flows behind the scenes. Maryland, Minnesota, and New York all require federal immigration agents to present a warrant when seeking to access DMV data—though in Minnesota's case, this only applies to driver, not vehicle data, of those with non-REAL ID licenses. Research suggests that Maryland is struggling to implement the warrant requirement in its new law; in Minnesota and New York, data suggest their laws are being effectively upheld, though ICE traffic stops continue. While Washington's “sanctuary” law forbids state agencies from sharing data with ICE/CBP for purposes of civil immigration enforcement, data shows that actions taken to curtail federal agents' access to DMV data have been ineffective.



As of October 13, 2026, UWCHR researchers have **confirmed 356 cases** in which data held by WA's Dept. of Licensing was accessed by federal agents prior to immigration arrests.

REPORT RECOMMENDATIONS

As the experiences of Maryland, Minnesota, New York, and Washington clearly show, the federal government's immigration enforcement agencies have taken advantage of numerous avenues to access DMV data across the nation—and when one pathway closes, they tend to exploit another. Any attempt to bring such practices into compliance with laws passed in these states therefore needs to tackle the problem holistically, rather than piecemeal.

UWCHR's research suggests the following best practices:

All four pathways

There are four main ways that federal immigration agencies can access DMV data: by directly accessing the DMV databases; by using Nlets to send messages to state DMVs and receive information back; by using private data brokers; by asking collaborating law enforcement agents to look up information for them and share it. Efforts to curtail the use of one pathway will only likely result in the use of another, until a comprehensive approach is taken that tackles all the possible pathways for DMV-to-DHS data sharing. Of the states examined in the report, both Maryland and New York have come closest to achieving this objective by passing the most comprehensive legislation to address the problem.

Enforcement

To be effective, prohibitions on impermissible data use should include serious enforcement mechanisms, including restitution for victims of misuse, as is already contemplated for victims of other types of data breaches, and an explicit avenue for impacted individuals and the organizations that serve them to obtain court injunctions ordering a halt to prohibited behavior when it does occur. Between the four states studied, UWCHR found evidence of state DMVs sharing data via Nlets in ways that failed to comply with state law, yet it appears no one in those states has been sanctioned for their role in such activity, nor have courts intervened to stop it—and more importantly, that those harmed have not seen that harm redressed. None of the state laws examined incorporate a private right of action, however New York's Green Light law specifies that failure to comply constitutes a Class E felony.

Transparency

All four of the states examined in the report allow some degree of transparency into the DMV-to-DHS data pipeline by permitting public records requests to examine queries of DMV data. Of the states in question, Minnesota offers the greatest guarantees of this transparency by stipulating in law that all queries of DMV databases must be recorded and considered public record and also specifically granting data subjects (individuals about whom the government record exists) to obtain copies of government records about them. Washington, in practice, upholds a similar principle.

Many states, by contrast, provide little to no transparency into the workings of their Nlets agencies, arguing that as law enforcement records, they should be exempt from public disclosure. For example, California, Illinois, Maine, New Jersey, and Virginia applied some version of a blanket exemption to records of law enforcement queries on DMV databases; requests for information about Nlets queries filed in Oregon were rejected by state authorities on somewhat different grounds, but still rejected. These policies are deeply problematic, for they make it extremely difficult for residents of these states to ensure that laws protecting the privacy of their driver and vehicle information are upheld in practice.

Any serious attempt at curtailing the DMV-to-DHS data pipeline requires not only strongly written laws, but mechanisms whereby researchers can examine the effectiveness of such laws.