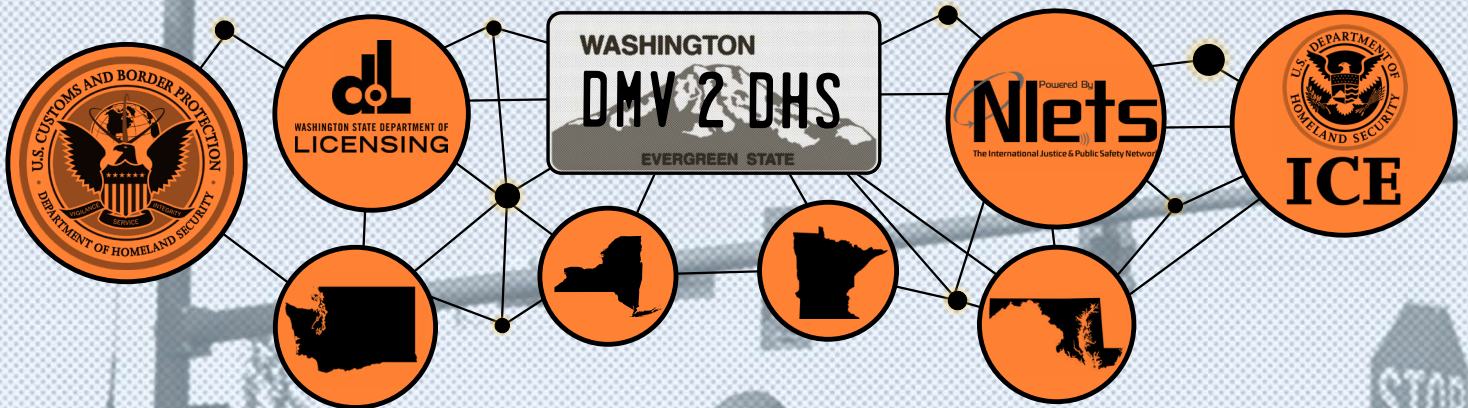


STOPPING THE DMV-TO-DHS DATA PIPELINE

VEHICLE AND DRIVER DATA SHARING WITH
FEDERAL IMMIGRATION AGENCIES



**Stopping the DMV-to-DHS Data Pipeline:
Vehicle and Driver Data Sharing with Federal Immigration Agencies**

University of Washington
October 2026

The University of Washington Center for Human Rights is committed to interdisciplinary excellence in the education of undergraduate and graduate students in the field of human rights; promoting human rights as a core area of faculty and graduate research; and engaging productively with local, regional, national, and international organizations and policymakers to advance respect for human rights.

Center for Human Rights
The Henry M. Jackson School of International Studies
University of Washington
Box 353650, Seattle, WA 98195-3650
Phone: (206) 685-3435 | Email: uwchr@uw.edu
www.jsis.washington.edu/humanrights

CONTENTS

<i>Executive Summary</i>	<i>4</i>
<i>ICE/CBP traffic stops, and why they matter</i>	<i>5</i>
<i>Background: New driver policies create new data pathways.....</i>	<i>9</i>
<i>The DMV-to-DHS pipeline: How does state DMV data end up in ICE/CBP's hands?</i>	<i>11</i>
<i>1) Direct access to state DMV databases</i>	<i>11</i>
<i>2) Nlets</i>	<i>11</i>
<i>3) Data brokers</i>	<i>13</i>
<i>4) State/local agency information-sharing.....</i>	<i>15</i>
<i>Methodology.....</i>	<i>16</i>
<i>Maryland</i>	<i>18</i>
<i>Minnesota</i>	<i>26</i>
<i>New York</i>	<i>33</i>
<i>Washington</i>	<i>38</i>
<i>Best practices</i>	<i>48</i>
<i>Conclusion</i>	<i>50</i>
<i>Appendix</i>	<i>52</i>
<i>Glossary</i>	<i>55</i>

EXECUTIVE SUMMARY

In recent months, traffic stops have become an increasingly frequent, visible, and violent means of immigration enforcement by ICE/CBP; around the country, federal courts have also found them to frequently be unconstitutional.¹ More than just a typical traffic stop, these arrests targeting drivers are fast, and often involve overwhelming force, in many cases they result in collisions, car chases, and violence. This tactic has not previously been used at scale in civil immigration enforcement, and it is causing fear, injury, and even death in immigrant communities.

In many cases, this new wave of arrests is being facilitated by state Departments of Motor Vehicles (DMV). As the University of Washington Center for Human Rights (UWCHR) has revealed in previous research, and as ICE/CBP agents have repeatedly testified in court, these stops typically happen when ICE/CBP travel to locations they believe to be “target rich,” notice a car or driver, look up the license plates in state DMV registries to obtain the names of its registered owner; and then check that name against their own databases. The entire process can unfold in just minutes, and while large-scale data about the ethnic identities of those arrested is not available, based on accounts reported by observers, it appears to target Latino men, especially those driving vehicles associated with construction or landscaping.

In states that have passed laws allowing noncitizens to obtain drivers’ licenses, the DMV-to-DHS data pipeline betrays the promises made to keep immigrants’ data safe. And in all states, the violence frequently associated with this type of arrests, the way in which they enable racial profiling, and the widespread fear such practices sow in targeted communities, raises concerns that are fundamental to democracy. For this reason, many states have taken action to curtail the flow of information from state governments, including their DMVs, to the federal agencies charged with immigration enforcement.

This report compares the efforts of four such 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.² The research presented here suggests that Maryland is still struggling to implement the warrant requirement in its new law; in Minnesota and New York, the data suggest these 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, the data presented here shows that actions taken here to curtail federal agents’ access to DMV data have been ineffective.

This report concludes with suggestions for best practices for all states seeking to curtail the DMV-to-DHS data pipeline. Chief among these

1 See, for example, *M-J-M-A v. Hermosillo*, No. 6:25-cv-02011-MTK, Dkt. 82 (D. Or. Feb. 4, 2026) (finding that ICE’s warrantless arrests were “likely to be found unlawful”); *Escobar Molina v. Dep’t of Homeland Sec.*, No. 25-31417 (BAH), Dkt. 67 (D.D.C. Dec. 2, 2025) (enjoining ICE from making warrantless arrests); *Sanchez Alfaro v. Mullin*, No. 26-0766 (GRB), Dkt. 15 (E.D.N.Y. Mar. 16, 2026) (“Courts nationwide have repeatedly rejected this manifestly illegal practice by ICE officers with little effect”).

2 In Minnesota, this only applies to attempts to access driver (not vehicle) data, and only for drivers who hold non-REAL ID compliant licenses made available to noncitizens. Minnesota does not require a warrant for ICE/CBP to access vehicle data. For more on this, see the section on Minnesota in this report.

is the need to tackle all four possible pathways through which DMV data can be shared with ICE/CBP: directly through database access; through the interstate querying system known as Nlets; through sale to data brokers, who may in turn sell it to ICE/CBP; and through local law enforcement who pass data to ICE/CBP. It is also vitally important to build effective enforcement mechanisms and ensure transparency so that any future violations are detected, and those responsible are held accountable.

ICE/CBP³ TRAFFIC STOPS, AND WHY THEY MATTER

This past summer, the killings of Lorenzo Salgado Araujo and Johan Sebastián Guerrero focused attention on ICE/CBP's increased use of aggressive traffic stops as part of the Trump administration's mass deportation agenda. But attention to the tactic proved brief, despite mounting evidence that its use is increasingly threatening the lives and liberties of citizens and noncitizens alike.⁴ While regular traffic stops are a policing tactic familiar to many Americans, research has long shown that the practice is associated with racially discriminatory outcomes⁵ and

escalating violence,⁶ and especially that the most aggressive "jump out"⁷ form currently practiced by ICE/CBP is deeply dangerous.⁸ The

Policing and Race. Cambridge University Press, 2018.; Kevin Roach, Frank R. Baumgartner, Leah Christiani, Derek A. Epp, and Kelsey Shoub, "At the Intersection: Race, Gender, and Discretion in Police Traffic Stop Outcomes." *The Journal of Race, Ethnicity, and Politics* 7, no. 2 [2020]: 1–23. <https://doi.org/10.1017/rep.2020.35>.; Boehme, Hunter M, and Scott M Mourtgos, "The Effect of Formal De-Policing on Police Traffic Stop Behavior and Crime: Early Evidence from LAPD's Policy to Restrict Discretionary Traffic Stops." *Criminology & Public Policy* 23, no. 3 [2024]. <https://doi.org/10.1111/1745-9133.12673>.

6 Jeannine Bell and Stephen Rushin, "Limits on Traffic Stops: Saving Lives by Constraining Police Authority." *Arizona State Law Journal* 57, no. 1 [2015]: 45–96, <https://lawscholars.luc.edu/en/publications/limits-on-traffic-stops-saving-lives-by-constraining-police-autho/>.

7 The teams carrying out this type of traffic stop are sometimes known as "jump out squads," and have been associated with serious policing abuses. As the DC Justice Lab explains, "A jump-out search undermines constitutional protections established by the 4th amendment because they occur without probable cause or reasonable suspicion required to search a civilian without a warrant or arrest." They also "increase the likelihood of a violent police encounter because they are not clearly identifiable as police officers, so someone may be more likely to defend themselves. (See DC Justice Lab, "Jump-Outs," November 21, 2024, <https://dcjusticelab.org/jump-outs/>.) In some cases, vigilante squads operating within police departments have used jump-out tactics to terrorize, extort, and abuse entire communities, often while glorifying violence against civilians. See for example, "Baltimore Declares End To Plainclothes Policing After Officer Indictments." *NPR*, March 9, 2017, <https://www.npr.org/2017/03/09/519500047/baltimore-declares-end-to-plainclothes-policing-after-officer-indictments>; Waylon Cunningham, "Jump Out Boys Win Appeals after Sheriff's Department Firing." *Los Angeles Times*, January 1, 2021, <https://www.latimes.com/california/story/2021-01-01/jump-out-boys-win-appeals-after-sheriffs-department-firing>; Nicole Flatow, "If You Thought Stop-And-Frisk Was Bad, You Should Know About Jump-Outs." *ThinkProgress*, December 10, 2014, <https://archive.thinkprogress.org/if-you-thought-stop-and-frisk-was-bad-you-should-know-about-jump-outs-385b89fc08d3/>; Kamilah Newton, "We call them 'jump out boys': Videos of protestors getting picked up by unmarked police cars spark outrage, but many say it's not new." *Yahoo News*, July 31, 2020, <https://www.yahoo.com/lifestyle/jump-out-boys-videos-protesters-getting-picked-up-unmarked-police-cars-spark-outrage-many-say-not-new-205040238.html>; Christopher Cann, "ICE Is Relying More on Vehicle Stops. Ex officials say that's dangerous," *USA Today*, July 17, 2026, <https://www.usatoday.com/story/news/nation/2026/07/17/ice-vehicle-stops-immigration-shootings/90942546007/>; Alex Pareene and Sam Raim, "Traffic Stops Were Already Harmful. ICE Is Making Them Worse." *Vera Institute of Justice*, July 31, 2026, <https://www.vera.org/news/traffic-stops-were-already-harmful-ice-is-making-them-worse>.

8 See, for example, Dana Bazelon, "American Police Have Turned Away from this Terrifying, Chaotic Practice. ICE is Embracing It." *Yahoo News*, July 24, 2025, <https://www.yahoo.com/news/articles/american-police-turned-away-terrify->

3 In this report, we refer to the squads carrying out traffic arrests as "ICE/CBP" because since they typically do not wear uniforms or show badges when making traffic stops, it is not possible to identify the agency or agencies involved in any given arrest. Furthermore, their own documents show they often operate in combined teams, and as we explain in this report, in at least some cases they appear to perform queries in DMV data-sharing networks under one another's Originating Agency Identifier (ORI) accounts.

4 See Dara Lind, "The Throughline: Why So Many ICE Traffic Stops Are Turning Deadly." *Documented*, July 24, 2026, <https://documentedny.com/2026/07/24/ice-agents-fatal-vehicle-stops/>; Christopher Cann, "ICE is relying more on vehicle stops. Ex-officials say that's dangerous." *USA TODAY*, July 17, 2026, <https://www.usatoday.com/story/news/nation/2026/07/17/ice-vehicle-stops-immigration-shootings/90942546007/>; ACLU, "Agents of Chaos and Cruelty," July 16, 2026, <https://www.aclu.org/publications/agents-of-chaos-and-cruelty-how-the-trump-administrations-national-deportation-policing-force-has-attacked-american-communities>

5 Frank R Baumgartner, Derek A Epp, and Kelsey Shoub. *Suspect Citizens: What 20 Million Traffic Stops Tell Us About*

term “jump out” refers to a practice in which multiple unmarked vehicles, sometimes lacking license plates, suddenly surround a target while driving, and unidentifiable officers leap from the car to confront its driver with overwhelming force. While ICE/CBP didn’t invent the tactic, its use at scale in immigration enforcement is new,⁹ and raises a thicket of human rights and constitutional questions about racial profiling,¹⁰ due process, and the use of force in everyday law enforcement encounters.

In this report, we focus on just one set of those questions, exploring the ways in which state Departments of Motor Vehicles (DMVs) often provide vital assistance to ICE/CBP in these arrests—even in cases where their state law prohibits them from doing so—by permitting federal agents to query information from their driver and vehicle registries.¹¹ This is the DMV-to-DHS data pipeline. Sworn statements by federal agents before courts in Oregon,¹²

Arizona,¹³ Maryland,¹⁴ Minnesota,¹⁵ and New York¹⁶ make the pattern clear: ICE/CBP agents spot a vehicle that attracts their attention, run its plates to find out the name of its registered owner, and then cross-reference their name against other data sources to decide whether or not to detain the driver. If they decide to do so, they typically arrest the driver within minutes. While ICE has not released any data about the

13 For example, in one case ICE agents described their means of apprehending a person following record checks on a car at Home Depot: “On January 30, 2026, at approximately 1030 hours, Immigration and Customs Enforcement (ICE) Mobile Criminal Apprehension Team (MCAT) Enforcement Removal Operations (ERO) Officers were present at the Home Depot located at 4848 N 43rd Ave, Phoenix, AZ 85031. While at this location, ICE MCAT officers were conducting record checks of vehicles in the immediate vicinity. ICE MCAT officers observed a blue Chevrolet Silverado bearing Arizona license plate EPA33D. Record checks revealed that the vehicle was registered to [name redacted]. Records indicated that [name redacted] had previously been removed from the United States in 2012 via expedited removal. .At approximately 1050 hours, ICE MCAT officers observed the blue Chevrolet Silverado with two male occupants departing the Home Depot and heading south through the parking lot onto N 44th Ave. Near the intersection of N 44th Ave and W Glenrosa Ave, ICE MCAT officers initiated a vehicle stop utilizing their emergency lights,” from *United States of America v. Luis Azemar Isaac*, Case 2:26-cr-00084-SHD, Doc. 1 (D. Ariz. January 31, 2026): <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/ICE-affidavit-license-plate-record-checks-AZ.pdf>. In an entirely different case, but also involving license plate checks performed on a car observed at a Home Depot, an ICE agent Justin McNeil testified before a jury, “We ended up at a Home Depot there...I don’t remember what made us decide to go there. I think we were in the area looking for another target, and then we just ended up getting into the parking lot there and observing people around us there. [We] drove around just looking for suspicious vehicles and whatnot. You know, typical ones that targets that we usually find. And so, anyway, I ended up running through the parking lot, found several license plates, and started running them through our databases.” See *United States of America v. Isaac Luis-Azamar*, No. 2:26-cr-00084-SHD (D. Ariz. July 14, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/26-cr-00084-SHD-USA-vs.-Luis-Azamar-Jury-Trial-Day-1-excerpt-kp.pdf-testimony-about-running-plates.pdf>

14 See *United States v. Santos Alvarenga-Rodriguez*, No. 1:26-mj-00522-CJC, Doc. 1 (D. Md. March 3, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/Maryland-affidavit-Alvarenga-Rodriguez.pdf>

15 See Affidavit of Timothy G. Schanz, No. 0:26-mj-00023-DLM, Doc. 1-1 (D. Minn. January 16, 2026), https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/gov.uscourts.mnd.230473.1.1_2.pdf

16 Josefa Velásquez and Arielle Martinez, “ICE is arresting immigrants on Long Island by surveilling parking lots and running license plates” *Newsday*, July 23, 2026, <https://www.newsday.com/long-island/investigations/ice-immigration-traffic-stops-license-plates-eq5xhbw3>

[ing-094500529.html](https://www.usatoday.com/story/news/nation/2026/07/17/ice-vehicle-stops-immigration-shootings/90942546007/)

9 Christopher Cann, “ICE is relying more on vehicle stops. Ex-officials say that’s dangerous.” *USA TODAY*, July 17, 2026, <https://www.usatoday.com/story/news/nation/2026/07/17/ice-vehicle-stops-immigration-shootings/90942546007/>

10 See, for example, Ryan Mancini, “Immigration Officers Called Latinos Racial Slurs During Stops: Video,” *The Hill*, July 27, 2026, <https://thehill.com/homenews/administration/5996553-aclu-socall-immigration-video-slurs/>

11 ICE has undertaken separate enforcement initiatives targeting immigrants with commercial drivers’ licenses, but we do not address these practices here. For more on these operations, see Lila Desjardins and Layla Quran, “Thousands of Immigrant Truckers Lose Commercial Licenses in Trump Administration Crackdown,” *PBS NewsHour*, May 5, 2026, <https://www.pbs.org/newshour/show/thousands-of-immigrant-truckers-lose-commercial-licenses-in-trump-administration-crackdown>

12 See Maxine Bernstein, “ICE officers reveal arrest quotas, facial recognition use in Oregon dragnet,” *The Oregonian/OregonLive*, December 9, 2025, <https://www.oregonlive.com/crime/2025/12/ice-officers-reveal-arrest-quotas-facial-recognition-use-in-oregon-dragnet.html>

types of vehicles or drivers impacted by this practice, across the country it appears to target Latino men, especially those driving work vans or trucks.¹⁷

It is important to note that despite heightened public concern about Automated License Plate (ALPR) readers, such as those operated by Flock and its competitors, this pattern does not rely on the use of ALPR technology. It is entirely possible that at times when searching for a specific individual, ICE/CBP make use of ALPR technology to find that individual, and then travel to their location to arrest them; but the records of the ICE/CBP traffic stops UWCHR has analyzed in Washington suggest that more frequently, ICE/CBP query the license plates of cars already in front of them. This is also the practice federal agents have described under oath in multiple court proceedings.

Given the speed¹⁸ at which the DMV-to-DHS pipeline operates, arrests are frequently carried

out within minutes after a query is performed. This often takes place without a warrant,¹⁹ sometimes in the midst of traffic and in the presence of bystanders,²⁰ and significantly, such arrests can involve violence. They also sow fear in the communities where they happen. Not only bystanders, but multiple federal judges, have commented on how terrifying these arrests can be: in one case from Massachusetts, Judge Brian Murphy ordered the release of a person who had initially fled because, in the words of the judge, “This Court finds it eminently reasonable to flee out of fear” given that the experience of being suddenly surrounded by “unidentified strangers” seems more like “a carjacking rather than a measured law enforcement action.”²¹ Indeed, when Johan Sebastián Guerrero became the 22nd person shot at by immigration officers during Donald Trump’s second term, one analysis found that 19 of those 22 shootings had taken place during ICE traffic stops.^{22, 23} Since then, the shootings

17 See Alex Pareene and Sam Raim, “Traffic Stops Were Already Harmful. ICE is making them worse,” Vera Institute of Justice, July 31, 2026, <https://www.vera.org/news/traffic-stops-were-already-harmful-ice-is-making-them-worse>; ACLU, “Agents of Chaos and Cruelty,” July 16, 2026, <https://www.aclu.org/publications/agents-of-chaos-and-cruelty-how-the-trump-administrations-national-deportation-policing-force-has-attacked-american-communities>

18 On October 1, 2026, the AP reported that a memo had been sent to all ICE ERO agents on September 30, 2026 instructing them not to engage in high-speed car chases, and imposing additional requirements for traffic stops. (See Ryan J. Foley, “New ICE Guidance bans high-speed car chases and sets tighter rules for traffic stops, a memo shows,” *Associated Press*, October 1, 2026, <https://apnews.com/article/ice-of-ficers-car-chases-vehicle-stops-training-ded50fcee99efab90e55e580250ba2ab>); it is unclear whether this represents a meaningful policy shift. ICE has claimed that it does not; an official statement by an ICE spokesperson claimed the guidance was “nothing new... Occasionally, ICE leadership issues guidance reminders to law enforcement officers... This memo makes no changes to how ICE conducts vehicle stops.” (See Luke Barr, “ICE memo lays out limits on vehicle stops,” *ABC News*, October 1, 2026, <https://abcnews.com/US/ice-sets-limits-officers-stop-vehicles/story?id=136923893>.) The very next day, a high-speed chase occurred, apparently involving ICE/CBP agents, on the freeway in Bellevue, WA, (see Seattle Submissions, “Alleged ICE agents were spotted pursuing a van,” Facebook, October 1, 2026, 1:10pm, <https://www.facebook.com/reel/1855457415478294/>) suggesting that the memo had not translated into a meaningful change of the agency’s practices regarding vehicle stops.

19 While courts have ruled that police can conduct “pre-textual stops”—pulling a car over for a minor traffic violation, but then using that traffic stop to investigate more serious crimes—ICE and CBP lack that authority, and can only legally pull over a vehicle if they have “reasonable suspicion” that the person has violated federal law. One of the ways they generate this “reasonable suspicion” is by looking up license plates to find out information about the person they believe is at the wheel; the information they discover in the DMV database is thus key to their legal argument justifying the traffic stop.

20 See, for example, Cindy Von Quednow, Omar Jimenez, Whitney Wild, and Bill Kirkos, “Chase involving federal agents led to a crash and angry community response in Chicago,” *CNN*, October 15, 2025, <https://www.cnn.com/2025/10/14/us/chicago-ice-protesters-crash>

21 Eleandro Almeida De Souza v. David Wesling, et al., Case 1:26-cv-13761-BEM (D. Mass. September 11, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/Massachusetts-judge-disparaging-ICE-credibility-l213s.pdf>

22 Ariana Figueroa, “Immigrants, DHS agents and traffic stops: Violent outcomes repeat across the US” *News From The States*, July 17, 2026, <https://www.newsfromthestates.com/article/immigrants-dhs-agents-and-traffic-stops-violent-outcomes-repeat-across-us>

23 It is impossible to accurately quantify the total number of traffic stop arrests, since ICE does not compile quantitative data that would allow researchers to discern which arrests are conducted pursuant to traffic stops, as opposed to other forms of “non-custodial” arrests such as arrests at courthouses or jails, or at homes or workplaces; the only ICE documents that reveal the specific method of arrest are I-213s, “Records of Deportable/Inadmissible Aliens” which,

of Wilber Rafael Garcés Pérez on September 20, 2026²⁴ and Oscar Belgal on October 8, 2026 added to the growing list of people shot during ICE traffic stops; the Associated Press reported on October 9 that “ICE agents have fired their guns during more than a dozen vehicle stops since last year, killing at least four people and wounding others.”²⁵



FOR THOSE COMMITTED TO SAFEGUARDING CIVIL RIGHTS, THIS IS AN IMPORTANT QUESTION TO ANSWER, BECAUSE EVEN WHEN WE HAVE LIMITED ABILITY TO AFFECT FEDERAL PRACTICES, IT REMAINS WITHIN OUR POWER TO DEMAND OUR STATES DO BETTER.

Many states prohibit their DMVs from sharing data for purposes of federal immigration enforcement—some, like Washington and Oregon, do so as part of their “sanctuary” laws, and others, like Massachusetts or New York, bar the practice as part of packages of legislation passed in recent years to permit noncitizens to qualify for drivers’ licenses and car insurance. These laws compel state agencies to rework long-established pathways for data sharing, and to resist new ones—but as ICE ramps up its street arrests, there is evidence that some of these laws are being flouted.

similar to a law enforcement arrest report, memorialize the method through which officers “encounter” the subject of the document.

²⁴ According to the *New York Times*, “ICE agents were checking license plates in northwest Austin” when they came across Mr. Garcés, hit his vehicle, and then shot him. See Christina Morales, Hamed Aleaziz, and Billy Witz, “Man Shot by ICE Agent Says His Car Was Struck Twice Before He Was Shot,” *The New York Times*, September 21, 2026, <https://www.nytimes.com/2026/09/21/us/ice-shooting-austin-texas.html>

²⁵ Associated Press, “ICE officer shoots a man while making an arrest in New York, officials say,” *PBS.org*, October 9, 2026, <https://www.pbs.org/newshour/politics/ice-officer-shoots-a-man-while-making-an-arrest-in-new-york-officials-say>

This report examines evidence from Maryland, Minnesota, New York, and Washington. All four states have seen frequent use of the ICE/CBP “jump out” stop as a key enforcement mechanism over the past two years. And all four, to varying degrees and in varying ways, have banned their state motor vehicle registries from sharing data with ICE/CBP for purposes of immigration enforcement. UWCHR researchers set out to examine whether and how these states’ laws have made a difference.

For those committed to safeguarding civil rights, this is an important question to answer, because even when we have limited ability to affect federal practices, *it remains within our power to demand our states do better*. Immigration enforcement draws on many forms of surveillance—including automated license plate readers, facial recognition, cell phone tracking, and more—and all of these are important to understand and contest. But Departments of Motor Vehicles (DMVs) are, by definition, state agencies, and at least in theory, the data they collect is therefore more subject to public control than other forms of surveillance technology which are either predominantly in private hands, or spearheaded by federal agencies themselves without data inputs under the control of state or local authorities.

Furthermore, this issue does not only affect immigrants. Federal immigration agencies have engaged in acts of intimidation against U.S. citizens engaged in the Constitutionally protected act of observing their operations,²⁶ including driving to their homes after querying

²⁶ See, for example, Jude Joffe-Block, “ICE Denies Having a Protester Database. But a Letter to Congress Sheds More Light,” *NPR*, June 10, 2026, <https://www.npr.org/2026/06/10/nx-s1-5843159/ice-protester-database-dhs>; Jude Joffe-Block, “Lawsuit Challenges Intimidation of DHS Observers Across the Country,” *NPR*, September 10, 2026, <https://www.npr.org/2026/09/10/nx-s1-5961220/dhs-ice-observers-surveillance-lawsuit>; and Kat Lonsdorf, Jude Joffe-Block, and Meg Anderson, “ICE Has Spun a Massive Surveillance Web. We Talked to People Caught In It,” *NPR*, March 5, 2026, <https://www.npr.org/2026/03/04/nx-s1-5717031/ice-dhs-immigrants-surveillance-confrontation-deportation-mobile-fortify>

their license plates when they saw them in the street²⁷. In Washington, UWCHR researchers documented queries on U.S. citizens' license plates by federal immigration agencies who observed them conducting "ICE watch" activities.

To be sure, stopping the flow of information from DMVs to DHS won't be enough: ICE/CBP commit abuses unrelated to traffic stops, and they have many other digital surveillance tools in their arsenal, all of which demand further investigation. But working to ensure our states aren't facilitating the abuse of their residents by federal agents is a great place to start. Together, we can unravel the interrelated surveillance technologies that are causing harm in our communities.

BACKGROUND: NEW DRIVER POLICIES CREATE NEW DATA PATHWAYS

In recent years, many states have chosen to make drivers' licenses and vehicle registration available to all residents who pass road safety and insurance requirements, regardless of citizenship.²⁸ As of August 2025, 19 states, plus the District of Columbia and Puerto Rico, had adopted some form of "Licenses for All."²⁹ There is evidence that expanding access to drivers'

licenses in this way improves overall traffic safety,³⁰ while permitting greater access to health care and the labor market for immigrants and their families.³¹ Yet while such policies offer benefits, they also create challenges, for they place data that can be used to identify and locate members of a vulnerable population in the hands of state agencies that have historically shared driver data liberally across state lines.

Washington was the first state to offer drivers' licenses to all, in 1993. At that time, legislators did not foresee the rise of mass deportation, so did not include measures in the law to secure immigrants' driver or vehicle data from use for immigration enforcement. In 2018, however, when it was discovered that the state's DMV—in Washington, the agency is known as the Department of Licensing, or DOL—had been handing over immigrants' data upon request, then-governor Jay Inslee ordered immediate changes.³² The controversy generated by those revelations helped fuel the passage of the 2019 Keep Washington Working Act, which bars the provision of "nonpublicly available personal information" by state or local government agencies to federal immigration authorities "in a noncriminal matter, except as required by state or federal law."³³

27 See Austin Campbell, "Federal Agents are Intimidating Legal Observers at Their Homes: 'They Know Where You Live,'" *The Intercept*, March 5, 2026, <https://theintercept.com/2026/03/05/ice-cbp-minnesota-surveillance-intimidation-observers/>; and Jon Collins, "Privacy Advocates: ICE Using Private Data to Intimidate Observers and Activists," *MPR News*, January 13, 2026, <https://www.mprnews.org/story/2026/01/13/ice-using-private-data-to-intimidate-observers-and-activists-advocates-say>

28 The REAL ID Act of 2005 explicitly allows states to issue drivers' licenses to all regardless of migration status, so there is no contradiction between state and federal law on this point.

29 See "States Offering Driver's Licenses to Immigrants" *National Conference of State Legislatures*, March 13, 2023, <https://www.ncsl.org/immigration/states-offering-drivers-licenses-to-immigrants>

30 Hans Lueders, Jens Hainmueller, and Duncan Lawrence, "Providing Driver's Licenses to Unauthorized Immigrants in California Improves Traffic Safety" *Proc. Natl. Acad. Sci. U.S.A.* 114 (16) 4111-4116, [2017] <https://doi.org/10.1073/pnas.1618991114> find that granting access to drivers' licenses in California had no impact on the rate of accidents, and specifically reduced the incidence of hit-and-run accidents.

31 See Cristian Escalera, Paula D. Strassle, Stephanie M. Quintero, Ana I. Maldonado, Diana Withrow, Alia Alhomsi, Jackie Bonilla, Veronica Santana-Ufret, and Anna María Nápoles, "Perceived general, mental, and physical health of Latinos in the United States following adoption of immigrant-inclusive state-level driver's license policies: a time-series analysis" *BMC BMC Public Health*, 22:1609 [2022]. <https://doi.org/10.1186/s12889-022-14022-x>, and Tianyuan Luo and Genti Kostandini 2026, "Driver's License Reform and the Labor Supply and Benefit Access of Undocumented Farm Workers" *Agricultural Economics* 57, no. 3: e70111 [2026]. <https://doi.org/10.1111/agec.70111>.

32 See MyNorthwest Staff, "Gov. Inslee 'Angered' Over DOL Providing Private Information to Feds," *My Northwest*, July 15, 2028, <https://mynorthwest.com/local/gov-inslee-angered-at-dol/867640>

33 Wash. Rev. Code § 10.93.160 (2026).

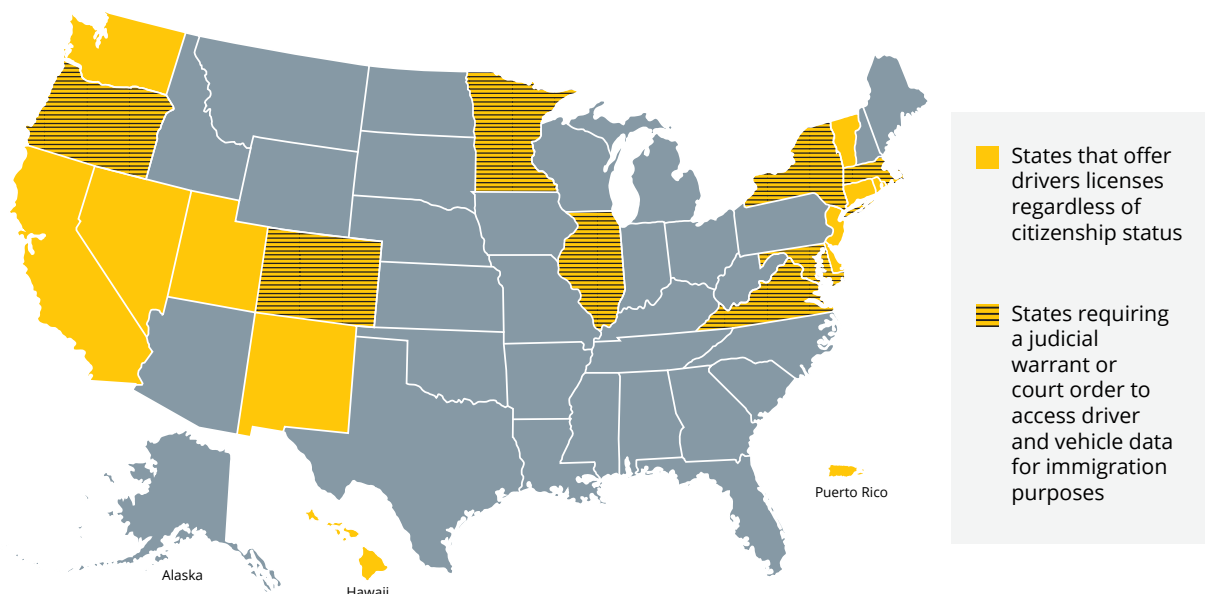


Figure 1: As of August 2025, 19 states, plus the District of Columbia and Puerto Rico, offer drivers' licenses regardless of citizenship status: California, Colorado, Connecticut, Delaware, Hawaii, Illinois, Maryland, Massachusetts, Minnesota, New Jersey, New Mexico, New York, Nevada, Oregon, Rhode Island, Utah, Vermont, Virginia, Washington, District of Columbia, and Puerto Rico. Some states require warrants or court orders for federal agencies to access state-held driver and vehicle data for immigration enforcement purposes. Those states include, but are not limited to: Colorado, Illinois, Massachusetts, Maryland, Minnesota,³⁴ New York, Oregon, and Virginia.

By contrast, Maryland, Minnesota, and New York are part of a wave of states that passed laws to extend drivers' licenses to non-citizens much more recently, and therefore included specific protections in their policies to assure residents that their private data would be secured from federal immigration authorities. While the specific provisions vary from state to state, many states bar the provision of driver or vehicle data to federal immigration agencies absent a judicial warrant or court order; and some further require, in cases where a judicial warrant is presented, for the state DMV to notify the individual whose data was sought within three days.

While many of these laws appear, on paper, to provide strong protections for driver and vehicle data, the volume and nature of immigration arrests occurring on the ground suggest that such protections may not be as airtight as they appear. In particular, research shows that when one means of obtaining DMV data is curtailed,

ICE/CBP often simply look for another open channel.³⁵ For this reason, in subjecting each state's policies to empirical scrutiny to see how they're holding up in light of ICE's determination to increase arrests, UWCHR researchers looked for evidence of four different possible pathways through which data can be shared. We describe these four pathways below, and then outline our research methodology, before turning to the empirical evidence we gathered from each state.



WHILE MANY OF THESE LAWS APPEAR, ON PAPER, TO PROVIDE STRONG PROTECTIONS FOR DRIVER AND VEHICLE DATA, THE VOLUME AND NATURE OF IMMIGRATION ARRESTS OCCURRING ON THE GROUND SUGGEST THAT SUCH PROTECTIONS MAY NOT BE AS AIRTIGHT AS THEY APPEAR.

³⁴ Minnesota's court order requirement for ICE/CBP only covers the driver data of individuals who have applied for or received a non-REAL ID compliant driver's license. It does not cover vehicle data, nor does it cover license data for those who have a REAL ID compliant license.

³⁵ See Georgetown Center on Privacy and Technology, *American Dragnet: Data-Driven Deportation in the 21st Century*, May 10, 2022, <https://americandragnet.org/>.

THE DMV-TO-DHS PIPELINE: HOW DOES STATE DMV DATA END UP IN ICE/CBP'S HANDS?

There are four principal³⁶ ways in which federal immigration officers access DMV data for use in immigration enforcement today:³⁷

1) DIRECT ACCESS TO STATE DMV DATABASES

Many states allow external parties access to their state driver and vehicle databases, often as a means of generating revenue, and sometimes as a service provided gratis to other governmental bodies. In some states, as we discuss in this report, ICE and CBP are among the entities empowered to perform direct searches of DMV data, either as one-off searches of the database, or, in the most concerning of these cases, by downloading driver and vehicle data in bulk, to query at will on their own computers. In some states, private data brokers access state databases, and may then package the data they download into surveillance products for sale to ICE/CBP and others.

2) NLETS

The International Justice and Public Safety Network, commonly referred to as “Nlets,”

³⁶ We are also aware that at times, federal immigration agencies access DMV data by presenting a written request to DMV authorities, but because there does not appear to be a large volume of such requests, we focus here on the more automated forms of communication via databases, which appear to represent a much more frequent source of data.

³⁷ In this report, we detail these practices in Maryland, Minnesota, New York, and Washington; for a comprehensive national explainer, see Georgetown Center on Privacy and Technology, *American Dragnet: Data-Driven Deportation in the 21st Century*.

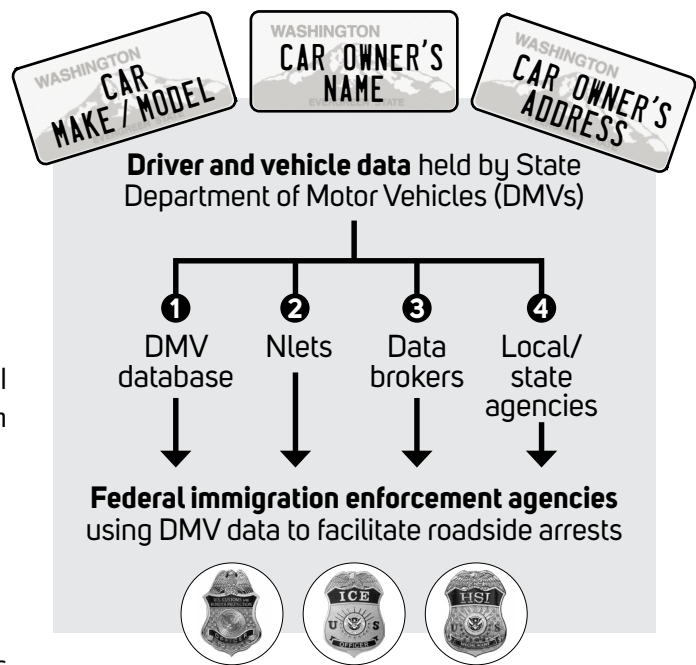


Figure 2: The DMV-to-DHS Pipeline describes four main ways in which federal immigration agencies access state DMV data for purposes of immigration enforcement: direct access to DMV databases; access via Nlets; access via data brokers; and access via local/state agencies. Agents use this data to obtain information on the registered owner of a vehicle they see, then are able to cross-reference their own databases to determine that person's citizenship status.

was established in the 1960s to facilitate information-sharing by law enforcement agencies across multiple states. It is a private non-profit organization, not a government entity. Nlets members include all fifty states and the District of Columbia; its federal members include Customs and Border Protection (CBP), the Department of Justice, Federal Bureau of Investigation, U.S. Citizenship and Immigration Services (USCIS), Immigration and Customs Enforcement (ICE), and more.³⁸ Each user of the network is assigned a nine-digit alphanumeric code, known as an ORI (for Originating Agency Identifier), by the FBI, which functions like a username, allowing them to access the system and recording all queries performed on it as associated with that user.

³⁸ See “General Nlets Fact Sheet,” Nlets, October 2024, <https://nlets.org/sites/nlets/files/2024-10/General%20Nlets%20Fact%20Sheet%20Oct%202024.pdf>

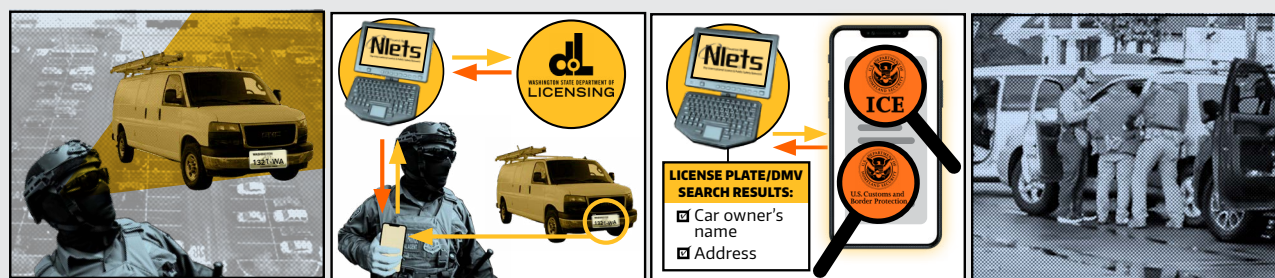


Figure 3: Depiction of how ICE/CBP use Nlets as a tool for surveillance: traveling to locations they expect to find immigrants, running license plates in Nlets to obtain information from state DMVs, and cross-referencing that information with other databases to determine whether to make an arrest.

Nlets also has private business members, some but not all of which are listed on their website as either “strategic partners”³⁹ or “hosting partners.”⁴⁰ It is not clear what, if any, limitations are placed on these private parties’ use of data exchanged through the network. Some of these hosting partners are integrated with data brokers like Thomson Reuters’ CLEAR, which ICE is known to use in tracking immigrants,⁴¹ but the full extent of data-sharing by Nlets with for-profit data brokers is not known.⁴²

What *is* known is that in many states, Nlets serves as the primary means through which federal immigration authorities query state DMVs to link vehicles they observe to specific individuals.⁴³ While Nlets does not permit the

bulk download of data, an agent who spots a vehicle on the street can use the network to send a query to the DMV of the state the car is registered in, using a series of codes known as “message keys” which then generate real-time responses from the DMV. Typically in such operations, officers use the RQ (“registration query”) message key, and receive information such as the name, address, and other details about the vehicle’s registered owner.

These details—especially the name of the vehicle owner—can then be cross-referenced against other sources to obtain further information about the individual’s immigration status. While Nlets does allow users to query the immigration status of individuals using its message key IAQ, which stands for “immigration alien query,” and

39 See “Strategic Partners,” Nlets, <https://nlets.org/communities/strategic-partners>

40 See “Colo Hosting,” Nlets, <https://nlets.org/communities/hosting-partners>

41 See National Immigration Law Center, *Nlets: Questions and Answers*, November 2020, p. 12, <https://www.nilc.org/wp-content/uploads/2020/11/Nlets-Q-and-A-1.pdf>.

42 Since 2025, UWCHR researchers have repeatedly reached out to Nlets leadership seeking to better understand the network’s operations, but we have never received a response.

43 For example, in a 2020 letter objecting to the state of New York’s elimination of their access to such data, Acting DHS Secretary Chad Wolf wrote, “New York DMV records have long been used by ICE law enforcement personnel to

verify or corroborate an investigatory targets’ Personally Identifiable Information (PII), which can include their residential address, date of birth, height, weight, eye color, hair color, facial photograph, license plate, and vehicle registration information. Moreover, ICE’s expeditious retrieval of vehicle and driver’s license and identification information has helped identify targets, witnesses, victims, and assets.” See Chad F. Wolf, Acting Secretary of Homeland Security letter to Mark J.F. Schroeder, Acting Commissioner and Theresa L. Egan, Executive Deputy Commissioner, New York State Department of Motor Vehicles, February 5, 2020, https://www.dhs.gov/sites/default/files/publications/20_0206_as1-letter-to-ny-dmv-signed.pdf

local law enforcement, at least in Washington, do make frequent use of this tool,⁴⁴ ICE records and court testimony suggest that following a registration query of Nlets, ICE/CBP primarily turn to their own internal databases to discern vehicle owners' immigration status.

3) DATA BROKERS

Many states generate revenue by selling driver and vehicle data to private companies for different types of commercial use, such as insurance companies, credit bureaus, and others. These companies are interested in DMV data for purposes like assessing drivers' risk for insurance coverage, or ensuring that vehicle owners receive notification of safety recalls. Yet some of these same companies, in addition to their involvement in the credit or insurance markets, also resell the data they buy from state DMVs to other parties, who use it for other purposes—including immigration enforcement.

For example, Experian is one of the three major credit reporting agencies in the United States; the company compiles packages of information which are then used by businesses to inform decision making about whether to rent someone an apartment or to issue them a car loan. Among the data Experian gathers is vehicle registration information;⁴⁵ and among the

Data brokers

Data brokers collect, sell, or license personal consumer information from various sources to third parties for purposes like assessing insurance rates, providing credit reports, running background checks, conducting targeted ads, and creating searchable directories.

Data held by data brokers can include property records; utility records; bank accounts; credit reports; court documents; records of marriage, divorce, bankruptcy and other proceedings; and social media profiles, among others.

parties they sell it to is Thomson Reuters,⁴⁶ who in turn packages it, alongside data from other sources,⁴⁷ into a comprehensive investigative product called CLEAR,⁴⁸ which they sell to ICE.⁴⁹ (In addition, Experian has a direct contract with ICE; though the terms of that contract are not publicly available, information posted online

44 In Washington, according to data released to UWCHR in records request R018617-121425, Nlets' IAQ query was queried 60 times in a single ten-day period, mostly by local law enforcement agencies. While this report focuses on the use of license plate data in immigration arrests, and not on Nlets' IAQ function, the fact that the network provides a way for law enforcement agents to query a person's immigration status, a practice mostly banned under the state's sanctuary law, raises questions about the degree to which the network may enable noncompliance with sanctuary laws.

45 As Experian advertises, "Experian Automotive is a recognized leader in automotive data and insights. We have over 900 million vehicles in our North American Vehicle DatabaseSM, including automotive industry statistics such as title, registration, mileage readings, and key events, plus more than 11 billion vehicle history records, including title brand and accident-related events." See "Auto Registration Database," Experian, Accessed September 28, 2026, <https://www.experian.com/automotive/auto-vehicle-data>,

46 As Thomson Reuters themselves state, "Our data comes from 5 live gateways: all three credit headers (Equifax, Transunion, and Experian), real-time incarceration and arrest records, and live vehicle data." See "Skip Tracing Top Tips," Thomson Reuters, Accessed September 28, 2026, <https://legal.thomsonreuters.com/en/insights/articles/top-8-tips-to-get-the-most-from-clear-for-skip-tracing>

47 These sources include property records; utility records; bank accounts; credit reports; court documents; records of marriage, divorce, bankruptcy and other proceedings; and social media profiles, among others. For more, see "Prevent Fraud, Detect Risk, and Investigate Crime With Powerful On-line Investigation Software," Thomson Reuters, <https://legal.thomsonreuters.com/en/products/clear>.

48 Ibid.

49 The Department of Homeland Security has a five-year, \$25.2 million contract with Thomson Reuters Special Services LLC, which expires in November 2026. See Department of Homeland Security, *Contract Number 70CMSD21C00000002 with Thomson Reuters Special Services LLC*, USAspending.gov, https://www.usaspending.gov/award/CONT_AWD_70CMSD-21C00000002_7012_-NONE_-NONE-. In addition, ICE recently sought authorization to sign another contract with Thomson Reuters worth \$125 million for what the agency describes as "lead development and targeting to identify violations of U.S. immigration and customs laws," via "continuous monitoring and real-time alerting," among other purposes. See Justification & Approval for Other Than Full and Open Competition, RFO FAR 8.401(b) (Class Deviation 25-20), <https://www.documentcloud.org/documents/28492574-ice-thomson-reuters-125-million/?ref=404media.co>



MANY HAVE CRITICIZED DATA BROKERS FOR ENABLING LAW ENFORCEMENT TO “BUY ITS WAY AROUND THE BILL OF RIGHTS” BY SIDESTEPPING THE REQUIREMENTS OF THE FOURTH AMENDMENT TO THE U.S. CONSTITUTION.

suggests that it involves the use of credit data to support investigations by ICE Homeland Security Investigations.⁵⁰

Another broker to whom many DMVs sell data is LexisNexis. LexisNexis sells subscriptions to investigative databases such as LexID and Accurint, which, like CLEAR, aggregate driver and vehicle data purchased from state DMVs with data culled from other sources. LexisNexis held a five-year, \$24.5 million contract with ICE which ended August 31, 2026;⁵¹ this now appears to have been extended for up to an additional year, for another \$6.7 million.⁵² The contract

language, obtained by journalist Sam Biddle, reveals that at the time of the contract’s initial signing, LexisNexis integrated data on vehicles, including registration information from DMVs, with “near real-time” data from a network of automated license plate readers.⁵³ As reporters from *The Intercept* explain, “In conjunction with Thomson Reuters plate-reader data, the information provided by LexisNexis creates a potential for powerful tracking. Vehicle ownership and registration information from motor vehicle departments, for instance, can tie specific people to plate numbers.”⁵⁴ And since all of this data can be purchased on the open market without ever obtaining a judicial warrant, and deployed against citizens and noncitizens alike, many have criticized data brokers for enabling law enforcement to “buy its way around the Bill of Rights” by sidestepping the requirements of the Fourth Amendment to the U.S. Constitution.⁵⁵

50 See Department of Homeland Security, *Contract Number 70CMSD23P00000139 with Experian Information Solutions, Inc.*, USAspending.gov, https://www.usaspending.gov/award/CONT_AWD_70CMSD23P00000139_7012_-NONE_-NONE-; under FOIA, UWCHR has requested the contract and is awaiting response.

51 See Department of Homeland Security, *Contract Number 70CMSD21C00000001 with LexisNexis Risk Solutions Inc.*, USAspending.gov, https://www.usaspending.gov/award/CONT_AWD_70CMSD21C00000001_7012_-NONE_-NONE-.
52 The details of this are unclear, but see for example, Department of Homeland Security, *Contract Number 70CMSD21C00000001 with LexisNexis Risk Solutions Inc.*: “The U.S. Department of Homeland Security (DHS), through its Immigration and Customs Enforcement (ICE) Office of Acquisition Management in Irving, TX, has issued a Special Notice indicating its intent to award a sole source interim contract to LexisNexis Risk Solutions Inc. This procurement, identified under number 192126FLMURQ0071, is being executed under the authority of 41 U.S.C. § 3304(a)(1) and Federal Acquisition Regulation (FAR) 6.302-1, which allows for noncompetitive awards when only one responsible source is capable of meeting the agency’s requirements. The primary objective of this procurement is to ensure uninterrupted access to LexisNexis Risk Solutions’ proprietary investigative database services, specifically LexID and Accurint Virtual Crime Center...The anticipated contract will cover a seven-month base period, with the possibility of five additional one-month option periods, and is valued at approximately \$6.7 million.” See also “Law Enforcement Investigative Database Subscription” *Higher Gov*, <https://www.highergov.com/contract-opportunity/law-enforcement-investigative-database-subscrip->

[tio-192126flmurq0071-s-cf1a7/](https://www.usaspending.gov/award/CONT_AWD_70CMSD21C00000001_7012_-NONE_-NONE-): “This opportunity appears to have a confirmed incumbent based on the prior contract 70CMSD21C00000001 awarded to LexisNexis Risk Solutions for a law enforcement investigative database subscription (LEIDS) valued at \$24,509,115 (02/25/21–08/31/26). The current requirement similarly seeks continued access to LexisNexis investigative database capabilities (LexID and Accurint Virtual Crime Center) to support investigative, screening, vetting, lead development, and tactical planning functions. The overlap in purpose and the need for continued subscription access suggest the prior work is a direct continuation of the same type of ICE investigative database service.”

53 See *Contract 70CMSD21C00000001*, Performance Work Statement (PWS) Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE) Law Enforcement Investigative Database Subscription, December 10, 2020, p. 5 to 8 (p. 47-49 of PDF): <https://www.documentcloud.org/documents/23854204-2021-icfo-34162-1/>

54 See Sam Biddle, “LexisNexis Is Selling Your Personal Data to ICE So It Can Try to Predict Crimes” *The Intercept*, June 20, 2023 <https://theintercept.com/2023/06/20/lexisnexis-ice-surveillance-license-plates/>

55 See, for example, Don Bell, “Fact Sheet: Closing the Data Broker Loophole,” Project on Government Oversight, January 12, 2026, <https://www.pogo.org/fact-sheets/fact-sheet-closing-the-data-broker-loophole/>; Aaron X. Sobel, “End-Running Warrants: Purchasing Data Under the Fourth Amendment and the State Action Problem,” *Yale Law and Policy Review*, Volume 42, Issue 1 [2023], <https://www.pogo.org/fact-sheets/fact-sheet-closing-the-data-broker-loophole/>; Emile Ayoub and Elizabeth Goitein, “Closing the Data Broker Loophole,” *Brennan Center for Justice*, February 13, 2024, <https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole>.

- The contractor will not use ICE's queries (the license plate numbers input into the system) for its commercial purposes. The contractor will only use the queries submitted by ICE to maintain an audit log.
- The contractor will ensure ICE user queries are conducted anonymously to ensure other individuals or entities that use the LPR service (whether a law enforcement agency, commercial entity, or otherwise) are not able to identify that ICE is investigating a license plate.

Figure 4: Excerpt from Contract 70CMSD21C00000001 between ICE and LexisNexis, requiring the data broker to allow ICE to conduct all searches of their license plate data anonymously. Such contract agreements hinder the ability of audits to ensure that recipients and subrecipients of DMV data are adhering to permissible use requirements and state laws.

To be clear, some states require data brokers to certify that they will not permit the parties to whom they sell DMV data to use it for immigration enforcement; all four states examined here have such a requirement. But are such requirements enforceable, and are their violations even detectable? Language embedded in one contract between ICE and LexisNexis suggests the company has committed to making oversight of such commitments, at least as regards the ALPR data it ingests, impossible. Specifically, the contract (see Figure 4) requires LexisNexis to structure its database querying system in such a way that records of ICE's searches cannot be used or shared for any purpose – indeed, in such a way that even for LexisNexis itself, it would be impossible to know which of its data had been queried by ICE, and to what end.⁵⁶

This means that if LexisNexis itself, or any of the company's business partners (including the

parties from whom they had obtained the data they sold to ICE) sought to conduct an audit to ensure all queries complied with specific permissible use requirements, this would not be possible. In essence, this contract provision renders such audits meaningless, reducing data brokers' certifications of compliance to promises they themselves can't verify.

4) STATE/LOCAL AGENCY INFORMATION-SHARING

There is also a fourth way federal immigration officers access driver and vehicle data: by obtaining it from state or local agencies, including law enforcement. In some states, local law enforcement does this in their official capacity, having signed 287(g) agreements deputizing local police or sheriffs to carry out immigration enforcement duties—or choosing, even in the absence of such agreements, to share data with federal officers. On the other hand, "sanctuary" states or localities have typically enacted specific prohibitions to prevent state or local agency employees from collaborating in immigration enforcement unless they are presented with a judicial order, but these are not always effective at stopping informal collaboration behind the scenes. This type of informal data-sharing can be very difficult to identify and prevent.

⁵⁶ The contract requires that the contractor, in this case Lexis Nexis, "not use any information provided by the agency (query data) for its own purposes or share the information with other customers, business partners, or any other entity," (See Performance Work Statement (PWS) Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE) Law Enforcement Investigative Database Subscription, December 10, 2020, p. 6 (p. 48 of PDF)) as well as "the contractor will ensure ICE user queries are conducted anonymously to ensure other individuals or entities that use the LPR service (whether a law enforcement agency, commercial entity, or otherwise) are not able to identify that ICE is investigating a license plate" p. 7 (p. 49 of PDF). <https://www.documentcloud.org/documents/23854204-2021-icfo-34162-1/>.

METHODOLOGY

As stated above, the laws on the books may say one thing, but how they're being upheld in the street is often quite different. For this reason, UWCHR researchers developed an empirical methodology to test the efficacy of state laws protecting immigrant driver and vehicle data from use in federal immigration enforcement.

First, we sought to identify states with high numbers of ICE/CBP arrests by traffic stops, and in which states agencies possess records about noncitizen drivers. To assess the frequency of traffic stops, we collected information from court documents⁵⁷ which describe the specific method used to identify and apprehend an immigrant on immigration-related charges; ICE records that, similarly, describe the method of identification and apprehension as involving a traffic stop or relying on license plate information;⁵⁸ and descriptions of witnessed arrests provided to our research team by attorneys, rapid response teams, or posted on social media.⁵⁹ On the basis of this information, we identified an initial set of eleven states⁶⁰ where DMVs hold records about undocumented drivers, and where ICE/CBP appear to be engaging in many vehicular arrests.

In these states, UWCHR researchers gathered information about all four DMV-to-DHS data pipelines, as described below. We sought both general information about how the pipeline works, and specific information about whether it contributed to individual ICE/CBP arrests about which we had compiled evidence in each state.

- a. Direct database access: In each state, we sought records about who has access to the DMV's database, under what terms of use, and to what extent users' searches are audited or overseen by the state. We also requested records of any queries made on the license plates of vehicles involved in specific known arrests.⁶¹
- b. Nlets: We filed public records requests of the state agencies involved in administering Nlets queries of DMV data; in most states, this is typically a law enforcement agency like the state police.⁶² In addition to requesting general information on the number and nature of Nlets queries made by federal immigration agencies, we filed requests seeking the records generated by any Nlets queries performed in the lead-up to known immigration arrests. We made the same requests to state police (or their equivalents) and state DMVs, as both institutions' systems should allow access to this information; in some states, DMVs provided information that state police did not (and vice versa).

⁵⁷ We reviewed habeas corpus petitions, criminal charges for unauthorized reentry, and suits brought against DHS for engaging in warrantless arrests, culling data about arrest methods involving the querying of license plates.

⁵⁸ Typically, these documents are I-213s, "Records of Deportable Aliens," compiled by ICE in the course of documenting an "encounter" with a person they consider "deportable."

⁵⁹ We considered social media posts credible when they were accompanied by videos or photos of the arrest, thus corroborating that it was an act of immigration enforcement action pursuant to a traffic stop rather than a regular law enforcement operation, or a vehicle abandoned for unknown reasons.

⁶⁰ These states were California, Illinois, Maine, Maryland, Massachusetts, Minnesota, New Jersey, New York, Oregon, Virginia, and Washington. (This is not intended as an exhaustive list.)

⁶¹ We typically sought this information for the date of the arrest and for approximately two weeks to one month prior to the arrest. In some cases, however, we requested records for a longer period if we had specific information that suggested surveillance may have begun earlier.

⁶² Nlets designates a "Control Terminal Agency" (CTA) in each state, typically a state-level law enforcement agency. Each CTA is responsible for administering access to the national Nlets system through an interface it controls, in compliance with national requirements established by the FBI.

- c. Data brokers: From each state DMV, we requested copies of all active contracts with data brokers, as well as copies of any audits performed pursuant to those contracts. Unfortunately, because data brokers are private businesses, queries made on the databases they construct are not public information, so it is not possible to submit data brokers to empirical scrutiny using public records.⁶³
- d. Local/state agency information-sharing: UWCHR lacks the capacity to conduct empirical investigations into the practices of the thousands of local law enforcement agencies spread across four states, so we did not attempt to do this here. However, in our findings below, we do note cases in which the data we received pursuant to the above three types of inquiry suggest that local law enforcement is actively facilitating the DMV-to-DHS pipeline.

Not all states granted us access to their records. In fact, UWCHR researchers were denied access to state records necessary to conduct empirical research on data-sharing in California, Illinois, Maine, Massachusetts, New Jersey, Virginia, and Oregon. This made it impossible for us to subject state laws to empirical tests in those states, though there is reason to believe the same data pipelines discussed in this report

may exist there as well. For example, the state of Oregon is currently facing a suit brought by immigrant rights advocates over precisely this practice;⁶⁴ and California has recently passed legislation to increase rather than curtail the sharing of its drivers' data across state lines, raising concerns about immigrant privacy.⁶⁵

In cases where a known immigration arrest during a traffic stop was not linked to any searches of DMV data, we looked for other evidence that DMV data was used, either through data brokers or local law enforcement collaboration. The most compelling such evidence is available in court testimony or ICE documents in which the arresting agents describe how they came to identify and apprehend the person, although this is only available in the small minority of total ICE/CBP arrests that wind up in federal court. Even still, in multiple cases discussed below, ICE agents have explained under oath that they queried DMV data as part of their arrest process, and if we cannot find evidence this happened through direct database access or Nlets, we can presume it must be through either data brokers or informal data-sharing among law enforcement agents. Unfortunately, in these cases, it is not possible to prove which specific pathway was used.

63 Furthermore, as noted above, some data brokers' contracts with DHS agencies stipulate that the data broker must configure their systems in such ways that ICE can search the data anonymously, likely rendering it impossible for anyone to examine how ICE uses those databases even with methods *other* than public records. (See *Contract 70CMS-D21C00000001*, Performance Work Statement (PWS) Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE) Law Enforcement Investigative Database Subscription, December 10, 2020, p. 6-7: <https://www.documentcloud.org/documents/23854204-2021-icfo-34162-1/>)

64 See Conrad Wilson, "Oregon State Police Violated State Law by Sharing Data for Years, Lawsuit Says," *Oregon Public Broadcasting*, May 6, 2026, <https://www.opb.org/article/2026/05/06/oregon-state-police-violated-sanctuary-law-sharing-data-ice-lawsuit-claims/>

65 Khari Johnson, Wendy Fry, and Yue Stella Lu, "California to share driver license data despite fears it could expose unauthorized immigrants," *CalMatters*, June 30, 2026, <https://calmatters.org/politics/2026/06/driver-license-sharing/>. While the California law incorporates new "guardrails," the state's total lack of transparency into law enforcement sharing of DMV data means Californians have no option but to trust their state government to administer the program wisely.

MARYLAND

State Nlets administrator, State access point for Nlets	State DMV, Year drivers' licenses made available to noncitizens	State laws limiting data sharing for immigration enforcement purposes	 DMV-to-DHS pipeline pathways
Maryland State Police (MSP), Maryland Electronic Telecommunications Enforcement Resource System (METERS)	Motor Vehicle Administration (MVA), 2013	2021 Driver Privacy Act, 2026 Data Privacy Act	Direct access by federal agencies to MVA database: Evidence reveals that this pathway is currently open, though limited. DHS searches of MVA data via Nlets: Some DHS ORIs have been blocked, but the pathway remains open to others. Access via data brokers: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation. Access via state/local law enforcement: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation.

WHAT THE LAW SAYS

Maryland's data information protection framework for restricting the use of driver and vehicle data in immigration enforcement has been built in three distinct waves, primarily as a response to documented instances of ICE abuse. Unlike New York's and Minnesota's framework, which erected protections when driving privileges were extended to undocumented individuals, Maryland's architecture was built incrementally. This has resulted in a layered protection system, with the core statutory instruments spanning four pieces of legislation

beginning with the Maryland Highway Safety Act of 2013. Earlier this year, Maryland passed the Data Privacy Act of 2026,⁶⁶ which amended the earlier Maryland Online Data Privacy Act⁶⁷

⁶⁶ See text of Data Privacy Act Md. H.B. 711, 2026 Leg., Reg. Sess., ch. 874 (2026), <https://legiscan.com/MD/text/HB711/2026>

⁶⁷ The Maryland Data Privacy Act was passed in 2024, and went into effect on October 1, 2025. For more information, see Attorney General of Maryland Anthony G. Brown, "Data Privacy in Maryland," <https://oag.maryland.gov/resources-info/Pages/data-privacy.aspx?ref=policyedgeai-intelligence-terminal.ghost.io>

to offer among the strongest protections in the nation to prevent the use of driver and vehicle information for immigration enforcement.

Maryland law stipulates that:

- Any party seeking to access the state DMV (known locally as the Motor Vehicle Administration, or MVA) databases for purposes of immigration enforcement must present a judicial warrant.
- This prohibition restricts access to the MVA database as well as access via Nlets system, which is administered by the Maryland State Police and known as METERS.⁶⁸ Maryland also bars any person who receives personal information—such as, for example, a local law enforcement officer—from sharing that information with immigration authorities, unless presented with a valid warrant or court order.⁶⁹
- Lastly, Maryland's laws prohibit the sale of Maryland driver and vehicle data by data brokers to agencies who have conducted or supported civil immigration enforcement within the last six months.⁷⁰

68 “(b) An entity operating a database or a message switching system shall:

(1) deny access to the database or message switching system to any person who is seeking access for the purpose of enforcing immigration law, unless the person presents a valid warrant issued by a federal court or a court of this State.” MD. Code Ann., Public Safety, § 3-529(b)(1) (2025), *Justia*, <https://law.justia.com/codes/maryland/public-safety/title-3/subtitle-4/section-3-529/>

69 See Md. Code Ann., Gen. Provisions § 4-320(g)(2) (2025), *Justia*, <https://law.justia.com/codes/maryland/general-provisions/title-4/subtitle-3/part-ii/section-4-320/>; as amended by HB 711, 2026 Md. Laws ch. 874.

70 Specifically, Maryland Commercial Law § 14-4701 imposes certain obligations on “controllers,” barring them from “knowingly sell[ing] the personal data of a consumer to a federal, State, or local governmental unit that, within the 6 months that immediately precede the sale of the personal data, has engaged in or supported civil immigration enforcement through the provision of personnel or material resources.” (Maryland Commercial Law § 14-4701(1)(6). “Controllers” are defined as entities who “alone or jointly with others determine the purpose and means of processing personal data.” Most data brokers would arguably qualify as “controllers” under this definition. For more, see “CAIR Md. Joins Coalition Urging State Investigation of Data Brokers Over Alleged Privacy Violations,” CAIR, August 19, 2026, https://www.cair.com/press_releases/cair-md-joins-coalition-urging-state-investigation-of-data-brokers-over-alleged-privacy-violations/

On paper, these laws should block all four pathways to the use of Maryland driver and vehicle information for civil immigration enforcement purposes. In a statement provided to UWCHR, Maryland authorities described various steps taken to protect residents' driver and vehicle data.⁷¹ In practice, however, UWCHR researchers found that federal agencies continue to access Marylanders' driver and vehicle data in precisely the ways these laws seek to prohibit.

WHAT'S HAPPENING ON THE ROADS

Today, there is abundant evidence of the use of traffic stops based on DMV queries as a form of immigration enforcement across Maryland. Marylanders have been identified through their license plates while in the Lowe's parking lot;⁷² while waiting at a red light;⁷³ in a McDonald's

71 The full statement, provided on October 11, 2026, reads, “Maryland takes its responsibility to secure personal information from being misused against its residents, including for civil immigration enforcement purposes, seriously. For several years now, MVA removed the direct access into the MVA database for civil immigration enforcement purposes. When it became clear that federal agencies were using third-party database access for civil immigration enforcement purposes in 2025, Maryland implemented a programming change for its own law enforcement lookup tool, which now requires all users to upload a warrant when the search is immigration related. Further, MVA took the affirmative steps to identify and block hundreds of law enforcement requests through NLETS that are associated with civil immigration enforcement. The process of identifying and blocking immigration enforcement agency codes is ongoing. As a result of this action, requests from blocked agencies do not return any personal information, instead information is provided on how to request information, if the search is not related to civil immigration enforcement. Maryland has successfully blocked hundreds of thousands of inquiries from being used for civil immigration enforcement. Additionally, the Maryland MVA requires all data partners to sign privacy agreements, which includes a certification to follow all Maryland laws, including the prohibition against using information gained for civil immigration enforcement purposes.”

72 See Affidavit of Sean O'Rourke in *United States v. Tiago Alexandre Sousa-Martins*, No. 1:26-cr-00045-CDA, Doc. 1-1 (D. Md. January 16, 2026). <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/Sousa-Martins-PC-Affidavit-PACER.pdf>

73 See *United States v. Osvaldo Alquejay-Cordova*, a/k/a “Oswaldo Alquejay-Cordova,” No. 1:26-mj-01567-DRM, Doc. 1 (D. Md. January 23, 2026) <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/Alquejay-complaint.pdf>

parking lot;⁷⁴ or while driving on the state highway.⁷⁵ A large proportion of these arrests appear to target people driving work vans or trucks, frequently with ladders on top or landscaping equipment in the back. In some cases, drivers have been shot⁷⁶ or otherwise experienced violence during their apprehension.

Most concerning, evidence gathered by UWCHR suggests that Maryland's MVA continued to share data facilitating these arrests even after the July 1, 2026 entry into effect of the 2026 Data Privacy Act, which imposed the clearest prohibition yet on the practice. While detailed questions submitted by UWCHR researchers to Maryland officials have gone unanswered, it appears that federal agents continued to access data via Nlets without presenting warrants, and to use that data for purposes of immigration enforcement.

1. Direct access by federal agencies to the MVA

In addition to its use via Nlets, Maryland's MVA makes its data available for sale⁷⁷ in three forms: Interactive Driver and Vehicle Record Inquiry Service (IDVR); Bulk vehicle and driver data delivery service ("Bulk"); and MVA Direct System Access to Vehicle and Driver Records ("PTP"). IDVR is a pathway which allows one-off queries of the MVA database by registered users, rather than the downloading of data; Bulk and PTP access permit searches on the

database as well as the extraction of data from its contents.

In April 2026, the Department of Public Safety and Correctional Services, which oversees the MVA, claimed that "Federal agencies do not have direct access to the Motor Vehicle Administration database,"⁷⁸ yet a review of records of IDVR service in 2025 showed that a small number of federal agencies, including the DHS' Federal Protective Service⁷⁹, did have direct access as recently as 2025.⁸⁰ UWCHR reviewed a written statement provided by the Federal Protective Service to the MVA, asserting that they had no involvement in immigration enforcement, and did not find any evidence that DHS-FPS queries of MVA data were associated with immigration arrests. Nonetheless, given the FPS' murky mandate,⁸¹ access by FPS and other federal agencies to such pathways must continue to be monitored to ensure compliance with state law.

2. ICE/CBP searches of Nlets/METERS

In Maryland, the State Police are the agency administering the Nlets switch allowing federal agents access to MVA data—and other data sources—via an interface known as METERS.

74 See Affidavit of Carly Adams in *United States v. Melvin Escobar Rodriguez*, No. 1:26-mj-01115-CJC, Doc. 1 (D. Md. May 7, 2026) <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/affidavit-Escobar-Rodriguez-plates.pdf>

75 Video of an arrest on Route 175 is available on Facebook: <https://www.facebook.com/reel/821161547704410>; the white work van's license plate number was later found to have been queried in METERS multiple times the morning of its driver's arrest.

76 See Alex Mann, "Partner of Man Shot By ICE in Glen Burnie Speaks Out as He Fights for Freedom," *The Banner*, July 10, 2026, <https://www.thebanner.com/community/local-news/anne-arundel-county-ice-glen-burnie-christ-mas-shooting-donald-trump-3DZDIVAZW5C77GN4ZGA64QX-7WY/>

77 Data charges are waived for government agencies, who are provided access to MVA data free of charge.

78 Quoted in Ruben Castaneda, "ICE Using Driver's License Data in Md. Immigration Enforcement State: Senator Blames Loophole for Access," *The Baltimore Sun*, April 9, 2026, <https://www.baltimoresun.com/2026/04/09/ice-immigration-deportation/>

79 According to records provided to UWCHR pursuant to public records request # PR-CN00008663, the Department of Homeland Security's Federal Protective Service (FPS) has current access to the MVA's IDVR service. An anonymous source told UWCHR researchers that after the MVA terminated its access, along with that of other DHS units, in 2021, FPS provided an attestation that it would not use data obtained from IDVR for purposes of immigration enforcement, and its access was reinstated.

80 A list of users of the MVA's IDVR, DBM, and Bulk services in 2025, with the number of downloads by each, was provided to UWCHR researchers via public records request # PR-CN00008663. It is relevant to note that IDVR users are unable to download data in bulk.

81 See Spencer Reynolds, "Inside the Federal Protective Service, Homeland Security's Domestic Police Force," *Brennan Center for Justice*, October 8, 2024, <https://www.brennancenter.org/our-work/research-reports/inside-federal-protective-service-homeland-securitys-domestic-police>

1:26-mj-0072-CDA

PROBABLE CAUSE

11. On December 24, 2025, officers with the Department of Homeland Security (“DHS”) Immigration and Customs Enforcement (“ICE”) Enforcement and Removal Operations (“ERO”) (“ERO officers”) were performing field operations related to the apprehension and removal of individuals violating United States immigration laws in the District of Maryland. Specifically, six ERO officers spread across five government owned vehicles were patrolling when members of the group observed a white Nissan cargo van bearing Maryland registration [REDACTED] (the “**Subject Vehicle**”) in the parking lot of the Lowes home improvement store located at 415 George Clauss Boulevard, Severn, Maryland, near the delivery entrance. An ERO officer reviewed Maryland Motor Vehicle Administration (“MVA”) records and learned that the **Subject Vehicle** is registered to [REDACTED] at an address in Baltimore, Maryland. The ERO officers on site obtained a photograph of [REDACTED] from the MVA database and disseminated it amongst each other to aid in identifying him. ERO officers then visually identified [REDACTED] against the MVA photograph as he exited the Lowes and approached the **Subject Vehicle** before entering it. Specifically, one ERO Officer (“ERO Officer 1”) had a clear frontal view of [REDACTED], which Officer 1 relayed to others including ERO Officer 2 and ERO Officer 3. Those officers confirmed that they also made similar observations and believed the individual to be [REDACTED]. An ERO Officer then ran [REDACTED] information against immigration databases maintained by the Department of Homeland Security (“DHS”). His query revealed that [REDACTED] was listed as a non-U.S. citizen who had overstayed his B-2 visa status since 2008.

12. ERO officers surveilled and followed the **Subject Vehicle** as [REDACTED] drove it away from the Lowes to the vicinity of West Court, located in Glen Burnie, Maryland.

***Figure 5:** A federal court affidavit describing ICE ERO officers on patrol, identifying a car at a Lowe’s parking lot, searching the car’s license plate number in Maryland Motor Vehicle Administration (MVA) data to identify the name of the registered owner and obtain a photograph. Officers then cross-reference the name in their own database to determine the vehicle owner’s citizenship status, use the MVA-provided photo to identify and confirm the driver, and proceed to surveil the vehicle and make an arrest. Yellow highlight and personal driver information redaction by UWCHR.*

The available evidence suggests that federal immigration agents make routine use of Nlets to query its contents.

Descriptions of this process have emerged in multiple federal court cases. For example, in one case, ICE agents shot a man while attempting to arrest him after scanning the license plates on his work van in a Lowe’s parking lot on December 24, 2025; an excerpt from the sworn affidavit⁸² is provided below, in Figure 5.

In another case from January 2026, an FBI agent attested in a sworn affidavit that ICE officers were tasked with identifying immigration violators, so they ran the license plates on vehicles they came across; the officers are described as having conducted nine queries on individuals who “were not found to be in violation of immigration laws” before, on the tenth query, discovering that the license plate

District Court in Baltimore MD: <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/affidavit-in-Maryland-on-use-of-DMV-data-to-arrest-in-Lowes-parking-lot.pdf>

⁸² See Document 1-1 in Case 1:26-cr-00045-CDA in the U.S.

on a Toyota Corolla was associated with a person whose Maryland driver's license included the restriction codes "AU."⁸³ These codes are part of the MVA database, which includes restriction codes, such as "may not be used to purchase a firearm" (which is coded as A) and "not acceptable for federal purposes" (which is coded as U).⁸⁴ According to one of the ICE officers, they believed the AU designation indicated that the owner of the vehicle was likely to lack legal authorization to be present in the United States, so they pulled the vehicle over. During the arrest, a physical altercation ensued; the arrestee was later criminally charged with "assaulting, resisting, or impeding" federal officers.⁸⁵ The charges were later dismissed, but the arrested man, who had no criminal record and claimed to have resided in the United States for 19 years, was still deported to El Salvador.⁸⁶ In this case, then, federal immigration agents admittedly used their access to MVA data to query cars at random, leading to what was likely a warrantless civil arrest and deportation.

In addition to reviewing court cases, UWCHR researchers consulted MVA and MSP records to determine whether federal queries preceded known immigration arrests of Maryland drivers in 2026. In nine cases, UWCHR received confirmation that known immigration arrests

were preceded by queries of the MVA data using METERS/Nlets, just minutes or hours before the arrest. Most likely, these represent just a fraction of the total arrests made possible by this pathway. The cases are detailed below:

- On March 14, 2026, according to an ICE officer's sworn affidavit, officers spotted a Honduran man in a McDonald's parking lot in Salisbury, MD, and "submitted [his] license plate registration through various law enforcement databases." They then discovered it was registered to a man who had been previously deported, so they proceeded to arrest him and charge him with illegal re-entry. On the day of his arrest, MVA records show a law enforcement query of his license plates via Nlets/METERS, although Maryland State Police claimed they had "no responsive records" when asked about METERS queries.
- On March 30, 2026, according to an ICE officer's sworn affidavit, officers from Salisbury ICE Enforcement and Removal Operations (ERO) "encountered" a Guatemalan man in Trappe, MD, when they pulled over a truck in which he was a passenger; its driver was the truck's registered owner and their target in doing the vehicle stop. They interviewed all occupants of the vehicle and Gonzalez admitted to being in the country without authorization after a previous deportation. He is now being charged with unlawful reentry under 8 U.S. Code § 1326. Records released to UWCHR by Maryland's MVA revealed two Nlets/METERS queries on the day of the arrest.⁸⁷
- On April 25, 2026, an unknown person driving a white truck was arrested in Jessup, MD, by federal immigration authorities, according to photos and video of the

83 See Affidavit of Amy Renee Ferron for United States v. Santos Alvarenga Rodriguez, No. 1:26-cr-00116-JKB, Doc 1 (D. Md. March 3, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/Maryland-affidavit-Alvarenga-Rodriguez.pdf>

84 See Tyler Maryland and MDOT Motor Vehicle Administration, *MDOT MVA Direct System Access to Vehicle and Driver Records: Integration Guide Version 3.1*, p. 63, <https://egov.maryland.gov/mva/PTP%20Integration%20Guide.pdf>

85 The fact that he was criminally charged is the only reason we have access to sworn affidavits regarding the circumstances of his arrest; in most cases, information about how ICE located an individual driver is not publicly available. See United States v. Santos Alvarenga Rodriguez, No. 1:26-cr-00116-JKB, Doc. 16 (D. Md. April 2, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/charges-against-Alvarenga-Rodriguez.pdf>

86 See the Government's Motion to Dismiss for United States v. Santos Alvarenga Rodriguez, No. 1:26-cr-00116-JKB, Doc. 23 (D. Md. May 14, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/order-to-dismiss-charges-against-Alvarenga-Rodriguez.pdf>

87 When asked for the same records, the Maryland State Police told UWCHR they could not be released as they were confidential.

incident posted to social media.⁸⁸ UWCHR sought records of associated METERS queries from the MSP and were told the agency had no records responsive to our request. However, MVA records revealed *many* METERS queries the morning of the arrest, shown in Figure 6 below.

- On April 30, 2026, multiple social media users posted images of a white work van alleging its driver had been arrested by ICE/CBP.⁸⁹ Using the license plate number visible in the posted images, UWCHR sought records of queries on that number from both the MSP and MVA. The MSP responded that any records of such queries would be confidential and could not be released. MVA records, however, revealed a query of Nlets/METERS on the morning of the reported arrest.
- On July 5, 2026, multiple photos and videos posted to social media⁹⁰ show an ICE arrest of an unknown person on University Boulevard in Langley Park. MVA records released to UWCHR reveal a METERS query by law enforcement on that vehicle's license plate number the morning of the arrest.
- On July 6, 2026, a social media post⁹¹ reports that the driver of a grey work truck, shown with ladders on top, was arrested by ICE on Pulaski Highway in Baltimore; the truck's license plate number is visible in the photos. MVA records released to UWCHR revealed multiple METERS queries by law enforcement on the morning of the arrest.

- On July 10, 2026, an unknown driver of a white work van was arrested at a McDonalds in Beltsville; photos confirming ICE/CBP conducted the arrest were posted online.⁹² MVA records released to UWCHR show many METERS queries on the day of arrest.
- Also on July 10, 2026, an unidentified driver of a grey Chevrolet truck was arrested in Adelphi, MD, reportedly by ICE/CBP; MVA records show 3 METERS queries the day of the arrest.
- On July 11, 2026, an unknown person was arrested by ICE/CBP while driving a white Ford SUV on North Frederick Avenue in Gaithersburg MD. Photos of the arrest and the abandoned vehicle left behind were posted on social media⁹³; using its visible license plate number, UWCHR researchers sought and received records which show many METERS queries and one "criminal justice" query on the day of the arrest.

In April 2026, Maryland's DPSCS has said in a written statement, "The administration has taken steps to ensure that federal law enforcement access through third-party systems, such as the International Justice and Public Safety Network, also known as Nlets, complies with state and federal law. For months, the state has been working urgently to modernize outdated database systems. As this work takes place, the administration has instituted measures to prevent immigration authorities from accessing MVA data without a judicial warrant."⁹⁴

88 Video of arrest available on Facebook: <https://www.facebook.com/reel/821161547704410> and photos: <https://www.facebook.com/share/p/1HPHLYXBV8/>

89 See the photo of the abandoned van on Facebook: <https://www.facebook.com/BaltimoreDM/posts/pfbid0n3tX-BHRb2nwzyEUyRxeVlFQMPxTEmkwFNS53YH52imiKrP8jrc-BGPgEpBpwDEEz5/> and video: <https://www.facebook.com/reel/2305029593404950>

90 For example, see Facebook photos here: <https://www.facebook.com/share/p/1Uzpw7Xrq/>, <https://www.facebook.com/groups/940082819341837/permalink/28661323960124350/>, and <https://www.facebook.com/share/p/1EdWaqpwNn/>

91 See <https://www.facebook.com/share/p/1Jnahih69E/>

92 See on Facebook: <https://www.facebook.com/reel/27501598869449443>, <https://www.facebook.com/share/p/185CQ5jiU5/>, and <https://www.facebook.com/share/p/1UWE2azXwB/>

93 See <https://www.facebook.com/ctrejo010/posts/pfbid-0ZgNwazTPUrbT1bdyUm8ebPXmkFuSeJoQAGYm91GGw5v-Vnk5aS2amYsGc4w5g4BSGI?rldid=SbEH1BhM2kqCBeI>

94 Quoted in Ruben Castaneda, "ICE Using Driver's License Data in Md. Immigration Enforcement State: Senator Blames Loophole for Access," *The Baltimore Sun*, April 9, 2026, <https://www.baltimoresun.com/2026/04/09/ice-immigration-deportation/>

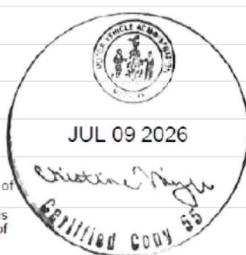
Customer Record Search Inquiry Report				
Search Type	Search Text	Who	Additional Info	Inquiry Time
External		Law Enforcement Inquiry	Meters	25-Apr-2026 07:20:38
External		Law Enforcement Inquiry	Meters	25-Apr-2026 07:31:20
External		Law Enforcement Inquiry	Meters	25-Apr-2026 07:43:04
External		Law Enforcement Inquiry	Meters	25-Apr-2026 07:43:15
External		Law Enforcement Inquiry	Meters	25-Apr-2026 07:43:22
External		Law Enforcement Inquiry	Meters	25-Apr-2026 10:30:38
External		Law Enforcement Inquiry	Meters	25-Apr-2026 10:30:58
External		Law Enforcement Inquiry	Meters	25-Apr-2026 10:31:06
External		Law Enforcement Inquiry	Meters	25-Apr-2026 10:31:15
9 Rows		As Motor Vehicle Administrator for the State of Maryland and by virtue of the authority vested in me under the Transportation Article, Maryland Vehicle Law, I do hereby certify, under the penalty of perjury, that this is a true copy taken from the original now on file and part of the records of this Administration. 		

Figure 6: On April 25, 2026, a person driving a white truck was arrested by federal immigration authorities in Jessup, MD, according to photos and video of the incident posted to social media. Records released to UWCHR, shown above, revealed nine queries of that vehicle's license plate number in METERS/Nlets by "Law Enforcement Inquiry" that same day (plate number redacted by UWCHR). The Maryland records released publicly do not identify the law enforcement agency making the query.

While this statement does not specify what measures have been taken, the state of Maryland's statement to UWCHR in October 2026 explains further: the state instituted a "programming change for its own law enforcement lookup tool," which requires all Maryland law enforcement users to indicate whether their search is immigration related, and if so, to upload a warrant prior to receiving access to the relevant data. However, this requirement applies to state and local law enforcement accessing MVA data via METERS, not to federal agencies using Nlets to access the system. As Maryland's statement to UWCHR explains, the state has gone about blocking federal agencies from access to MVA data on a case-by-case basis.⁹⁵ Yet an unknown number of DHS ORIs remain unblocked.

In addition to the data sharing itself, the discrepancies in the responses by different agencies to UWCHR queries is worrisome, underscoring the importance of increased

transparency. In one of the cases mentioned above, for example, an ICE officer stated in a sworn affidavit submitted in federal court that she and her colleagues ran a vehicle's license plates through law enforcement databases to determine who was its owner; when UWCHR sought copies of such queries, representatives of the State Patrol responded that no such records existed, whereas MVA produced records confirming two queries via Nlets/METERS immediately preceding the arrest. (In still other cases, MSP responded to UWCHR requests saying that the data could not be provided because it was confidential, yet the MVA provided data confirming that Nlets/METERS searches preceded the arrests.)

Similarly, the MSP told UWCHR, "We have had no queries made in METERS from ICE or CBP from 1-1-26 to 6-1-26 for MVA records,"⁹⁶ Yet this is hard to reconcile with the records received from the MVA in the above nine cases, which specifically document METERS queries prior to known immigration arrests. Similarly,

⁹⁵ See footnote 71 for the full text of Maryland's statement to UWCHR

⁹⁶ Maryland public records request # 26-2417

the Maryland State Police—the entity which administers Nlets/METERS—has reported to the Maryland legislature that over the past four years, they have received zero requests for personal information from federal agencies for purposes of immigration enforcement, but this is difficult to square with other available records, such as the federal court affidavit shown in Figure 5, which documents a search of MVA data in 2025.⁹⁷ Unfortunately, representatives of the Department of Public Safety and Correctional Services did not respond to multiple requests from UWCHR for interviews or information.

3. Data brokers

LexisNexis—one of the top providers of motor vehicle data to DHS—is one of the top users of MVA data, having made a total of 1,046,936 downloads in 2025 alone, according to data provided by the MVA to UWCHR.⁹⁸

The MVA does require that users indicate, as part of their access to the data, their understanding of permissible use standards,

which include stipulations that they “may not disclose information obtained as a result of their access to personal information from Motor Vehicle Records to any federal agent or federal agency for the purpose of federal immigration enforcement.”⁹⁹ However, each user verifies their own compliance, as well as that of any sub-users with whom they share data. Per the terms of LexisNexis’ contract with the Department of Homeland Security, any audit would be unable to uncover evidence of ICE queries anyway,¹⁰⁰ so it is unclear how informative or useful the process could be.

For this reason, a coalition of immigrant rights and privacy organizations recently requested that Maryland Attorney General Anthony Brown initiate investigation and enforcement against a number of data brokers to whom Maryland MVA sells data, and who are known to in turn sell data to DHS, including LexisNexis and Thomson Reuters.¹⁰¹

97 In 2021, Under MD General Provisions Code § 4-320.1, the Department of State Police is required to report to the General Assembly each year on June 1 as to the number of requests received from federal agencies for personal information, a photograph, or a facial recognition search, for purposes of federal immigration enforcement in the previous calendar year, and for the past four years they have claimed no such information was requested from federal authorities. See Maryland Department of State Police, *Federal Requests for Photograph or Facial Recognition Search for Immigration Enforcement 2025, General Provisions Article, Section 4-320.1*, June 1, 2026, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/GP4-320.1b3_CY2025.pdf; Maryland Department of State Police, *Federal Requests for Photograph or Facial Recognition Search for Immigration Enforcement 2024, General Provisions Article, Section 4-320.1*, June 1, 2025, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/GP4-320.1b3_CY2024.pdf; Maryland Department of State Police, *Federal Requests for Photograph or Facial Recognition Search for Immigration Enforcement 2023, General Provisions Article, Section 4-320.1*, May 2024, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/GP4-320.1b3_CY2023.pdf; and Maryland Department of State Police, *Federal Requests for Photograph or Facial Recognition Search for Immigration Enforcement 2022, General Provisions Article, Section 4-320.1*, June 2023, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/GP4-320.1b3_CY2022.pdf.

98 This data was released to UWCHR pursuant to records request PR-CN00008948.

99 State of Maryland Department of Transportation Motor Vehicle Administration, *Privacy Protection Policy*, p. 1, provided to UWCHR in records request PR-CN00008946.

100 As noted above, “The contract requires that the contractor, in this case Lexis Nexis, “not use any information provided by the agency (query data) for its own purposes or share the information with other customers, business partners, or any other entity,” (See *Contract 70CMSD21C00000001*, Performance Work Statement (PWS) Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE) Law Enforcement Investigative Database Subscription, December 10, 2020, p. 7 (p. 34 of the PDF): <https://www.documentcloud.org/documents/23854204-2021-icfo-34162-1/>) as well as “the contractor will ensure ICE user queries are conducted anonymously to ensure other individuals or entities that use the LPR service (whether a law enforcement agency, commercial entity, or otherwise) are not able to identify that ICE is investigating a license plate.”

101 See We Are CASA et al., “Consumer Complaint Regarding Violations of Maryland Privacy Law by Multiple Actors in the Data Industry,” *before the Office of the Maryland Attorney General*, August 19, 2026, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/Coalition-Privacy-Complaint-to-Maryland-OAG-2026-08-19.pdf>.

MINNESOTA

State Nlets administrator, State access point for Nlets	State DMV, Year drivers' licenses made available to noncitizens	State laws limiting data sharing for immigration enforcement purposes	 DMV-to-DHS pipeline pathways
Minnesota Bureau of Criminal Apprehension (BCA), Law Enforcement Message Switch (LEMS)	Driver and Vehicle Services (DVS), 2023	2023 Driver's License For All Act 2026 revisions to bill (These laws only apply to non-REAL ID compliant driver data, leaving access to all other drivers' data and vehicle data open)	Direct access by federal agencies to DVS database: Evidence reveals that this pathway is currently open for vehicle data. DHS searches of DVS data via Nlets: Evidence reveals that this pathway is currently open for vehicle data. Access via data brokers: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation. Access via state/local law enforcement: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation.

WHAT THE LAW SAYS

Minnesota's 2023 law "Driver's License for All" allows undocumented residents to qualify for drivers' licenses, and incorporates important data protections to ensure their privacy:¹⁰²

- First, the state's DMV—known locally as Driver and Vehicle Services, or DVS¹⁰³—is

¹⁰² For more on this, see Andrew Hazzard, "Could Trump use Driver's License for All data for deportations? Minnesota Officials Say Protections Are in Place as Applications Roll In," *Sahan Journal*, November 15, 2024, <https://sahanjournal.com/immigration/drivers-license-for-all-minnesota-undocumented-trump-deportation/>

¹⁰³ In Minnesota, Driver and Vehicle Services (the "DMV") is part of the Division of Public Safety. See "DVS getting

not allowed to share information about individuals who have applied for or received a non-REAL ID compliant driver's license with ICE/CBP unless ordered by a court to do so. This prohibition applies both to parties accessing data via direct requests of the MN DMV and to those accessing its data via Nlets, which is administered locally by the Bureau of Criminal Apprehension through the Law

Minnesotans ready for Driver's License for All" *Minnesota Department of Public Safety*, August 3, 2023, <https://dps.mn.gov/news/dvs-getting-minnesotans-ready-drivers-license-all>

4/25/2026-5/7/2026 Responses

(Total Queries: 3)

Repository: Driver and Vehicle Services

Transaction ID	Date	Time	Originating Agency (ORI) Identifiers		Query Type	Search Criteria:
79d231f2-e747-490e-8e1b-af20daa473f6	4/27/2026	8:26:29 AM	MNICE0100	Dept of Homeland Security - St. Paul	Search Motor Vehicle	
931cff58-e6cb-4d93-b31f-8bc621fca4fd	4/28/2026	11:37:11 AM	MNICE0100	Dept of Homeland Security - St. Paul	Search Motor Vehicle	
df9e818f-9d1a-4273-80f4-71ae99450660	4/28/2026	11:40:53 AM	MNICE0100	Dept of Homeland Security - St. Paul	Search Motor Vehicle	

Figure 7: Minnesota Driver and Vehicle Services (DVS) documents obtained under public record law by UWCHR show the ORI MNICE0100, associated with Department of Homeland Security - St. Paul, performed a “Search Motor Vehicle” query directly in the DVS’ database of the same license plate number three times during a two-day period in late April 2026. One week later, on May 6, community observers reported the arrest of a man driving this vehicle in Minneapolis. Plate number redacted by UWCHR. In addition to direct searches of MN DVS data, ICE queried the plate number in Nlets/LEMS to obtain vehicle information, see Figure 8.

Enforcement Message Switch (LEMS). It also prohibits local law enforcement officers who may receive information about a non-REAL ID compliant driver’s license holder from sharing that information with federal immigration authorities.¹⁰⁴

- Second, third party data brokers who purchase data from the state of Minnesota must provide certification that they will not share private data about non-REAL ID compliant license holders with federal immigration enforcement authorities. They are also required to submit to regular third-party audits.¹⁰⁵

Significantly, however, Minnesota law does *not* prohibit sharing of *vehicle registration information* with immigration authorities. In other words, it is entirely legal under Minnesota law for Minnesota’s DMV to provide federal immigration authorities access to Minnesotans’ vehicle information by querying their license plates.

Unsurprisingly, UWCHR researchers have found significant evidence that this is happening.

¹⁰⁴ Minnesota Code Sec. 171.12. Subd. 7b., *Office of the Revisor Statutes*, <https://www.revisor.mn.gov/statutes/cite/171.12>

¹⁰⁵ See Marjaan Sirdar, “Minnesota ‘Driver’s Licenses For All’ Bill a National Model For Data Privacy Protections, Advocates Say,” *Unicorn Riot*, April 20, 2023, <https://unicornriot.ninja/2023/minnesota-drivers-licenses-for-all-bill-a-national-model-for-data-privacy-protections-advocates-say/>

WHAT’S HAPPENING ON THE ROAD

ICE/CBP traffic stops were a key part of Operation Metro Surge in Minnesota in early 2026, and they have continued—albeit at a lesser rate of intensity—since then. UWCHR research suggests reason to be concerned about federal immigration enforcement agencies accessing Minnesota DMV data through all four of the possible pathways.

1. Direct queries of DVS database by ICE

UWCHR researchers found evidence of ICE/CBP accessing Minnesota’s Driver and Vehicle Services (DVS) database directly, without relying on Nlets, to query vehicle data. The May 6, 2026 arrest of a driver of a maroon GMC van occurred shortly after the van’s license plates were queried through Nlets/LEMS, as discussed in the next section. Yet just a week prior, a user account associated with ICE (identified as “Department of Homeland Security - St. Paul” in Bureau of Criminal Apprehension (BCA) records) queried the van’s license plate number in the DVS database directly, as seen in Figure 7. This does not appear to contradict Minnesota law, however, because the law does not require protections for vehicle data.

4/25/2026-5/7/2026 Responses

(Total Queries: 4)

Repository: Law Enforcement Message Switch (LEMS)

Transaction ID	Date	Time	Search Criteria	Originating Agency (ORI) Identifiers	Query Type(s)/Message Key
49B0A00A35	4/29/2026	7:16:53 AM		VTICE1961	Immigration and Customs Enforcement
WWWXBZZGH4	4/29/2026	7:16:54 AM		VTICE1961	Immigration and Customs Enforcement
49B0A25C46	5/5/2026	6:00:54 AM		VTICE1961	Immigration and Customs Enforcement
WWWXB5QSS2	5/5/2026	6:00:55 AM		VTICE1963	Immigration and Customs Enforcement

Figure 8: Documents released to UWCHR from the MN BCA show two different ORIs associated with ICE—VTICE1961 and VTICE1963—querying Nlets/LEMS for information on the same license plate number on April 29, 2026 and May 5, 2026, (plate number redacted by UWCHR). The next day, May 6, 2026, community observers reported the arrest of a man driving this vehicle in Minneapolis. In addition to querying the plate number in Nlets/LEMS, DHS directly searched MN DVS database for vehicle information related to this license plate number, see Figure 7.

2. ICE/CBP searches of Nlets/LEMS

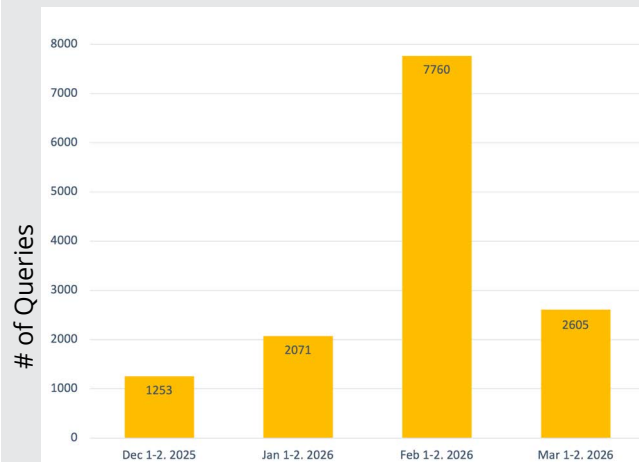
Minnesota officials have applied a block to Nlets/LEMS queries originating in ORIs associated with all DHS agencies, including ICE ERO, ICE HSI, USCIS, and CBP.¹⁰⁶ However, this block only applies to queries about drivers with non-REAL ID licenses, not to queries about vehicles, or about individuals with REAL ID compliant licenses. For this reason, significant vulnerabilities remain.

UWCHR researchers found ample evidence of license-plate based queries of Nlets/LEMS by ICE and CBP in 2026, including cases in which queries preceded immigration arrests.

Indeed, searches by ICE and CBP of Nlets/LEMS were so voluminous that when UWCHR researchers requested the number of queries made during monthlong periods, BCA public records personnel responded that the operation

was causing their antiquated computers to freeze up, forcing them to query the system merely hours at a time. In response, UWCHR researchers requested data from a single CBP ORI during the first two days of December 2025, January 2026, February 2026, and March 2026. The responses¹⁰⁷ are shown in Figure 9.

Number of Nlets queries of Minnesota driver and vehicle data made by the ORI VACBP1500, in the first two days of the months of: December 2025; January 2026; February 2026; and March 2026



Source: Minnesota Bureau of Criminal Apprehension (BCA), request R010163-032326

Figure 9: Number of queries made by the ORI VACBP1500, associated with Customs and Border Patrol, of Minnesota state driver and vehicle data via Nlets/LEMS increased significantly during the beginning of February 2026, likely reflecting the dramatic increase in ICE enforcement associated with Operation Metro Surge in early 2026.

¹⁰⁶ Interview of Pong Xiong, Director of Minnesota DVS, by Angelina Godoy, September 11, 2026. This relates to points made in the letter spearheaded by Sen. Ron Wyden (D-OR) in November 2025 (See Senator Ron Wyden (D-OR) et. al, Congressional letter to Democratic Governors regarding ICE access to DMV databases, 12 November 2025, <https://www.wyden.senate.gov/imo/media/doc/congressional-dmv-ice-letter-to-dem-governorspdf.pdf>), and subsequently reported in the media; see Raphael Satter, “Exclusive: Democratic-led States are Inadvertently Sharing Drivers’ Data with ICE, Officials Say,” *Reuters*, November 12, 2025, <https://www.reuters.com/world/democratic-led-states-are-inadvertently-sharing-drivers-data-with-ice-officials-2025-11-12/>; Reuters, “Exclusive-Democratic-Led States Are Inadvertently Sharing Drivers’ Data With ICE, Officials Say,” *USNews*, November 12, 2025, <https://www.usnews.com/news/politics/articles/2025-11-12/exclusive-democratic-led-states-are-inadvertently-sharing-drivers-data-with-ice-officials-say>; and Raphael Satter, “Only these four Democratic-led states aren’t sharing drivers’ data with ICE” *Independent*, November 12, 2025, <https://www.the-independent.com/news/world/americas/ice-democratic-states-protecting-drivers-license-data-b2864155.html>

¹⁰⁷ This data was obtained from MN BCA pursuant to request R010163-032326, which sought “the number of queries, via the BCA, of DVS databases made by the FBI-authorized originating agency identifier (ORI) of VACBP1500, in the months of: December 2025; January 2026; February 2026; and March 2026.” Upon learning of the IT challenges posed by this request, UWCHR researchers agreed to reduce the scope to the first two days of each month.

The variance in number of queries likely reflects the dramatic increase in ICE enforcement associated with Operation Metro Surge in early 2026.

UWCHR researchers also requested all registration queries performed via the Nlets/LEMS system on specific days; the records released in response show, for example, that on January 20, 2026, a total of 24,999 RQ (“registration query”) searches were performed via the Nlets/LEMS system. More than half of these queries were conducted by users associated with federal immigration enforcement agencies, logging in under 61 unique ORIs.¹⁰⁸

In at least seven cases confirmed to date, federal immigration agencies¹⁰⁹ used Nlets/LEMS to run license plate queries and obtain information which later led to immigration arrests of Minnesota drivers. These included the following:

108 However, just counting the number of queries can be misleading, since not every query is necessarily related to a civil immigration arrest on Minnesota streets; some may have been related to border crossings in Minnesota, or other legitimate functions performed by law enforcement agencies in Minnesota or elsewhere when encountering a car with Minnesota license plates. For this reason, quantitative measures are useful background, but the more significant findings are those that connect about specific queries prior to known immigration arrests.

109 UWCHR researchers also uncovered puzzling evidence that suggests, but does not confirm, possible local law enforcement collaboration in immigration enforcement. For example, on January 11, activists Brandon Siguenza and Patty O’Keefe were arrested by ICE; their arrest was not only captured on video, but also widely reported in the media because they were U.S. citizens whose arrest and subsequent eight-hour detention appear to form part of a pattern of intimidatory acts experienced by ICE watch observers during Operation Metro Surge. BCA records show that on the day of their arrest, the license plates of O’Keefe’s car were queried by the Minneapolis Police—and on subsequent days, by other law enforcement agencies, including the St. Paul Police Department, the Olmsted Sheriff Department of Rochester, and even more surprisingly, the Los Angeles Police Department. There is no logical reason why the LAPD would be querying O’Keefe’s plates, given that her car was located in Minneapolis; but recent reporting by the Minnesota Star Tribune has shown that many out-of-state law enforcement agencies played an active role in querying Minnesotans’ license plate data through cooperative access to its network of Flock cameras during the surge, so it is possible that they also performed searches via Nlets in support of federal immigration enforcement during the surge.

- On January 11, 2026, observers in Eagan, MN documented an arrest on the side of Yankee Doodle Road, posting videos that showed multiple cars boxing in a dark Toyota sedan, with ICE agents present. The incident was widely reported on social media in an attempt to inform the family of the unknown arrestee, whose car was left at the scene.¹¹⁰ The day of his arrest, BCA records show, the man’s license plate number was queried by CBP using Nlets/LEMS.
- On January 11, 2026, near Burnsville Parkway and Highway 13, a man was arrested driving a Chevrolet Avalanche; records show that his license plates were queried days earlier by CBP, and that the morning of his arrest, they were queried twice by agents from ICE using Nlets/LEMS.
- On January 12, 2026, a woman was dragged from her vehicle in a supermarket parking lot by masked men in vests marked “ICE”; she cried out loudly asking for mercy because she had three children at home. The arrest was captured on video and posted on social media. BCA records confirmed that the day of her arrest, her vehicle’s license plates were queried by CBP.
- On January 14, 2026, according to an affidavit filed in court by FBI officer Timothy Schanz, ICE deportation officers were “running publicly visible license plates through ICE databases” to determine the names of their registered owners at around 6 pm. Based on further database checks performed on the names they obtained, they chose to pull over the driver of one vehicle, who fled. BCA records released to UWCHR show that the car’s license plate was queried between 6 and 8 pm by ICE and CBP.

110 The Facebook video shows ICE agents questioning a man near a dark colored Toyota sedan on the shoulder of a road, reportedly Yankee Doodle Road in Eagan MN, on January 11, 2026, <https://www.facebook.com/share/v/1HdLPqk-wq1/>; this video and multiple additional posts (see [here](#) and [here](#)) indicate that the man was arrested and the car left behind in a parking lot of nearby Central Park Commons.

- On January 22, 2026, a man known as “Carlos” who worked cleaning Marshalls and HomeGoods stores was reportedly arrested by ICE in Eagan, MN, leaving his car behind in the Marshall’s parking lot; a coworker posted an image of the car to alert his family. Records show that the morning of his arrest, his license plate was queried in the Nlets/LEMS system by CBP.
- On May 6, 2026, community observers reported an arrest of a man driving a maroon GMC van with boards or drywall strapped to the top, near 28th and Oakland in Minneapolis; pictures of the vehicle were posted on multiple social media accounts. The arrest was also mentioned by Minneapolis City Council member Jason Chavez, who wrote, “This morning, a resident was stopped and kidnapped by ICE near 28th and Oakland Ave South.”¹¹¹ BCA records showed multiple queries made in the days before the arrest by two different Nlets/LEMS accounts associated with ICE.
- On August 18, 2026, a person was arrested in Yakima, Washington state, while driving a car with Minnesota license plates. Records from the BCA showed that a query was made on the car’s license plates that very morning by agents using a CBP ORI.

Of course, these arrests are likely only a fraction of the total number of immigration arrests following Nlets/LEMS queries of Minnesota’s DMV data.

Furthermore, there is evidence that license plate queries were used to obtain information about community observers of ICE activity—information that was then used to subject them to harassment and intimidation for

their Constitutionally-protected activities.¹¹² This illustrates how not only immigrants are vulnerable to the release of their personal data through these pathways—indeed, the same techniques can be, and are, used by federal and local law enforcement to surveil U.S. citizens without a warrant.¹¹³



**INDEED, THE SAME TECHNIQUES
CAN BE, AND ARE, USED BY
FEDERAL AND LOCAL LAW
ENFORCEMENT TO SURVEIL U.S.
CITIZENS WITHOUT A WARRANT.**

112 See Rachel Leingang and Maanvi Singh, “Minneapolis ICE Watchers Face Violence, Teargas and Arrests. They Keep Showing Up,” *The Guardian*, January 29, 2026, <https://www.theguardian.com/us-news/2026/jan/29/minneapolis-ice-observers>; Nina Moini, Aleesa Kuznetsov, Alanna Elder, and Ellen Finn, “‘I Was Flooded with Fear’: Minnesotans Describe Their Encounters with ICE, Being Detained,” *MPR News*, January 13, 2026, <https://www.mprnews.org/episode/2026/01/13/minnesotans-describe-their-encounters-with-ice-agents>; Spencer Ackerman, “ICE Tried To Turn This Minneapolis Teacher Into An Informant,” *Forever Wars*, March 12, 2026, <https://www.forever-wars.com/ice-tried-to-turn-this-minneapolis-teacher-into-an-informant/>; Kat Lonsdorf, Jude Joffe-Block, and Meg Anderson, “ICE Has Spun a Massive Surveillance Web. We Talked to People Caught In It,” *NPR*, March 5, 2026, <https://www.npr.org/2026/03/04/nx-s1-5717031/ice-dhs-immigrants-surveillance-confrontation-deportation-mobile-fortify>; and Austin Campbell, “Federal Agents are Intimidating Legal Observers at Their Homes: ‘They Know Where You Live,’” *The Intercept*, March 5, 2026, <https://theintercept.com/2026/03/05/ice-cbp-minnesota-surveillance-intimidation-observers/>

113 The biennial publication, Minnesota Department of Public Safety, Driver and Vehicle Services, *MNDRIVE Systems Audit Report 2025*, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/DVS_Information_System_-_Biennial_Audit.pdf, makes reference to multiple disciplinary actions taken in reactions to cases of misuse of the MNDRIVE database; in an interview, Pong Xiong noted that most of these were cases of unauthorized “browsing” of individuals’ data for personal reasons (interview with Angelina Godoy, September 11, 2026). This is similar to commonly-found unauthorized uses of other types of databases containing personal information; see, for example, Erin Hale, “Flock Adds Safeguards to Licence-plate Readers After Wave of Stalking Cases,” *Al Jazeera*, August 14, 2026, <https://www.aljazeera.com/news/2026/8/14/flock-adds-safeguards-to-licence-plate-readers-after-wave-of-stalking-cases>

111 See Jason Chavez - Minneapolis Ward 9’s Facebook post, May 6, 2026 <https://www.facebook.com/share/p/1Dc-qMdjeP8/>

Certification of Use and Disclosure of Certain Data

CERTIFICATION:

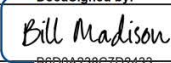
The Purchaser and customers of the Purchaser who access DVS Data must not use noncompliant (a credential that does not meet the REAL ID Act) driver's license or identification card data for civil immigration enforcement purposes or disclose any of the data to a state or federal government entity that primarily enforces immigration law or to any employee or agent of any such government entity. Such entities include but are not limited to: U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Patrol (CBP), U.S. Citizenship and Immigration Services (USCIS), and U.S. Homeland Security (DHS).

Pursuant to Minn. Stat. § 171.12, subd. 7b, if the data purchaser violates this certification, the data purchaser may be liable in a civil action brought under Minn. Stat. § 13.08, may be subject to criminal penalties under Minn. Stat. § 13.09, may have subsequent requests for noncompliant driver's license or identification card data be denied by the commissioner, and may permanently lose access to DVS Data.

By signing this certification, the data purchaser agrees to the terms of the certification and will be held responsible for the compliance of any user of the data.

Name: Bill Madison

Title: CEO Insurance Solutions

Signature: 
8000A230C7D2433...

Date: 6/5/2025

Figure 10: A certification provided by LexisNexis Risk Solutions Inc. to the state of Minnesota guaranteeing compliance with Minnesota state data sharing laws regarding DVS data's use for federal immigration enforcement purposes, obtained by UWCHR under public records law.

4. Indirect access by ICE to DVS data through data brokers

Minnesota also has active contracts with over a dozen data brokers,¹¹⁴ including LexisNexis and Experian, who as stated above, are known to sell data, directly and/or indirectly, to ICE. These contracts specify that the state of Minnesota transmits updated data every day to R.L. Polk, LexisNexis, Experian, and Driver's History Information Sales,¹¹⁵ every week to Penn Credit Corporation and Passport Labs; and once a month to Landmark Media Enterprises.

Minnesota's contracts with data brokers specifically prohibit them from disclosing driver's license data "to a state or federal government entity that primarily enforces immigration law." They task each data broker with "ensur[ing] that authorized users accessing DVS data will not use noncompliant (credential that does not meet the REAL ID Act requirements) driver's license or identification card data for civil immigration enforcement purposes or disclose the data "to a state or federal government entity that primarily enforces immigration law."¹¹⁶ In addition, Minnesota requires all data

¹¹⁴ UWCHR obtained contracts between the DVS and Driver's History Information Sales LLC; Experian Information Solutions Inc.; Explore Information Services, LLC; Landmark Media Enterprise d/b/a Cross Sell LLC; LexisNexis Risk Solutions, Inc.; Passport Labs, Inc.; Penn Credit Corporation; R. L. Polk; Safety Holdings Inc.; Tessera Data, Inc.; and Verisk Analytics Business.

¹¹⁵ Per the Contract Number 251295, Driver's History Information Sales LLC is a fully-owned subsidiary of the national credit bureau TransUnion, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/DVS_Drivers_History_Information_Income_Contract_251295.pdf.

¹¹⁶ This language appears on Experian's Contract Number 253642, p. 4-5, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/DVS-Experian_Income_Contract_253642.pdf; Polk's Contract Number 253635, p. 4-5, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/DVS-RL_Polk_Income_Contract_253635.pdf; and LexisNexis' Contract Number 253607, p. 4-5, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/LexisNexis-DVS_RPK_253607.pdf. The same language also appears in Appendix A to LexisNexis' Contract Number 253607, p. 11: "Authorized users must not use noncompliant (credential that does not meet the REAL

brokers to sign a certification indicating that it will not disclose any of the data purchased to “a state or federal government entity that primarily enforces immigration law.” Below, for example, is the certification provided by LexisNexis Risk Solutions Inc. This is the same branch of LexisNexis which, according to federal procurement data, contracts with ICE.¹¹⁷

While LexisNexis claims here that it does not sell Minnesota DVS data to ICE, on its website, LexisNexis does advertise Minnesota among the states for which it has access to “information about individuals or corporations who have registered or titled motor vehicles with a state motor vehicle registration agency.”¹¹⁸ One of the products referenced in ICE’s contract with LexisNexis is Accurint,¹¹⁹ which advertises on its own website that includes Real-Time Motor Vehicle Registration Search.¹²⁰

It is, of course, theoretically possible that LexisNexis makes Minnesota DVS data available to other purchasers of Accurint, but not to ICE,

and that the above certification is therefore accurate. But given the aforementioned clauses in LexisNexis’ contract with ICE making it impossible to know which data is searched by ICE, it would be at least difficult, and perhaps impossible, to verify that this is true.

The state of Minnesota’s contracts with data brokers do require that the companies submit to annual third-party audits, and submit copies of the audit report to DVS and the Office of the Legislative Auditor;¹²¹ they also require that data brokers provide the state of Minnesota with a list of parties to whom they sold DVS data each year.¹²² But when UWCHR sought a copy of the audit reports and customer data, we were told that this information was “nonpublic trade secret data.”¹²³

ID Act) driver’s license or identification card data for civil immigration enforcement purposes or disclose the data to a state or federal government entity that primarily enforces immigration law or to any employee or agent of any such government entity. If the authorized user violates this certification, they may be liable in a civil action brought under Minnesota Statutes, section 13.08, may be subject to criminal penalties under Minnesota Statutes, section 13.09, and may have subsequent requests for noncompliant driver’s license or identification card data be denied by the Commissioner.”

117 See, for example, Department of Homeland Security, *Contract Number 70CMSD21C00000001 with LexisNexis Risk Solutions Inc*, USA Spending, https://www.usaspending.gov/award/CONT_AWD_70CMSD21C00000001_7012_-NONE_-NONE- showing a contract for nearly \$25 million

118 See “Motor Vehicle Registrations Source,” LexisNexis® Risk Management Solutions Help, https://riskmanagement.lexisnexis.com/bps/web20_help/RSKM/bsp_source_motor_vehicle_registrations_r.html

119 See “Law Enforcement Investigative Database Subscription,” Higher Gov, <https://www.highergov.com/contract-opportunity/law-enforcement-investigative-database-subscriptio-192126flmurq0071-s-cf1a7/>

120 See “Real-Time Motor Vehicle Registration Search,” Accurint, https://www.accurint.com/help/ln/real-timeMVR_help.html.

121 The language is included in sections 10.3-10.4 of the data brokers’ contracts: “Under Minnesota Statutes § 168.327, subdivision 6, the Purchaser must annually engage an independent third party to audit its uses of bulk data and its information technology security procedures, including: (1) the methods and practices employed in the processing methods and use of driver and vehicle services data; (2) compliance with the certification required under Minnesota Statutes § 171.12, subdivision 7b, paragraph (d), and address any material deficiencies. Under Minnesota Statutes § 168.327, subdivision 6, the Purchaser must submit a copy of the independent third-party report to DVS and the Office of Legislative Auditor within 30 days of completion. Completion date is defined as the date the audit report signed by the independent third party. The report must include a certification that DVS Data is being protected as required by Minnesota Statutes section 171.12, subdivision 7b.” See, for example, Minnesota’s LexisNexis *Contract Number 253607*, p.5.

122 Section 10.5 of the contracts read “10.5. Each February, the Purchaser must provide the State with an updated list of each person or entity that received DVS Data from the Purchaser and the permissible use of each person or entity.” See, for example, Minnesota’s LexisNexis *Contract Number 253607*, p.5.

123 Driver and Vehicle Services MN Department of Public Safety, email to Professor Angelina Godoy, July 30, 2026, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/UW-Mail-Records-Center-DRIVER-AND-VEHICLE-SERVICES--R002958-072226-blurred.pdf>

NEW YORK

State Nlets administrator, State access point for Nlets	State DMV, Year drivers' licenses made available to noncitizens	State laws limiting data sharing for immigration enforcement purposes	 DMV-to-DHS pipeline pathways
New York State Police, New York Statewide Police Information Network (NYSPIN)	New York Department of Motor Vehicles (DMV), 2019	2019 Green Light Law	Direct access by federal agencies to NY DMV database: UWCHR research did not find evidence that this pathway is open. DHS searches of NY DMV data via Nlets: UWCHR research did not find evidence that this pathway is currently open for cars with NY license plates. Access via data brokers: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation. Access via state/local law enforcement: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation.

WHAT THE LAW SAYS

New York has enacted what is widely regarded as one of the most restrictive state level frameworks in the country for the use of DMV data for immigration enforcement. The core legislation is the Driver's License Access and Privacy Act (known as the "Green Light Law"), which stipulates that:

- The New York DMV is barred from sharing records¹²⁴ "to any agency that primarily

enforces immigration law or to any employee or agent of such agency" unless presented with a lawful court order or judicial warrant signed by an Article III judge.¹²⁵ Further, all parties who have access

attended, source of income, status as a recipient of public benefits, the customer identification number associated with a public utilities account, [and] medical information or disability information." See Complaint ¶ 31, *United States v. State of New York et al.*, No. 1:25-CV-0205 (N.D.N.Y. Feb. 12, 2025), <https://www.justice.gov/opa/media/1389406/dl> (quoting N.Y. Veh. & Traf. Law § 201(8)).

¹²⁵ N.Y. Veh. & Traf. Law § 201(12)(a), added by 2019 N.Y. Laws ch. 37. The stipulation that the warrant be signed by a judge appointed under Article III of the U.S. Constitution excludes not only the "administrative warrants" which ICE/CBP issue themselves, but also any order of an immigration court judge, since immigration courts are part of the executive, rather than the judicial, branch and therefore not

¹²⁴ The category of "records" protected here is expansive. As described in the federal government's complaint in *U.S. v. New York*, the "DMV 'records or information' covered by this provision include a person's 'photo image, . . . social security number, telephone number, place of birth, country of origin, place of employment, school or educational institution

to DMV data—this includes, but is not limited to, local or state law enforcement—are also barred from sharing DMV data with federal immigration agencies.¹²⁶

- In cases where an immigration agency *does* present a warrant, allowing them to access a New Yorker's information in the custody of the DMV, the DMV is required to notify the individual whose records were sought within three days; this notification includes identifying the agency that sought their information.¹²⁷
- New York also requires all data brokers purchasing DMV data to certify that they will not disclose that data to federal immigration agencies.¹²⁸
- An amendment introduced in 2020 strengthened the original law's information sharing prohibitions by making violations a class E felony.¹²⁹

While the federal government attempted a constitutional challenge against the New York Green Light Law, the lawsuit was dismissed with prejudice in December 2025.¹³⁰

New York implemented the Green Light Law by blocking Nlets queries from ORI numbers associated with ICE ERO, ICE HSI, and CBP from accessing New York DMV drivers' licenses and vehicle data; as a result of these blocks,

when agents from these agencies attempted to query Nlets via NYPSIN, they received a message indicating they were no longer able to access those records.¹³¹ The federal government retaliated by suspending New Yorkers' access to trusted traveler programs such as Global Entry, and filed suit against the state.¹³² In April 2020, New York introduced amendments to the Green Light Law, allowing for information-sharing of DMV records "as necessary for an individual seeking acceptance into a trusted traveler program," but the core restrictions on data-sharing remained in place; in the words of CBP Deputy Commissioner Robert Perez, "the law continues to prevent CBP from accessing, using or sharing DMV records for other important mission-related purposes, including... verifying the identity of a vehicle's owner before a traffic stop."¹³³

WHAT'S HAPPENING ON THE ROADS

Despite these strong prohibitions on data-sharing, however, ICE/CBP traffic stops are a frequent¹³⁴ practice across New York; they are particularly pronounced in Latino communities on Long Island and Staten Island,¹³⁵ but court documents show they occur in central and

independent.

126 N.Y. Veh. & Traf. Law § 201(12)(b), added by 2019 N.Y. Laws ch. 37.

127 N.Y. Veh. & Traf. Law § 201(12)(a)

128 New York Vehicle & Traffic Code, Ch. 71, Title 2, Art. 2, §201 at 12(b).

129 Rebecca C. Lewis, "DMV Defends Green Light Law Meant to Protect Immigrants," *City & State New York*, January 7, 2025, <https://www.cityandstateny.com/policy/2025/01/dmv-defends-green-light-law-meant-protect-immigrants/401979/>.

130 *United States v. State of New York et al.*, No. 1:25-CV-0205 (N.D.Nnon-commercial driver's.Y.), Order on Mot. to Dismiss (Dec. 23, 2025); see Civil Rights Litigation Clearinghouse, case summary at <https://clearinghouse.net/case/46112/>.

131 Complaint ¶ 30, *United States v. New York*, No. 1:25-CV-0205.

132 See "DHS Lifts Ban on Trusted Traveler Programs for New York Residents," *American Immigration Lawyers Association*, July 23, 2020, <https://www.aila.org/library/dhs-suspends-enrollments-renewals-in-cbp-trusted>; Complaint ¶ 30, *United States v. New York*, No. 1:25-CV-0205.

133 See Department of Homeland Security, *Robert E. Perez testimony on "Examining DHS' Management of Trusted Traveler Programs"*, September 30, 2020, <https://democrats-homeland.house.gov/imo/media/doc/Testimony%20-%20Perez.pdf>

134 While ICE arrests in the New York City immigration court at 26 Federal Plaza have attracted great attention in the media, researchers from The City have found that street arrests have actually been far more common in the NY metro area, though the fact that they are happening in so many sites, and take place so quickly, makes them harder to track and witness. See Gwynne Hogan, Rosalind Adams, and Haidee Chu "We Found 430 ICE Street Arrests in the New York Area. More Than 93% Targeted Latinos." *The City Reporter*, May 27, 2026, <https://projects.thecity.nyc/ice-street-arrests-investigation-racial-profiling/>

135 *Ibid.*

upstate New York as well.¹³⁶ While the practice is common, UWCHR researchers did *not* find any evidence that the New York's DMV was facilitating the practice by sharing data. Indeed, New York's "Green Light law"¹³⁷ banning this practice would appear to be largely upheld in practice.



UWCHR RESEARCHERS DID NOT FIND ANY EVIDENCE THAT THE NEW YORK'S DMV WAS FACILITATING THE PRACTICE BY SHARING DATA. INDEED, NEW YORK'S "GREEN LIGHT LAW" BANNING THIS PRACTICE WOULD APPEAR TO BE LARGELY UPHOLD IN PRACTICE.

1. Direct access by federal agencies to the NY DMV

The NY DMV, like its counterparts in the other states examined, offers direct access to its database for contract sales, pay-per-search, and over-the-counter functionalities; the agency reaps approximately \$58 million

per year from these services, a larger sum than that garnered from the sale of data to data brokers.¹³⁸ According to the agency's website, the DMV collects approximately \$58 million per year from pay-per-search sales.¹³⁹ UWCHR obtained a list of all subscribers to these services;¹⁴⁰ they did not include federal immigration enforcement agencies, though some data brokers like LexisNexis, who in turn sell data to such agencies, do appear on the list.

2. ICE/CBP searches of Nlets/NYSPIN

In New York, the State Police operate the New York Statewide Police Information Network (NYSPIN) as the Nlets interface through which local, state, and national law enforcement agencies can query DMV data. New York officials have stated that they have blocked ICE/CBP's access to DMV data via Nlets/NYSPIN, and data gathered by UWCHR researchers appear to corroborate this assertion.

In New York, ICE/CBP still carry out traffic stop arrests, but somewhat differently. For cars *with out-of-state license plates*, there is evidence that ICE/CBP routinely query the state DMVs of those cars' home states to obtain driver and vehicle data. Researchers from *Newsday* in Long Island identified 84 traffic arrests in Long Island between January 20, 2025, and June 30, 2026, and analyzed court proceedings stemming from those cases, noting that "In sworn statements and court transcripts, agents repeatedly describe running out-of-state

136 See, for example, Document 21-11 filed in Case 2:26-cv-02082-SJB-JMW by the Worker's Center of Central New York.

137 The core legislation is the Driver's License Access and Privacy Act (Known as the "Green Light Law"), enacted in June 2019 as Chapter 37 of the laws of 2019 and codified within the N.Y. Vehicle and Traffic Law (VTL) § 201, subdivisions 8-12 N.Y. Veh. & Traf. Law § 201(8)-(12), added by 2019 N.Y. Laws ch. 37 (S1747-B), signed June 17, 2019, eff. Dec. 14, 2019. Full bill text available at: <https://legislation.nysenate.gov/pdf/bills/2019/S1747B>. A 2020 amendment sharpened the law's teeth by elevating disclosure of information to a class E Felony. See 2020 N.Y. Laws (budget amendment), amending N.Y. Veh. & Traf. Law § 201(12)(b); see also Rebecca C. Lewis, "DMV Defends Green Light Law Meant to Protect Immigrants" *City & State New York*, January 7, 2025 <https://www.cityandstateny.com/policy/2025/01/dmv-defends-green-light-law-meant-protect-immigrants/401979/>. Although the federal government filed suit against New York over the passage of this law, the case was dismissed with prejudice in December 2025. (*United States v. State of New York et al.*, No. 1:25-CV-0205 (N.D.N.Y.), Order on Mot. to Dismiss (Dec. 23, 2025); see Civil Rights Litigation Clearinghouse, case summary at <https://clearinghouse.net/case/46112/>.)

138 See "Sharing License and Registration Information," Department of Motor Vehicles, New York State <https://dmv.ny.gov/records/sharing-your-information>.

139 Ibid. The only stated limitation on use is DPPA: "Anyone who accesses DMV information must comply with the federal Driver's Privacy Protection Act (DPPA) <https://dmv.ny.gov/node/5281>. The DPPA was enacted by Congress after a careful debate about why states should be allowed to share DMV data. The DPPA prohibits states from disclosing a driver's personal information to anyone who does not have what the DPPA considers a permissible use. The DPPA defines "personal information" as an individual's photograph, social security number, driver identification number, name, address, telephone number, and medical information."

140 These lists were provided to UWCHR by the New York DMV pursuant to request # R001528-060826.

license plates of cars to get the registrant's name and then putting that name into federal immigration databases to determine the person's legal status in the country."¹⁴¹ The case of Luis, an Ecuadorian arrested while sitting in his car outside a Walmart in Deer Park, would appear to provide an example; his car had Virginia license plates.¹⁴² In another case, a man and his wife driving a car with Florida license plates were apprehended in a Walmart parking lot near Buffalo.¹⁴³

By reviewing declarations¹⁴⁴ and sworn testimony¹⁴⁵ by federal agents in New York

courts, UWCHR researchers found that, by contrast, when ICE/CBP officers conducted traffic stops of cars *with New York plates*, they described a process of not knowing the drivers' names in advance; after pulling the car over, agents would ask for the driver's ID and then run the driver's name against other records. This description is echoed in the accounts offered by drivers themselves.¹⁴⁶ This differs from accounts in all the other states examined, where a frequent feature of the aggressive "jump out" traffic stop is that from the beginning of the encounter, federal agents already know the name of the vehicle's owner, have run it against other databases to discern the person's immigration status, and have already made the decision to arrest the driver.

Relatedly, UWCHR researchers submitted records requests of all Nlets/NYSPIN queries made on multiple vehicles with New York plates which subsequently experienced an ICE/CBP arrest; in the three cases for which we have, to date, received records,¹⁴⁷ no queries by federal agents were made prior to the arrest, although records did show other queries by local agencies.¹⁴⁸

141 See Josefa Velásquez and Arielle Martinez, "ICE is arresting immigrants on Long Island by surveilling parking lots and running license plates," *Newsday*, July 23, 2026, <https://www.newsday.com/long-island/investigations/ice-immigration-traffic-stops-license-plates-eq5xhbw3>

142 Ibid. Because Virginia does not consider records of law enforcement queries to be public records, UWCHR researchers are unable to verify that a search was performed on the vehicle's plates prior to the couple's arrest.

143 See Declaration of F.R.P., No. 2:26-cv-02082-SJB-JMW, Doc. 21-10 (E.D.N.Y. April 13, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/declaration-re-conditions-in-Batavia.pdf>. Because Florida does not consider records of law enforcement queries to be public records, UWCHR researchers are unable to verify that a search was performed on Luis' plates prior to his arrest.

144 See Declaration of Deportation Officer, Kareem Biggs, in *Parada Cruz, Erik Sigfredo v. Noem*, et. al., No. 2:26-cv-01110-SJB, Doc. 5-1 (E.D.N.Y. February 27, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/ICE-officer-Biggs-describing-detention-on-vehicle-stop-NY.pdf>; and Declaration of Detention and Deportation Officer, Geraldo Paoli, Rene Antonio Benitez v. Kenneth Genalo, et. al., No. 2:26-cv-01122-SJB, Doc. 6-1 (E.D.N.Y. February 27, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/ICE-declaration-in-Benitez-case.pdf>; also Petition for Writ Habeas Corpus *Ivan Alexander Castro Escobar v. Mark Wayne Mullin, Todd M. Lyons, Kenneth Genalo, and Raul Maldonado Jr.*, No. 2:26-cv-01795-SJB, Doc. 1 (E.D.N.Y. March 26, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/Case-2-26-cv-01795-SJB-traffic-stop-NY-no-plate-search.pdf>, which includes on p. 6, "Upon information and belief, the Petitioner was detained by DHS agents after a vehicle stop. Upon information and belief, the arresting officers were not aware of the Petitioner's identity or immigration status prior to conducting the roadside stop."

145 For example, three different ICE officers in *William Enrique Sanchez Alfaro v. Almodovar*, et. al., No. 2:26-cv-00766-GRB, Doc. 20 (E.D.N.Y. April 7, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/sworn-testimony-in-Alfaro-case-no-plates.pdf>, describe the process of apprehending the driver of a vehicle they initially approached at a gas station: agents asked for the IDs of the driver and all occupants of the vehicle, then contacted other agents by telephone who ran "records checks" on those

individuals and then reported back to the agents on the scene instructing them to take the driver into custody. The records checks performed were for the individual's immigration history once his name was known because he provided his ID; this information was not obtained through queries of his vehicle.

146 See for example, in the Declaration of Alejandro Vera Angel, No. 2:26-cv-02082-SJB-JMW, Doc. 21-20 (E.D.N.Y. April 13, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/declaration-in-Benitez-case-car-boxed-in.pdf>; and in the Declaration of Maria Pacheco Vasquez, No. 2:26-cv-02082-SJB-JMW, Doc. 21-26 (E.D.N.Y. April 13, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/declaration-in-Benitez-case-Batavia.pdf>.

147 Unfortunately, New York responses to FOIA requests filed by UWCHR researchers have been extremely inconsistent; in multiple cases, requests were denied as impermissible under the Federal Driver Privacy Protection Act, even though in other similar requests, the information was provided. Six additional cases remain pending, in which the New York State Police have told UWCHR to expect a response by December 11, 2026; the requests were initially filed in May 2026.

148 For example, local responders reported the arrest of a driver of a bright blue Honda Civic in the parking lot of Bravo Supermarket in Hempstead, New York, on June 3, 2026

To be clear, the point here is not that cars with New York license plates were not subjected to ICE abuses; in fact, federal courts have found ICE's practice of warrantless arrests to be illegal regardless of what state the car's plates were from,¹⁴⁹ and have ordered the agency to stop the practice.¹⁵⁰ However, it appears that ICE officers are not able to obtain DMV data about cars registered in New York via Nlets/NYSPIN, and therefore unable to incorporate it in statements of "reasonable suspicion" used to justify traffic stop arrests; this distinguishes New York from Washington, Maryland, and Minnesota.

3. Access by federal agencies to the NY DMV via data brokers

According to data provided by the New York DMV to UWCHR, the agency only sells its data to two data brokers, Polk and Experian. Experian has a current contract with ICE's HSI division,¹⁵¹ and is known to sell data to Thomson Reuters; and Polk has sold data to Thomson-Reuters, a key source of data for ICE, in the past.¹⁵²

at 7:18 am; records indicate that a search was performed on the car's plates afterward by Nassau County parking authorities presumably indicating the car was left behind at the scene.

149 Based on a pattern of traffic-stop cases coming before his court, Judge Sanket Bulsara wrote, "This practice of after-the-fact arrest warrants can be called many things—illegal, improper, and unconstitutional, among them. But whatever label one wishes to apply, the practice is fundamentally at odds with and offensive to lawful, constitutional behavior in this country...Police and law enforcement cannot operate as roving bands, detaining individuals, figuring out the reasons later, and papering over their failures afterwards". See Erik Sigfredo Parada Cruz v. Markwayne Mullin, et al., no. 26-CV-1110-SJB and Rene Antonio Benitez v. Kenneth Genalo, et al., No. 26-CV-1122-SJB, (E.D.N.Y. April 16, 2026), <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/NY-judge-against-traffic-stops-gov.uscourts.nyed.542454.14.0.pdf>.

150 Judging by the data, however, the order issued April 16, 2026, does not appear to have stopped the arrests via traffic stop; data available to UWCHR does not permit researchers to ascertain whether the large number of ongoing traffic stops are now being performed with warrants.

151 See Department of Homeland Security, *Contract 70CMSD23P00000139 Experian Support Services*, webpage last modified 8/26/26, <https://www.highergov.com/contract/70CMSD23P00000139/>; under FOIA, UWCHR has requested the contract and is awaiting response.

152 See McKenzie Funk, "How ICE Picks its Targets in the Surveillance Age," *The New York Times Magazine*, October 2, 2019, <https://www.nytimes.com/2019/10/02/magazine/>

Language in both contracts suggest that selling their data to ICE or Thomson-Reuters would violate the terms of the contract. For example, on p. 3, the contracts read, "Contractor shall not divulge license plate numbers acquired from the Dept to any entity other than the NHTSA [National Highway Traffic Safety Administration]... license plate numbers may only be used for the following purposes (i) issuance of manufacturer's warranty, safety recall or similar notice; or (ii) statistical compilations." And on p. 4, the contracts bar redisclosure to third parties for purposes other than those aforementioned.

As the New York DMV explains, "In accordance with the federal DPPA and New York State law, DMV sells registration and vehicle data through an open procurement process every two years. The successful bidders cannot use DMV information for any purposes other than those in connection with the issuance of a manufacturer's warranty, safety recall, or similar notices – important things that keep the public safe. The data can be used for statistical compilations and analysis, which do not contain any personal, identifying information."¹⁵³

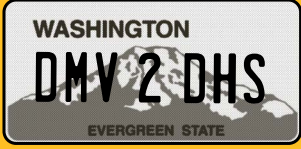
However, the contracts do not mention any requirement to submit to independent auditing, and indeed, it appears that no state audits have been undertaken to ensure compliance with these terms.¹⁵⁴

[ice-surveillance-deportation.html](#)

153 From "Sharing License and Registration Information," Department of Motor Vehicles, New York State <https://dmv.ny.gov/records/sharing-your-information>.

154 In request R001546-060926, filed June 9, 2026, UWCHR requested copies of the most recent audit reports performed to ensure compliance with the Polk and Experian contracts; the NY DMV responded that no such records existed.

WASHINGTON

State Nlets administrator, State access point for Nlets	State DMV, Year drivers' licenses made available to noncitizens	State laws limiting data sharing for immigration enforcement purposes	 DMV-to-DHS pipeline pathways
Washington State Patrol (WSP), A Central Computerized Enforcement Service System (ACCESS)	Department of Licensing (DOL), 1993	2019 Keep Washington Working	Direct access by federal agencies to DOL database: This pathway was open as recently as mid-2025, but subsequent UWCHR research did not reveal evidence that this pathway has been open since. DHS searches of DOL data via Nlets: Evidence reveals that this pathway is currently open. Access via data brokers: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation. Access via state/local law enforcement: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation.

WHAT THE LAW SAYS

As noted above, Washington began issuing drivers' licenses to qualified noncitizens as far back as 1993, but did not move to protect immigrant drivers' data from civil immigration enforcement until 2017, when then-Governor Jay Inslee issued an Executive Order mandating that "No executive or small cabinet agency may use agency or department monies, facilities, property, equipment, or personnel for the purpose of targeting or apprehending persons for violation of federal civil immigration laws, except as required by federal or state law or otherwise authorized

by the Governor."¹⁵⁵ This was expanded in 2019 with the passage of the state's "sanctuary" law, Keep Washington Working. These prohibitions apply to the Washington's DMV (known locally as the Department of Licensing, or DOL) as well as to most other state agencies,¹⁵⁶ but the law establishing them does not contain specific enforcement mechanisms.

155 State of Washington, Office of the Governor, Executive Order 17-01 (Jan. 23, 2017): https://governor.wa.gov/sites/default/files/exe_order/EO_17-01.pdf

156 The Department of Corrections was specifically carved out of this legislation, allowing it to continue sharing information with ICE/CBP for purposes of immigration enforcement.

Specifically, Washington law states that:

- The Keep Washington Working Act of 2019 (KWW) prohibits state agencies from using their resources to assist in civil immigration enforcement unless required by a court order. The law “prohibits the use of state or local government “funds, facilities, property, equipment, or personnel to investigate, enforce, cooperate with, or assist in the investigation or enforcement of any federal registration or surveillance programs or any other laws, rules, or policies that target Washington residents solely on the basis of race, religion, immigration, or citizenship status, or national or ethnic origin.”¹⁵⁷
- KWW’s restrictions apply not only to the Department of Licensing, but also to law enforcement. As the office of the Washington Attorney General’s published guidance explains, “KWW prohibits local LEAs from providing any ‘nonpublicly available personal information’ about any person (including those subject to community custody) to federal immigration authorities in a noncriminal matter—such as a civil immigration matter—except as otherwise required by state or federal law or a lawfully issued court order.” The name and address of a vehicle’s registered owner clearly constitute nonpublicly available information.

In addition, the Washington DOL incorporated permissible use restrictions that clearly bar the sharing of DOL data for purposes of immigration enforcement in its contracts with the Washington State Patrol, which administers the Nlets platform known as ACCESS, as well as with private data brokers. For example:

- Under the terms of the data licensing

agreement between DOL and WSP, the use of DOL data for civil immigration enforcement—by the WSP or the subrecipients with whom the WSP shares DOL data—is “explicitly prohibited without limitation.”¹⁵⁸ The WSP User Agreement currently in use¹⁵⁹ specifies that, “To comply with KWW, no criminal justice agency shall use or share ACCESS, or any information obtained through ACCESS, to support or engage in immigration enforcement activities. The prohibition on information sharing includes place of birth, present location, release date from detention, if applicable, and family members’ names, absent a court order, judicial warrant, or as may be required by the Public Records Act (PRA), chapter 42.56 RCW. Incidents of disclosure of such personal information shall be considered a breach of this agreement.”¹⁶⁰

- The contracts between Washington’s DMV and data brokers include strict limitations on the use of the data for immigration enforcement, either by the data broker

158 The most recent version of this agreement was signed in October 2022, with an amendment extending the end date to 10/31/28 (See Washington Department of Licensing, *Data Licensing Agreement Between Department of Licensing and Washington State Patrol DOL Contract No. K7798/WSP Contract No. K18262*, October 28, 2022, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/K18262-DOL_Data_Sharing-Executed_reprint.pdf; and Washington Department of Licensing, *Data Licensing Agreement Amendment Between Department of Licensing and Washington State Patrol DOL Contract No. K7798 Amendment No. 03/WSP Contract No. K18262-7*, October 3, 2025, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/K18262-7-DOL-EXE_reprint.pdf.) The amendment stipulates on p.2 that “In accordance with RCW 43.17.425 and Washington Executive Order 17-01, Recipient and Subrecipients are explicitly prohibited without limitation against sharing or using Data, including Protected Personal Information, for purposes of investigating, enforcing, cooperating with, or assisting in the investigation or enforcement of any federal or state regulation or surveillance programs or any other laws, rules, or policies that target Washington residents solely on the basis of race, religion, immigration, or citizenship status, or national or ethnic origin.”

159 Last updated in 2023, See Washington State Patrol, *2023 User Acknowledgement*, 2023, https://wsp.wa.gov/access/forms/attachment/access_user_acknowledgment/

160 Washington State Patrol, *2023 User Acknowledgement*, p. 3.

157 See Wash. Rev. Code § 43.17.425., Immigration and citizenship status—State agency restrictions: <https://app.leg.wa.gov/RCW/default.aspx?cite=43.17.425>

or other parties with whom the data broker shares Washingtonians' DMV data, stating specifically "In accordance with RCW 43.17.425 and Washington Executive Order 17-01, Recipient and Subrecipients are explicitly prohibited without limitation against sharing or using Data, including Protected Personal Information, for purposes of investigating, enforcing, cooperating with, or assisting in the investigation or enforcement of any federal or state regulation or surveillance programs or any other laws, rules, or policies that target Washington residents solely on the basis of race, religion, immigration, or citizenship status, or national or ethnic origin." The contracts also require regular audits for both data security and permissible use.

Despite these prohibitions, however, Washington's DMV has been repeatedly exposed as failing to uphold the law and allowing data to flow to DHS along at least two of the four pathways¹⁶¹ enumerated in this report.

WHAT'S HAPPENING ON THE ROADS

1. Direct access by federal agencies to the WA DOL database

Washington's DOL has two "self-service lookup services" that provide various governmental bodies access to its database: [Driver and Plate Search](#) (DAPS), which is available to a range of law enforcement and government agencies, and Driver Information and Adjudication System (DIAS), which provides access to the courts.¹⁶²

¹⁶¹ Indeed, in 2018 WA DOL also shared data in a fifth possible way: over email in direct response to requests from ICE. See Nina Shapiro, "Washington state regularly gives drivers' info to immigration authorities; Inslee orders temporary halt," *The Seattle Times*, January 11, 2018, <https://www.seattletimes.com/seattle-news/times-watchdog/washington-state-regularly-gives-drivers-info-to-immigration-authorities-inslee-orders-temporary-halt/>.

¹⁶² See Washington Department of Licensing, "Driver



**WASHINGTON'S DMV HAS BEEN
REPEATEDLY EXPOSED AS
FAILING TO UPHOLD THE LAW AND
ALLOWING DATA TO FLOW TO DHS**

In 2018, the DOL acknowledged that ICE and CBP were able to freely search records in the DAPS database; audit logs revealed that from 2016 to 2018, ICE Enforcement and Removal Operations (ERO) had searched the DOL's DAPS database more than 100,000 times.¹⁶³ At the time, the DOL sought to address concerns by terminating DAPS contracts with four DHS subagencies, and updating the permissible use clauses included in all DAPS contracts to expressly prohibit the use of the database "for purposes of investigating, locating, or apprehending individuals for immigration related violations."¹⁶⁴ Yet the problem arose again in 2025, when *KING 5* broke the news that the DOL had quietly reinstated DAPS access for federal agents, who had once again mined the database for information that led to civil immigration arrests.¹⁶⁵ In reaction, the governor's office took additional steps to terminate DAPS accounts held by ICE and

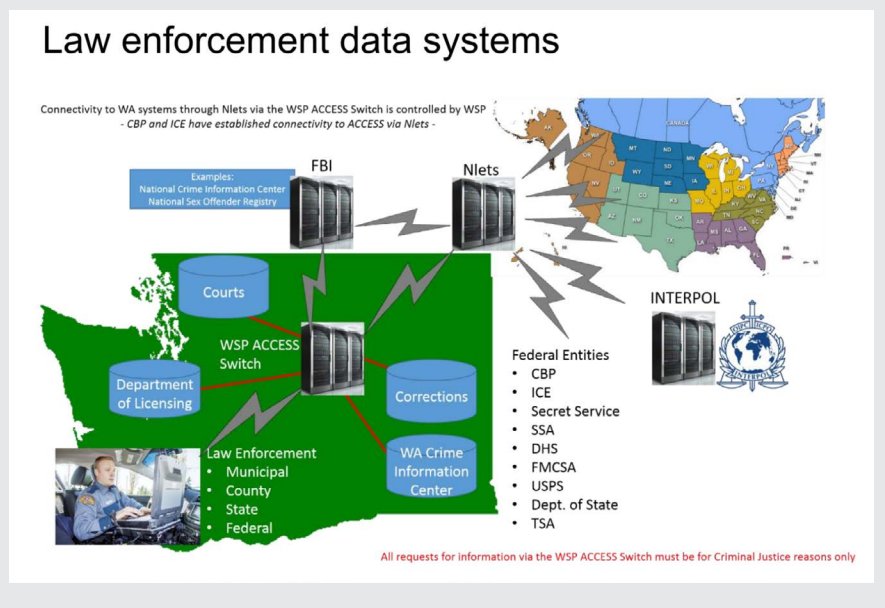
and Plate Search and Driver Information and Adjudication System," <https://dol.wa.gov/driver-and-plate-search-and-driver-information-and-adjudication-system>

¹⁶³ Georgetown Center on Privacy and Technology, *American Dragnet: Data-Driven Privacy in the 21st Century*, May 10, 2022, footnote 113, https://americandragnet.org/finding2#footnoteref113_tpf35b0.

¹⁶⁴ Washington State Department of Licensing, "DOL takes immediate steps to stop disclosure of information to federal immigration authorities," *Licensing Express*, January 15, 2018, <https://licensingexpress.wordpress.com/2018/01/15/dol-takes-immediate-steps-to-stop-disclosure-of-information-to-federal-immigration-authorities/>; see also Washington State Department of Licensing, *Presentation by the DOL to the Joint Transportation Committee*, May 17, 2018, p. 18, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/01/DOL-data-sharing-May-2018.pdf>

¹⁶⁵ Kristin Goodwillie, "This should have been prevented: Leaders respond to state slashing ICE database access after KING 5 investigation," *King 5*, August 27, 2025, <https://www.king5.com/article/news/investigations/investigators/king-5-investigation-washington-state-slashing-agreement-with-ice/281-4d3c69d9-56fe-49ed-8e2d-98a34615160d>

Figure 11, right: A slide included in “DOL Data Sharing,” a May 17, 2018 presentation given by DOL officials to the Washington State Joint Transportation Committee. The image shows how the WSP’s ACCESS enables institutions inside and outside of Washington state to query data from the Department of Licensing, as well as other state and local institutions. “CBP and ICE have established connectivity to ACCESS via Nlets” is italicized at upper left.



DHS, and suspended, but did not terminate, CBP’s account.¹⁶⁶ In addition, a number of other federal agencies retain active DAPS accounts; some of these have been reportedly enlisted in immigration enforcement under the current administration, though this is not their primary function.¹⁶⁷

Using public records requests, UWCHR researchers were able to verify DOL’s claims that DAPS access remained suspended in 2026; no evidence was found of DAPS searches

performed by CBP, ICE, or ICE-HSI from January to June 2026. This suggests that DAPS is not currently a pathway for DMV-to-DHS data sharing in Washington.

2. ICE/CBP searches of Nlets/ACCESS

The Washington State Patrol administers a platform called ACCESS which provides a pathway through which federal, state, and local law enforcement agencies, including federal immigration agencies, can query the DOL’s database using Nlets.¹⁶⁸ According to the WSP, more than 20,000 users across over 500 agencies use ACCESS.¹⁶⁹ Each of these queries performed on the system leaves a digital record, and UWCHR researchers have

¹⁶⁶ For details on which accounts were suspended and terminated, see Washington Department of Licensing, *DOL Customer Data Protections Quarterly Report*, June 1, 2026, p. 10-13, <https://dol.wa.gov/media/pdf/5331/2026-customer-data-protections-report-q1pdf/download?inline> Quarterly Report

¹⁶⁷ For example, the US Postal Inspection Service, which was listed in DOL’s June 2026 report as having an active DAPS account, has reportedly been involved in some immigration enforcement activities. See Jacob Bogage and Hannah Natanson “USPS law enforcement assists Trump ‘mass deportation’ effort, sources and records show,” *The Washington Post*, April 29, 2025, <https://www.washingtonpost.com/business/2025/04/29/usps-immigration-trump-deportations/>; similarly, the Internal Revenue Service has an active DAPS account and a data-sharing agreement with ICE, see Fatima Hussein, “Data of Thousands of Taxpayers Wrongly Shared with DHS, Court Filing Says,” *PBS News*, February 12, 2026, <https://www.pbs.org/newshour/politics/data-of-thousands-of-taxpayers-wrongly-shared-with-dhs-court-filing-says>

¹⁶⁸ As discussed above, these agencies can also query one another’s data, not simply that of the DOL. Nlets is a message switching system that facilitates the timely exchange of information on topics ranging from outstanding criminal warrants to hunting licenses to immigration status. More recently it has been proposed by the federal administration as a means to verify eligibility to vote. See Collin Wood, “DHS Lookup Tool May Expose Sensitive Data of Hundreds of Millions Of Americans, Secretaries of State Warn,” *StateScoop*, December 2, 2025, <https://statescoop.com/dhs-save-elections-secretaries-state-letter/>

¹⁶⁹ This number was provided to UWCHR Director Angelina Godoy in a written statement on June 19, 2026, responding to questions submitted on March 7, 2026.

used these records, jointly with records shared with us by community members documenting ICE/CBP arrests, to understand how Nlets/ACCESS is used for immigration enforcement. Using this method, UWCHR has confirmed 356 arrest incidents¹⁷⁰ between August 1, 2025 and October 13, 2026, as a result of the querying of DOL data via Nlets by federal agents. The real number of arrests pursuant to this data pathway is undoubtedly much larger, as researchers are only able to confirm the pathway's use in cases where details of an ICE/CBP arrest are reported to us.

ICE/CBP's use of Nlets to query DOL data is not new: as the below slide from a March 2018 presentation by DOL officials shows, since at least 2018, Washington DOL officials have been aware that ICE and CBP had access, via Nlets, to DOL data.

Furthermore, Washington DOL officials have also been aware that when they barred ICE/CBP from the DOL's DAPS database in early 2018, federal agencies began seeking the information via Nlets. As scholars at Georgetown Law

UWCHR has **confirmed 356 arrest** incidents between August 1, 2025 and October 13, 2026, as a result of the querying of DOL data via Nlets by federal agents. Researchers have identified **38 unique ORIs** affiliated with these incidents.

explain, drawing on the DOL's own published data (see below), "from 2016 to 2019, the number of yearly searches from DHS rose from approximately 400,000 to a staggering 1.1 million."¹⁷¹

In other words, Washington state officials have been aware of these multiple DMV-to-DHS pathways, and the way that the closure of one pathway resulted in the growing use of another, for years; yet the actions taken to investigate or address concerns proved insufficient to stop the practice. From January 1, 2026 to May 31, 2026 alone, DHS agencies conducted 1,037,724 searches of DOL driver and vehicle data,¹⁷² suggesting that 2026 figures are on track to double those from 2019.

Figure 12: WA Department of Licensing document, obtained by researchers at Georgetown Law School via public records requests, shows reporting on federal immigration agencies' access of WA driver and vehicle data in the 2019 fiscal year.

Requests via NLETS and WSP access from Federal Immigration Agencies – FY2019

~13% of requests were made by entities located inside Washington

~35% of requests included a request for image

Customs and Border Patrol in Blaine and Sumas have 10 terminals that allow direct access without going through NLETS

Requests from all DHS Agency Entities						
ORI	NLETS User	Total Requests	Total Individuals	Request for Image	Driver License Query	Driver History Query
CBP	No	2,590	1,659	73	2,552	27
CBP	Yes	1,336,951	658,032	470,714	1,071,564	265,387
DHS	Yes	11	9	11	11	-
ICE	Yes	56,248	30,801	17,940	55,784	464
USC	Yes	731	565	651	719	12
Total		1,396,531	691,066	489,389	1,130,630	265,890

Requests from DHS Agency Entities Inside Washington						
ORI	NLETS User	Total Requests	Total Individuals	Request for Image	Driver License Query	Driver History Query
CBP	No	2,590	1,659	73	2,552	27
CBP	Yes	160,079	136,423	20,745	159,633	446
DHS	Yes	1	1	1	1	-
ICE	Yes	11,574	2,930	11,219	11,461	113
Total		174,244	141,013	32,038	173,647	586



170 We use the term "incidents of arrests" rather than "arrests" because in some cases, more than one person was arrested in a single incident. This number does *not*, however, include cases in which an arrest was attempted but no one was taken into custody.

171 Georgetown Center on Privacy and Technology, *American Dragnet: Data-Driven Deportation in the 21st Century*, May 10, 2022, <https://americandrag.net.org/>.

172 This data was provided to UWCHR by the Department of Licensing in response to request # 26-13149.



UNFORTUNATELY, HOWEVER, THE STATE OF WASHINGTON APPEARS TO HAVE LARGELY FAILED TO REACT TO THE SYSTEMATIC AND HIGHLY PUBLICIZED MISUSE OF ITS NLETS/ACCESS SYSTEM FOR IMMIGRATION ENFORCEMENT; EVEN THOUGH ITS PRIOR AGREEMENTS STATE CLEARLY THAT SUCH USE WOULD CONSTITUTE A BREACH.

The DOL's ongoing provision of such data for purposes of civil immigration enforcement not only violates Keep Washington Working, but also defies the terms of the DOL's data licensing agreement with WSP, as well as the text of the user agreements signed by agencies as a condition of their participation in the WSP's ACCESS platform. While this may seem highly technical, the point is that the state has already incorporated specific requirements that Nlets comply with Keep Washington Working or face consequences, and yet has been inexplicably reticent to enforce these very agreements.

Unfortunately, however, the state of Washington appears to have largely failed to react to the systematic and highly publicized misuse of its Nlets/ACCESS system for immigration enforcement; even though its prior agreements state clearly that such use would constitute a breach,¹⁷³ and UWCHR

research first made evidence of such use public in January 2026, the state apparently has chosen not to interpret this to be a "breach or incident"¹⁷⁴ sufficient to follow the Washington state law's requirements to notify those whose personal data was unlawfully shared.¹⁷⁵

Furthermore, for the past three years the WSP has released identical one-page statements self-certifying its compliance and that of its

requires users to agree to comply with applicable federal and state laws and policies governing permissible use of the information. Second, agencies that participate in ACCESS are responsible for ensuring their personnel receive required training and follow established ACCESS policies regarding the appropriate use and dissemination of data obtained through the system. Third, the Washington State Patrol conducts routine compliance audits of participating agencies every three years. These audits review agencies' adherence to ACCESS policies, including permissible use requirements, account management, and related compliance controls. For users outside of Washington State who are not ACCESS users, but submit queries utilizing their respective message switches, the shared management philosophy of the FBI CJIS Security Policy, Advisory Policy Board, and CFR define how users and agencies are categorized and what level of access to data that they receive nationwide. Through these mechanisms—user acknowledgement, training and policy requirements, and periodic audits—the Washington State Patrol conducts oversight designed to promote and evaluate compliance with applicable legal and policy requirements governing the use of data."

174 Breach is defined in the agreement as "an unauthorized acquisition, loss of control, or exposure to an unauthorized person or business, or misuse of protected personal information." Incident is defined as "an event that confirms, or is reasonably thought to be, the unauthorized access to, or misuse of, protected personal information." "Protected personal information" is defined under Washington state law in RCW 46.04.209, 19.255.005, 42.56.590, and 18 U.S.C. Sec. 2725(3)–(4) to include identity information, including address, or Registered and legal vehicle owner name" (see RCW 46.04.209(e) at <https://app.leg.wa.gov/rcw/default.aspx?cite=46.04.209>).

175 While Clause 12.1 requires WSP to notify DOL of any "breaches or incidents" in which protected personal information is released in a manner deemed impermissible by the contract, no such notification appears to have happened even after it became widely known that DOL data was being used in civil immigration enforcement. When asked about whether a breach or incident had occurred, the Attorney General, Washington State Patrol, and Governor's office provided a statement to UWCHR that, "When there is a concern that users of the ACCESS system have violated the terms of our agreement we work closely with the agency they work for to ensure the violation is appropriately investigated. This includes investigating potential misuse (in concert with DOL) and suspending access to DOL data for potential misuse. Which was done for certain federal agencies pre-emptively who were candidates for misuse and suspending others after evidence surfaced."

173 UWCHR Director Angelina Godoy asked the Washington State Patrol what due diligence WSP performs to ensure the parties with whom it shares DOL data are in compliance with Washington law, and received the following written statement prepared by the Washington State Patrol, Attorney General's office, and Governor's office: "The Washington State Patrol administers the ACCESS program and implements several mechanisms intended to promote compliance with applicable laws, policies, and contractual requirements governing the use of Department of Licensing data. First, our ACCESS User Acknowledgement which outlines the legal and policy requirements governing access to and use of information available through the system. This acknowledgement

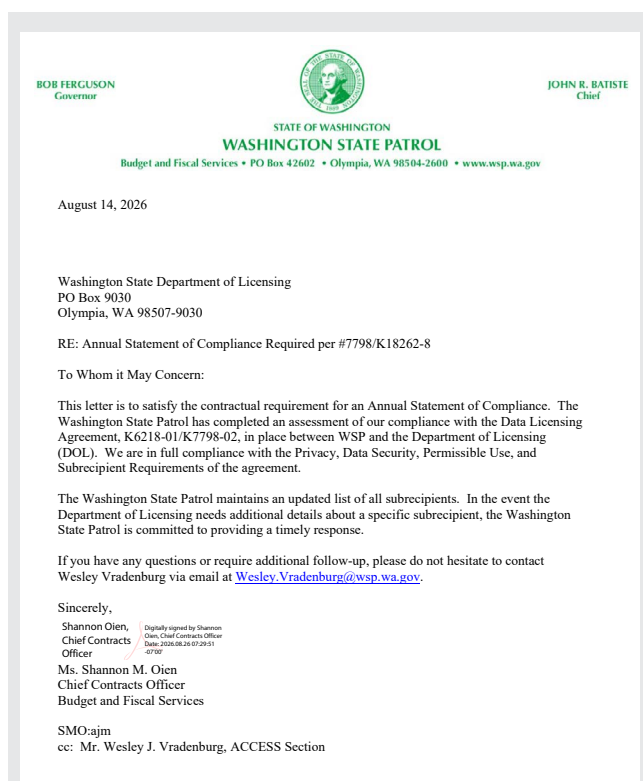


Figure 13: 2026 Annual Statements of Compliance from the Washington State Patrol self-certifying its adherence to the Data Licensing Agreement between WSP and WA DOL, claiming they are “in full compliance with the Privacy, Data Security, Permissible Use, and Subrecipient Requirements of the agreement.” This statement is identical to the 2025 and 2024 statements.

subrecipients to whom it shared data, with the terms of the contract governing the sharing of DOL data.¹⁷⁶

It is hard to square these repeated statements of being in “full compliance” with the documented and systematic violation of the WSP user agreements by its subrecipients associated with federal immigration agencies. It would appear that the required annual certification process has been reduced to a rubber stamp.

176 See Washington State Patrol, *Annual Statement of Compliance Required per #K7798/K18262*, August 28, 2024, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/K18262-4-DOL-EXE_reprint.pdf; Washington State Patrol, *Annual Statement of Compliance Required per #7798/K18262-7*, September 9, 2025, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/K18262-7-Letter-EXE.pdf>; and Washington State Patrol, *Annual Statement of Compliance Required per #7798/K18262-8*, August 14, 2026, https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/K18262-8-Stmnt_of_Compliance_2026-EXE.pdf.

This is not to suggest that no action has been taken by the state of Washington to address misuse of Nlets/ACCESS to obtain data from the DOL: the office of governor Bob Ferguson has indeed taken action, but it has been insufficient. In November 2025, in response to warnings of Nlets misuse by Senator Wyden (D-OR) and colleagues,¹⁷⁷ Washington state began to block Nlets queries originating from ICE ERO; in January 2026, this block was expanded to include accounts associated with ICE HSI. At the time, the governor’s office expressed its reluctance to block ORIs associated with CBP, citing concerns that an across-the-board block could undermine the agency’s ability to protect against threats like human trafficking;¹⁷⁸ it has continued to repeat this justification since then, often mentioning the scourge of trafficking¹⁷⁹ despite the fact that the DHS Center for Countering Human Trafficking is led by ICE HSI,¹⁸⁰ an agency the governor blocked months ago.

177 See U.S. Senator Ron Wyden, “Wyden, Espallat and 38 Members of Congress Urge Democratic Governors to Block ICE from Accessing Americans’ DMV Data,” November 12, 2025,

<https://www.wyden.senate.gov/news/press-releases/wyden-espallat-and-38-members-of-congress-urge-democratic-governors-to-block-ice-from-accessing-americans-dmv-data> 178 See, for example, Nina Shapiro, “Immigration agents still access WA licensing data, UW report shows,” *Seattle Times*, January 8, 2026, <https://www.seattletimes.com/seattle-news/immigration-agents-still-access-wa-licensing-data-uw-report-shows/>.

179 See, for example, the response here: “The governor’s office said there is no immediate way to address this incongruence in the near term. They want to avoid fully shutting off all access to the federal government in order to keep information flowing for public safety concerns — such as law enforcement that targets human trafficking,” in Gustavo Sagrero, “New Records Detail ICE Arrests in WA During Summer Surge. Yakima, Seattle Top the List,” *KUOW*, August 28, 2026, <https://www.kuow.org/immigration/2026-08-28/new-records-detail-ice-arrests-during-summer-surge-yakima-seattle-top-the-list>

180 See p. 8 of “Countering Human Trafficking: Year in Review (October 2023 to September 2024)” Department of Homeland Security, July 2025 https://www.dhs.gov/sites/default/files/2025-08/25_00809_ccht_fy24-year-in-review-annual-report_508.pdf: “The CCHT is DHS’s first unified, cross-Department coordination center for countering sex trafficking and forced labor, including the importation of goods produced with forced labor. Led by ICE HSI, the Center is a DHS-wide effort with the mission to advance counter-human trafficking law enforcement operations.”

So instead of blocking all CBP ORIs, the state has chosen to block them one by one, asking community groups to submit evidence of Nlets misuse for the governor's office to investigate.¹⁸¹ Using this method, as of September 18, 2026, the governor's office reportedly had blocked 5 ORIs associated with CBP but was continuing to operate on the presumption that other CBP users were accessing DOL data in good faith.¹⁸²

When agents attempt to query a license plate using a blocked ORI, the Washington State Patrol now sends out the following message in response:

WASHINGTON STATE PROHIBITS THE USE OF STATE SYSTEMS FOR CIVIL IMMIGRATION ENFORCEMENT PURPOSES. PLEASE SUBMIT LAWFUL INQUIRIES CONCERNING DEPARTMENT OF LICENSING DATA OR RECORDS THROUGH NEXTREQUEST
HTTPS://WADOLPUBLICRECORDS.NEXTREQUEST.COM

But it is apparent from records released to UWCHR that in many cases agents who receive this message simply switch to a different ORI and repeat the query, thus obtaining the information. For example, on April 14, 2026, the governor's office ordered the blocking of one CBP ORI, VACBP1500.¹⁸³ That same day, according to DOL records released to UWCHR researchers, Nlets queries of the DOL database began to be filed using a second CBP ORI, WACBP6700.¹⁸⁴

181 See July 9, 2026 letter from Karri Matau, President and CEO of the Community Foundation of Snohomish County, to Camille McDorman and Sahar Fathi in the office of Gov. Bob Ferguson, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/July-9-Inquiry-Letter.pdf>

182 The information here was shared with community organizations, in a meeting in which UWCHR researchers were present, on September 18, 2026 but the governor's office declined to clarify or confirm when asked for details, both in the meeting and subsequently. The governor's office has not responded to questions from UWCHR researchers since July 2026, and instead has redirected all communications from UWCHR to their public records office.

183 See documents released to UWCHR under record request R003021-071526: Washington State Patrol, emails to the WA Governor's Office and the WA DOL, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/R003021-071526-1.0.pdf>

184 In June 2026, UWCHR researchers filed request #

This switching of ORIs is also apparent in records obtained by UWCHR showing searches performed on individual vehicles by federal agents. For example, in multiple cases confirmed by UWCHR, queries performed by CBP ORIs preceded arrests carried out by ICE arrest teams, suggesting that, in fact, ICE continues to access Washingtonians' DOL data, either by logging into Nlets/ACCESS under CBP ORIs, or asking CBP to conduct searches on their behalf. Figure 14 provides an example.



**WITH EACH SELECTIVE BLOCK,
ALTERNATIVE ORIS PROLIFERATE.**

In another case, agents using the ORI VACBP1500 queried a vehicle's license plate in Lynden, WA on April 15, 2026—the day after the governor's office imposed the block on that account; when they did not receive the data they sought, an identical query was submitted using the ORI WACBP3500, to which the DOL provided the vehicle owner's information. Months later, the governor's office chose to block WACBP3500—but by that time, UWCHR records show that the queries had migrated to still other ORIs, including ORIs associated with other federal agencies.¹⁸⁵ As of October 9, 2026, UWCHR has documented searches performed by 38 unique ORIs affiliated with federal agencies prior to ICE/CBP arrests in Washington; with each selective block, alternative ORIs proliferate.

R010708-062326 of the Washington Department of Licensing, seeking a record of all Nlets/ACCESS queries performed by the ORI WACBP6700 during the month of April 2026; the records released revealed 198 queries were made by that ORI, beginning on April 14, 2026, the day VACBP1500 was blocked.

185 See documents released to UWCHR under record request R003021-071526: Washington State Patrol, emails to the WA Governor's Office and the WA DOL, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/R003021-071526-1.0.pdf>

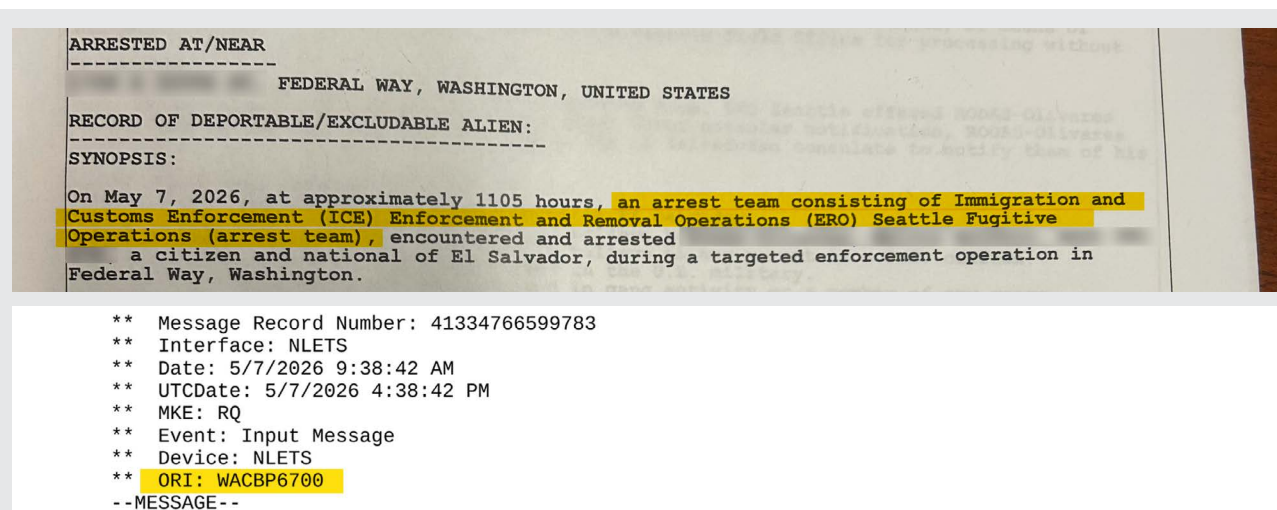


Figure 14: An I-213 arrest narrative (top) describing the civil arrest of an individual on May 7, 2026 at around 11:05 am in Federal Way, Washington, with an arrest team consisting of officers from ICE ERO Seattle Fugitive Operations. UWCHR researchers requested copies of all Nlets/ACCESS queries of that individual's license plate and received records (bottom) showing a search conducted shortly before the arrest by the ORI WACBP6700. Because the arrest narrative does not list CBP as present during the arrest, yet a CBP ORI was used in the investigation, these two documents suggest that either ICE was logging into Nlets/ACCESS under CBP ORIs, or asking CBP to conduct searches on their behalf.

This game of whack-a-mole is not providing meaningful protection for Washingtonians' data. While it is true that, as the governor's office told *KUOW* in late July, their efforts had blocked over 100,000 attempts to access DOL data via Nlets,¹⁸⁶ this number should be put in context: DOL data released to UWCHR revealed that from January 1, 2025—the month governor Ferguson took office—to May 31, 2026, DHS-affiliated agencies searched the DOL database for driver and vehicle information 3,696,147 times.¹⁸⁷

“

THIS GAME OF WHACK-A-MOLE IS NOT PROVIDING MEANINGFUL PROTECTION FOR WASHINGTONIANS' DATA.

¹⁸⁶ Gustavo Sagrero Álvarez and Esmey Jimenez, “WA Has Blocked Over 100,000 Federal Attempts to Access License Plate Data,” *KUOW*, July 24, 2026, <https://www.kuow.org/immigration/2026-07-24/wa-has-blocked-over-100-000-federal-attempts-to-access-license-plate-data>

¹⁸⁷ This figure is the sum of searches performed by users identified by the DOL as CBP, DHS, HSI, ICE, and USC in

3. Access to DOL data via data brokers

Like most state DMVs, Washington's DOL sells data to multiple data brokers; in 2025, the department disclosed active contracts with 14 companies, including Experian, and LexisNexis.¹⁸⁸ UWCHR researchers reviewed the contracts and amendments for LexisNexis, Experian, and R.L. Polk, all three of which have had contracts with DHS agencies in the recent past.¹⁸⁹ In all three cases, the contracts governing the sale of DOL data clearly forbid

response to requests 25-24279 and 26-13149. (26-13149 also included searches for part of June, but did not specify the dates covered, so we have removed the June data from these totals, which reflect January 1, 2025-May 31, 2026.

¹⁸⁸ The full list, provided to UWCHR in response to records request #25-24285, is: Data Ticket, Inc.; Datalink Services, Inc. (Transunion); Embark Safety LLC; Experian Information Solutions; Explore Information Services, LLC; HireRight LLC (formerly HireRight Solutions LLC); Insurance Information Exchange (iix, Verisk); LexisNexis Risk Solutions, Inc.; Novoaglobal, Inc.; R.L. Polk & Company (IHS Markit); Safety Holdings, Inc. (Samba Safety, Softech, American Drive Records); Sentinel Information Systems, LLC; Tesseract Data, Inc (TML Information Services, Inc.); and United Software Developers, Inc..

¹⁸⁹ See McKenzie Funk, “How ICE Picks its Targets in the Surveillance Age” *The New York Times Magazine*, October 2, 2019 <https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html>

the recipients from reselling that data to third parties for purposes of civil immigration enforcement. Various types of audits are required; permissible use audits, those most closely related to the concerns of this report, must be performed at least every three years.¹⁹⁰

LexisNexis' Risk Solutions holds a contract with DOL for the limited purpose of insurance carriers or their agents reviewing the driving records of insurance policyholders or applicants for coverage.¹⁹¹ The most recent copy of the contract provided to UWCHR clearly states that the "prohibition against permissive use and disclosure of confidential information includes, without limitation, using the data for purposes of investigating, locating, or apprehending individuals for immigration related violations."¹⁹² The contract further stipulates that the licensee—in this case LexisNexis—is responsible for overseeing the compliance of any subrecipients with whom it shares data.¹⁹³

In 2025, the Washington Department of Licensing provided UWCHR a copy of the results of LexisNexis' most recent [permissible use audit, from 2024](#). The audit found LexisNexis to be in full compliance with the permissible use requirements of the contract.

It is important to be clear that UWCHR has no

specific information linking LexisNexis or any other data broker to individual immigration arrests on Washington streets. However, as noted above, it is well known that LexisNexis plays a key role in provisioning ICE/CBP with data that these agencies use to surveil, locate, and arrest immigrants.¹⁹⁴ While it is certainly possible that the data the company purchases from Washington DOL are not included in the investigative packages the company sells to ICE/CBP, the only assurances we have that this is the case are those provided by the company itself—and as discussed above, the same company has signed at least one contract with ICE which specifies that it will structure ICE searches of the data provided in such a way that ICE's queries of that data are invisible, even to LexisNexis itself.¹⁹⁵ This would render state audits essentially useless, reducing the contract to a set of promises accepted on faith by the state of Washington.

190 See, for example, Washington State Department of Licensing, Data Licensing Agreement for Driver Record Information Between Department of Licensing and LexisNexis Risk Solutions, Inc. ("Contract K6579"), August 28, 2018, Section 18, p. 9, <https://jsis.washington.edu/humanrights/wp-content/uploads/sites/22/2026/10/K6579-DSA-Lexis-Nexis.pdf>. Contract K6579 is the most recent LexisNexis contract provided to UWCHR; UW was not provided a copy of DOL contract K7780 with LexisNexis, which runs through October 31, 2028.

191 See Contract K6579, Section 11, p. 6.

192 Note, no distinction is drawn between use of the data for civil vs criminal immigration violations; both uses are barred.

193 See Contract K6579, Section 13, p. 7.

194 See for example, Just Futures Law and Mijente, *The Data Broker to Deportation Pipeline: How Thomson Reuters and LexisNexis Share Utility and Commercial Data with ICE*, <https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/62df020189b0681d1b9398a8/1658782211567/Commercial+and+Utility+Data+Report.pdf>

195 Contract 70CMSD21C00000001 between LexisNexis and ICE requires that the contractor, in this case Lexis Nexis, "not use any information provided by the agency (query data) for its own purposes or share the information with other customers, business partners, or any other entity," (See *Contract 70CMSD21C00000001*, Performance Work Statement available here: <https://www.documentcloud.org/documents/23854204-2021-icfo-34162-1/>, p. 6 (p. 48 of PDF)) as well as "the contractor will ensure ICE user queries are conducted anonymously to ensure other individuals or entities that use the LPR service (whether a law enforcement agency, commercial entity, or otherwise) are not able to identify that ICE is investigating a license plate." p. 7 (p. 49 of PDF).

BEST PRACTICES

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 here, 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



ANY ATTEMPT TO BRING SUCH PRACTICES INTO COMPLIANCE WITH LAWS PASSED IN THESE STATES THEREFORE NEEDS TO TACKLE THE PROBLEM HOLISTICALLY, RATHER THAN PIECEMEAL.

the organizations that serve them to obtain court injunctions ordering a halt to prohibited behavior when it does occur. In two of the four states examined here—Maryland and Washington—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 these 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 here (Maryland, Minnesota, New York, or Washington) incorporate a private right of action which would allow those harmed by the sharing of their DMV data to sue for damages. But New York's Green Light law, as amended in 2020, goes the furthest in specifying that failure to comply constitutes a Class E felony—and further applying this to local law enforcement should they improperly share DMV data with federal immigration authorities. Other states not examined here provide yet a stronger model; Oregon, for example, included a private right of action in its 2021 Sanctuary Promise Act, and is currently facing a suit brought by the Rural Organizing Project in response to its sharing of driver and vehicle data via Nlets.¹⁹⁶

196 Conrad Wilson, "Oregon State Police Violated Law by Sharing Data with ICE for Years, Lawsuit Claims," *Oregon Public Broadcasting*, May 6, 2026, <https://www.opb.org/article/2026/05/06/oregon-state-police-violated-sanctuary-law-sharing-data-ice-lawsuit-claims/>

TRANSPARENCY

All four of the states examined here 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 record¹⁹⁷ and also specifically granting data subjects (individuals about whom the government record exists) to obtain copies of government records about them.¹⁹⁸ 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,¹⁹⁹ Illinois,²⁰⁰

Maine,²⁰¹ New Jersey,²⁰² and Virginia²⁰³ 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.²⁰⁴ These policies are deeply problematic, for they make it extremely difficult for residents of these states to ensure

197 See Minn. Stat. 171.12 § Subd. 1a <https://www.revisor.mn.gov/statutes/cite/171.12>: “All queries and responses, and all actions in which data are entered, updated, accessed, shared, or disseminated, must be recorded in a data audit trail. Data contained in the audit trail are public to the extent the data are not otherwise classified by law.” In practice, however, Minnesota BCA agency responses were slower and less informative than those provided by the WSP in Washington, which was consistently the most prompt and comprehensive of the state agencies examined here.

198 See Minnesota’s Government Data Practices Act <https://www.revisor.mn.gov/statutes/cite/13>

199 In response to multiple queries under California’s Public Records Act, including for example request # REQ-2026-3483, the California Department of Justice responded that, “Pursuant to Government Code Section 7923.600, investigation records are exempt from disclosure under the California Public Records Act. This exemption covers any investigatory files of a state or local police agency, or any other state or local agency if compiled for correctional, law enforcement, or licensing purposes. Therefore, the requested CLETS records are exempt from disclosure.”

200 An Illinois State Police public information officer asserted in response to request # 2026 PAC 94540 that “Information gathered for the Law Enforcement Agency Data System (LEADS) cannot be provided to you because the dissemination of LEADS information to non-law enforcement persons and entities is prohibited.” (May 7, 2026 letter from Sarah Wheeler to Angelina Godoy); UWCHR appealed this decision to the Office of the Illinois Attorney General, but was unsuccessful in obtaining the records sought.

201 The Director of Policy of the Maine State Police responded to multiple UWCHR requests for information that, “Law enforcement intelligence and investigative record information is confidential if there is a reasonable possibility that release would cause any of the twelve listed harms under 16 MRS §804.” (Letter from Rebecca Graham to Angelina Godoy, April 21, 2026)

202 UWCHR filed multiple requests for public information to the New Jersey State Police, the entity which administers Nlets access in the state. All received a similar response, stating (as, for example, in response to request W254507), “The Division of State Police can neither confirm nor deny the existence of records in response to your [Open Public Records Act] request. Confirming the existence or non-existence of such records would itself disclose information regarding law enforcement database usage and investigative activity. “Long before the enactment of OPRA, the confidentiality of information law enforcement authorities receive regarding possible criminal activity was recognized in our caselaw.” *N. Jersey Media Grp., Inc. v. Bergen Cty. Prosecutor’s Office*, 447 N.J. Super. 182,

203 (App. Div. 2016). Confidentiality in investigative techniques is “vital not only because it serves to protect government sources of information, but also because it enhances the effectiveness of investigative techniques and procedures.” Disclosure of such records, if they exist, would reveal law enforcement investigative techniques and system usage.” UWCHR subsequently entered mediation with the NJ State Police, but did not obtain access to the records sought.

203 The Virginia Department of State Police responded to UWCHR request # 26-5513, “Please be advised that the records you seek are exempt from dissemination pursuant to Virginia Code Sections 52-15, 19.2-389, and 2.2-3802, and pursuant to United State Code Section 28 U.S.C.A. § 534.” UWCHR did not appeal, given the State Police’s additional mention of the fact that the public records law in Virginia is for the most part only available to residents of the state.

204 First, the Oregon Department of Transportation informed UWCHR that “The Oregon Public Records Law gives ‘every person’ a right to inspect the public records of a public body in Oregon, with certain exemptions and limitations. ORS 192.314(1). A ‘person’ does not include public bodies. ORS 192.311(3). A public body may not use the Oregon Public Records Law to obtain public records from another public body. Because the University of Washington is a public body, we respectfully deny your request.” (June 11, 2026 response to request # R024509-052026). This was upheld on appeal. Subsequently, a private citizen sought records of Nlets queries of the Oregon DMV and was then rejected on the grounds that Oregon Public Records Law does not obligate the creation of a new record; performing a search, in this interpretation, would be creating a new record. This judgment, too, was upheld on appeal to the Department of Justice.

that laws protecting the privacy of their driver and vehicle information are upheld in practice. While all states restrict public access to details of police investigations—in part to protect the very subjects of such investigations, and to avoid divulging details that could render future investigations more difficult—UWCHR's requests did not seek personally-identifiable information about any individual, nor would granting them have exposed details of nonpublic investigative techniques. To assume that any type of record pertaining to any law enforcement activity must be withheld from the public effectively renders all law enforcement activity secret—precisely at a time when, germane to the topics examined here, multiple courts have found that federal law enforcement agencies have dangerously overstepped their bounds and trampled the core Constitutional rights of citizens and noncitizens alike.²⁰⁵

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—something these states deny their residents by rendering all DMV data queries a black box.

CONCLUSION

Across the country, escalating ICE/CBP enforcement is causing expanding harm—not only because every time a person is forcibly uprooted from their family and community, the impacts ripple outward from the individual, but also because of the increasingly aggressive and often illegal ways in which people are being apprehended. The sudden, disproportionate aggressiveness of “jump out” vehicular arrests

sows fear in entire communities,²⁰⁶ making people afraid to drive or leave their homes at all, even to seek medical care, schooling, or employment. As the American Immigration Council writes, “Enforcement actions involving unmarked vehicles or agents in plain clothes have led to confusion and justified fear—and have at times turned deadly—leaving communities reeling as they figure out how to move forward.”²⁰⁷



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.

In passing “Driver’s License for All” laws, states sought to encourage immigrants to feel safe navigating their roads and highways, and promised to protect their data in return. While it is true that few anticipated the most aggressive forms of immigration enforcement we’re seeing now, it is also true that leaders in many state DMVs did not bother to learn how vulnerable their longstanding data-sharing systems were—and are only now discovering the danger this carelessness is causing to entire communities.

It’s past time for state leadership to figure out solutions. While state leaders often point to the Trump administration as the primary culprit—

205 See Edvard Pettersson, “Judge Inclined to Stop Warrantless ICE Arrests Without Escape Risk Findings,” *Courthouse News Service*, August 13, 2026, <https://www.courthousenews.com/judge-inclined-to-stop-warrantless-ice-arrests-without-escape-risk-findings/>

206 See for example, Jared Rutecki, “Just Violence, Confusion: Federal Immigration Raids Also Bring Fear to Suburban Streets,” *WTTW*, November 12, 2025, <https://news.wttw.com/2025/11/12/just-violence-confusion-federal-immigration-raids-also-bring-fear-suburban-streets>

207 Micaela McConnell, “Fear as Policy: The Growing Mental Health Toll of Mass Deportation Policies,” *American Immigration Council*, August 12, 2026, <https://www.americanimmigrationcouncil.org/blog/mental-health-mass-deportation-immigration-policies/>

and it's undeniable that the responsibility for the cresting wave of anti-immigrant sentiment lies with the feds—the role played by state DMVs is neither trivial nor incidental. Not only are they facilitating the arrests by handing over immigrants' data, they're even giving legal cover for ICE/CBP's acts of indiscriminate racial profiling by enabling agents to identify the immigration status of drivers at the push of a button.

ICE agents, unlike police or sheriffs, are not legally permitted to engage in *pretextual* traffic stops—to pull a driver over for broken tail light, for example and then ask about other possible offenses; they must have a *reasonable suspicion* that a person is in violation of immigration law before stopping the vehicle. While the Supreme Court last year indicated its openness to the use of racial and occupational characteristics in ICE/CBP's decisionmaking process before carrying out so-called “Kavanaugh stops,”²⁰⁸ ICE rarely mentions such attributes explicitly in its arrest narratives. But they *do* mention data culled from state databases. In this sense, states that allow ICE/CBP access to the personal information stored in their DMV databases are not only handing over actionable information to the very agency terrorizing our neighbors—they're also providing justification for the arbitrary and violent practices that are causing such grievous harm.

This must stop.

208 Kristi Noem, Secretary, Department of Homeland Security, et al., v. Pedro Vasquez Perdomo, et al., No. 25A169 (2025), https://www.supremecourt.gov/opinions/24pdf/25a169_5h25.pdf.

APPENDIX

Overview of driver and vehicle data sharing—Maryland, Minnesota, New York, and Washington

State, Year drivers' licenses made available to noncitizens	State Nlets administrator, Name of state access point for Nlets, State DMV	State laws limiting data sharing for immigration enforcement purposes	Warrant or court order requirement for federal access of DMV data for immigration enforcement purposes	DMV-to-DHS pipeline pathways
Maryland, 2013	Maryland State Police (MSP), Maryland Electronic Telecommunications Enforcement Resource System (METERS), Motor Vehicle Administration (MVA)	2021 Driver Privacy Act, 2026 Data Privacy Act	Yes	Direct access by federal agencies to MVA database: Evidence reveals that this pathway is currently open, though limited. DHS searches of MVA data via Nlets: Some DHS ORIs have been blocked, but the pathway remains open to others. Access via data brokers: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation. Access via state/local law enforcement: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation.
Minnesota, 2023	Minnesota Bureau of Criminal Apprehension (BCA), Law Enforcement Message Switch (LEMS), Driver and Vehicle Services (DVS)	2023 Driver's License For All Act, 2026 revisions to bill, <i>Continued on next page.</i>	Partial. (Warrants required for non-REAL ID compliant license data, but not for vehicle data)	Direct access by federal agencies to DVS database: Evidence reveals that this pathway is currently open for vehicle data. DHS searches of DVS data via Nlets: Evidence reveals that this pathway is currently open for vehicle data. <i>Continued on next page.</i>

APPENDIX CONTINUED

State, Year drivers' licenses made available to noncitizens	State Nlets administrator, Name of state access point for Nlets, State DMV	State laws limiting data sharing for immigration enforcement purposes	Warrant or court order requirement for federal access of DMV data for immigration enforcement purposes	DMV-to-DHS pipeline pathways
		<i>Continued from previous page.</i> These laws only apply to non-REAL ID compliant driver data, leaving access to all other drivers' data and vehicle data open.		<i>Continued from previous page.</i> Access via data brokers: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation. Access via state/local law enforcement: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation.
New York, 2019	New York State Police (NYSP), New York Statewide Police Information Network (NYSPIN), Department of Motor Vehicles (DMV)	2019 Green Light Law	Yes	Direct access by federal agencies to NY DMV database: UWCHR research did not find evidence that this pathway is open. DHS searches of NY DMV data via Nlets: UWCHR research did not find evidence that this pathway is currently open for cars with NY license plates. Access via data brokers: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation. Access via state/local law enforcement: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation.

APPENDIX CONTINUED

State, Year drivers' licenses made available to noncitizens	State Nlets administrator, Name of state access point for Nlets, State DMV	State laws limiting data sharing for immigration enforcement purposes	Warrant or court order requirement for federal access of DMV data for immigration enforcement purposes	DMV-to-DHS pipeline pathways
Washington, 1993	Washington State Patrol (WSP), A Central Computerized Enforcement Service System (ACCESS), Department of Licensing (DOL)	2019 Keep Washington Working	No	Direct access by federal agencies to DOL database: This pathway was open as recently as mid-2025, but subsequent UWCHR research did not reveal evidence that this pathway has been open since. DHS searches of DOL data via Nlets: Evidence reveals that this pathway is currently open. Access via data brokers: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation. Access via state/local law enforcement: Impossible to test pathway due to lack of access to evidence to review. Remains a concern and requires further investigation.

GLOSSARY

287(g) agreements: Agreements that deputize local police or sheriffs to carry out immigration enforcement duties.

Audits: Ensuring the security of information systems requires regular auditing, or the undertaking of processes that monitor how users interact with stored information. This is important to detect hacking or breaches that might compromise the security and reliability of the data, as well as to ensure that users are complying with the rules which govern how the data is to be used (otherwise known as “permissible use.”)

Data brokers: Businesses that collect, sell, or license personal consumer information from various sources to third parties for purposes like determining insurance rates, providing credit reports, running background checks, or conducting targeted ads. Data sold by data brokers can include: property records; utility records; bank accounts; credit reports; court documents; records of marriage, divorce, bankruptcy and other proceedings; and social media profiles, among others. Some data brokers (LexisNexis, Thomson Reuters, Experian, and others) resell data they buy from DMVs to third parties. These same companies are also known to sell data to immigration enforcement agencies.

DHS: Department of Homeland Security, the federal agency that houses ICE (which includes both ICE-HSI and ICE ERO), CBP, and USCIS.

DMV: Department of Motor Vehicles is used as a general term in this report to refer to state-run agencies that handle vehicle registration and driver’s licensing. States use varying names to refer to this agency, for example: Maryland Motor Vehicle Administration (**MVA**); Minnesota Driver and Vehicle Services (**DVS**); New York Department of Motor Vehicles (**NY DMV**); and Washington Department of Licensing (**DOL**).

DMV databases: Each state’s DMV hosts data in at least one database, for example: Washington’s Drivers and Plates Search (DAPS) and Driver Information and Adjudication System (DIAS). Many states allow certain external parties access to their state driver and vehicle databases, often as a means of generating revenue, and sometimes as a service provided gratis to other governmental bodies.

DMV-to-DHS Pipeline: The passage of information from state Department of Motor Vehicles (DMVs) to immigration enforcement agencies (such as Department of Homeland Security, or DHS sub-agencies ICE and CBP). This report identifies four pathways: directly through database access; through the interstate querying system known as Nlets; through sale to data brokers, who may in turn sell it to ICE/CBP; and through local law enforcement who may pass data to ICE/CBP.

Driver and vehicle data: Data collected by state agencies related to vehicle registration and driver’s license information. This data could include: name and address of vehicle’s registered owner, driver’s license number, VIN numbers, license plate numbers, and car make/model.

Driver's license restriction codes: States may include codes on drivers' licenses or in DMV databases to indicate any restrictions on the license; these can include notations that a given license is not compliant with federal REAL ID requirements. Federal court testimony in Maryland has exposed how federal immigration agents have used these codes in state DMV data to identify individuals they suspected were non-citizens because of these restriction codes.

ICE/CBP: ICE (Immigration and Customs Enforcement) and CBP (Customs and Border Protection) are federal immigration enforcement agencies. In this report, we refer to the squads carrying out traffic arrests as "ICE/CBP" because it is often impossible to identify the agency or agencies involved in any given arrest due to the lack of identifiable uniforms or badges and the refusal to display warrants. Furthermore, ICE documents show they often operate in combined teams, and as we explain in this report, in at least some cases they appear to perform queries in DMV data-sharing networks under one another's Originating Agency Identifier (ORI) accounts.

"jump out": The term "jump out" refers to a practice in which multiple unmarked vehicles, sometimes lacking license plates, suddenly surround a target while driving, and unidentifiable officers leap from the car to confront its driver with overwhelming force.

Nlets: A national switchboard that facilitates information-sharing—including the sharing of DMV data—by law enforcement agencies across multiple states. In many states, Nlets serves as the primary means through which federal immigration authorities query state DMVs to link vehicles they observe to specific individuals. Each state has its own local administrator of Nlets, for example: Maryland State Police administers Nlets via Maryland Electronic Telecommunications Enforcement Resource System (**METERS**); Minnesota Bureau of Criminal Apprehension administers Nlets via Law Enforcement Message Switch (**LEMS**); New York State Police administers Nlets via New York Statewide Police Information Network (**NYSPIN**); and Washington State Patrol administers Nlets via A Central Computerized Enforcement Service System (**ACCESS**). Throughout this report, when referencing specific states' systems, UWCHR references Nlets with the state system through which it is administered, for example: **Nlets/METERS**; **Nlets/LEMS**; **Nlets/NYSPIN**; and **Nlets/ACCESS**.

Nlets message keys: Codes that determine the type of data being queried in Nlets. These can include: **RQ** (registration query); **DQ** (license query); and **IAQ** (immigration alien query).

ORI: Originating Agency Identifier, an nine-digit alphanumeric code, assigned by the FBI to federal agencies; the third to fifth digits in the sequence identify the particular agency performing an Nlets query. State officials may choose to block Nlets access for specific ORIs, however research has shown that when one ICE/CBP ORI is blocked, federal agents just move on to using another ORI.

Permissible use: Specific uses defined in contracts that contract parties must abide by. For DMV data sharing contracts in states with laws barring data from immigration enforcement use, permissible use clauses often include language such as "may not disclose information obtained as a result of their access to personal information from Motor Vehicle Records to any federal agent or federal agency for the purpose of federal immigration enforcement."

REAL ID: Passed by Congress in 2005, the REAL ID Act establishes minimum security standards for state-issued driver's licenses and identification cards; it also permits states to issue "non-REAL ID compliant" licenses to those without citizenship documentation. The state of Minnesota protects the data of those holding these "non-REAL ID compliant" licenses from disclosure to federal immigration officials.

Sanctuary laws/sanctuary states: Policies passed by state and local governments to limit the expenditure of state resources on federal immigration enforcement, which is a federal responsibility. These laws often include barring or limiting the provision of driver or vehicle data to federal immigration agencies, including requiring a warrant or court order for access.

Warrant: Warrants are documents, typically issued by a court, allowing law enforcement to undertake certain actions, like entering private property to conduct a search or make an arrest. In general terms, the requirement to obtain judicial approval prior to undertaking such actions offers protection against violations of the fourth amendment to the U.S. Constitution. However, ICE sometimes refers to its own documents as warrants even when they have not been independently reviewed by a judge; these are more properly termed "administrative warrants" because they have been created by the agency itself, and have not been reviewed by an independent judicial authority. In seeking to ensure that searches of their residents' private data in DMV databases are lawful, some states have passed laws requiring federal immigration agents to obtain a judicial warrant before being granted access.



Stopping the DMV-to-DHS Data Pipeline: Vehicle and Driver Data Sharing with Federal Immigration Agencies

Center for Human Rights
The Henry M. Jackson School of International Studies
University of Washington
Box 353650, Seattle, WA 98195-3650
Phone: (206) 685-3435 | Email: uwchr@uw.edu
www.jsis.washington.edu/humanrights