Support HB2163 (Tran): Protect the Personal Data of Virginia Drivers

Virginia DMV Data Sharing with ICE:

How Does It Happen and How HB2163 Can Stop it

The Virginia Department of Motor Vehicles (DMV) is one of the biggest warehouses of your personal information in the Commonwealth. In order to carry out its primary responsibility of ensuring vehicle and driver safety, DMV maintains one of the largest databases of information about Virginian residents. This data contains some of the most sensitive information including a person's social security number, date of birth, photo, and home address.

The sharing and selling of this data can have harmful consequences such as identity fraud, stalking or vigilante violence.[1] In many instances, it has led to ICE showing up at the doorsteps of unsuspecting residents and families such as in Maryland, Illinois, Washington and California. It has also turned the personal data of residents into a multi-million dollar business for big data companies.[2] These concerns have led many states to pass legislation that creates greater data protections on DMV data.[3] Now that Virginia has enacted its own non-REAL ID driver's privilege card, there is a renewed urgency to address the issue of immigration agents using this data to identify immigrants for raids and deportations.

I. Background on how the Department of Motor Vehicles currently shares information with third parties

Through a year-long investigation, we have found that the VA DMV shares and sells its data in a number of ways including:

- *Direct requests to DMV by government agencies or private companies:* This means that private companies or government agencies can request personal driver information directly from the DMV, including batch data. With batch data, companies can process large amounts of information on multiple individuals using certain search terms.
- *Indirect access through criminal justice platforms:* an agreement between the Virginia State Police and the DMV allows the State Police to share DMV information to government entities, including ICE, through its vast criminal justice platforms, such as the Virginia Criminal Information Network (VCIN) and its access portal to the International Justice and Safety Network (Nlets).
- *Data agreements with private companies:* VA DMV permits private companies to purchase DMV data, including batch data on thousands of drivers, through "information use" agreements. There are hundreds of data agreements and requests from private companies. Many of these private recipients of this data resell this data to hundreds if not thousands of third parties. As a result, these companies earn millions of dollars in revenue from obtaining the personal information of drivers.

This expansive data sharing occurs because Virginia law does not place sufficient restrictions on direct or third-party access to DMV data, including (1) the ability of ICE to access DMV data for immigration enforcement, either directly with DMV or indirectly through VCIN, and (2) the ability of private companies to resale and repurpose DMV data to third parties including ICE.

II. How Does ICE Get the information?

The lack of legal guardrails on DMV data sharing means that ICE can obtain—indirectly and directly—the personal information of Virginia drivers

from the DMV. ICE has a number of potential ways to access Virginia's DMV data to locate individuals for immigration raids and deportation. Based on our year-long investigation, we highlight the three main methods below:

A. STATE CRIMINAL JUSTICE DATA PLATFORMS

ICE can obtain DMV data indirectly through access to the Virginia Criminal Information Network (VCIN), a criminal justice data platform operated by the Virginia State Police (VSP). This allows ICE to bypass data protection and transparency policies required for direct requests to the DMV. The DMV has a memorandum of understanding with VSP that allows government agencies whom VSP grants access to VCIN to query the DMV database.[4]

Based on our research and investigation, we believe that VCIN is the main way that ICE accesses DMV data. Concerningly, DMV does not track which government entities have access to its data through VCIN nor the number of queries. As such, it is currently difficult to monitor VCIN's compliance with existing state DMV laws. For example, neither VSP nor DMV publish statistics on how often ICE queries VCIN for DMV data and for what purposes. This bill intends to address this gap around data security and transparency.

B. DIRECT REQUESTS FOR INFORMATION FROM ICE

ICE can obtain DMV data by directly requesting the information from the DMV. There are two ways of doing this:

- Case-by-case or batch requests: as explained earlier, these requests allow ICE to request individual and/or "batch data" on Virginia drivers. ICE regularly uses direct requests to the DMV to obtain driver personal information in VA.[5]
- Information use agreement: such an agreement between DMV and ICE provides ICE with direct access to DMV's driver query system. Prior to August 2018, DMV did have an information use agreement with ICE for access to DMV data.[6] However, according to FOIA, this agreement expired and ICE did not seek renewal.[7]

ICE likely did not renew its use agreement with DMV because ICE found another, easier method to access DMV data through the state criminal justice database, VCIN, as discussed in section (A) above.

C. INDIRECT ACCESS THROUGH PRIVATE RESALE OF DMV DATA

Lastly, ICE can obtain DMV data through private companies that purchase and resell the data to ICE. Multiple investigations by journalists, reports, and scholar research have confirmed that credit reporting companies and private data broker companies such as LexisNexis, RL Polk, Equifax and Thomson Reuters sell DMV data directly or indirectly to ICE, which the agency then uses to locate immigrants for raids and deportations.[8] The following are examples of private companies which purchase driver personal information in bulk from VA DMV and their connections with ICE:

- LexisNexis (d/b/a RELX) has direct contracts with ICE for access to its collected data including state DMV data.[9]
- RL Polk (d/b/a IHS Markit) is one of the oldest data companies which invented the first personal directory books. A recent New York Times investigation confirmed that RL Polk resells its DMV data to Thomson Reuters, leading at least one state DMV to conduct an audit action on Polk and requiring the company to take corrective action to ensure that data was not getting into the hands of ICE through Thomson Reuters.[10] As previously mentioned, Thomson Reuters has come under repeated criticism for selling data to ICE for use in immigration enforcement.[11]

Moreover, compliance and audit investigations conducted by other DMVs and oversight bodies have found that companies which purchase and share DMV data, including LexisNexis, have violated the terms and conditions of their data use agreements including selling data to unauthorized third parties or failure to comply with data security protocols.[12]

In the face of these emerging problems, VA DMV has implemented stopgap measures with these companies through the use of written agreements that restrict the sharing and repurposing of personal information. The DMV already requires the following terms and conditions from private companies seeking to purchase and resale data in bulk like LexisNexis and RL Polk:

- Submit an information use application which requires them to state a specific use or purpose for the data and why the information necessary to carry out this purpose;

- Enter into a written agreement for data access that specifies the authorized purpose;
- Restricts the use of the data by the requester and third parties to the specific purpose and no other purposes as a condition of the written agreement;
- Explicitly authorizes the dissemination of personal information by the requester to third parties in the written agreement.

These contract requirements allow these private companies to use the data for the original authorized purpose of their request such as insurance claims, vehicle title checks, and car manufacturer recalls but restrict their ability to resale the data to anyone for any purpose.

Codifying these practices is essential to protect against future misuse of personal data by third party private actors. The DMV could revise or eliminate these stopgap measures in the future; and regulation is clearly necessary as the same or similar companies that are recipients of Virginia's DMV data already share the DMV data of other states with ICE. Moreover, the DMV currently does not have any robust oversight mechanisms in place to track compliance with its use and privacy restrictions. Given the history of these companies violating the terms and conditions of data use agreements of other DMVs, regular audits will be critical to ensuring compliance.

III. What Does HB2163 (Tran) Do?

HB2163 is critical to protecting the personal information of Virginia drivers from being bought and sold by private companies and preventing ICE from misusing the DMV database to detain and deport immigrant residents of Virginia. The current bill would:

A. LIMIT THE USE OF DMV DATA FOR IMMIGRATION ENFORCEMENT (LINES 494 - 506)

As discussed above at Section (II)(B), ICE can and has made requests for DMV data to the DMV. HB2163 requires ICE and any other agencies to obtain a judicial warrant or court order to obtain DMV data for the purpose of civil immigration enforcement. Also, if there is a request for immigration enforcement purposes, the bill requires that the DMV notify the person who is the subject of such a request.[13]

B. CODIFY EXISTING DMV DATA PROTOCOLS FOR VA CRIMINAL JUSTICE DATABASES TO PREVENT INDIRECT ICE ACCESS TO DMV DATA (LINES 657-682)

As discussed at Section (II)(A), various federal, state, and local government agencies including ICE have access to DMV data through the criminal justice database VCIN, operated by Virginia State Police. Alarmingly, agencies can access and share DMV data, even when the inquiries are not related to a criminal justice purpose. Fortunately, the DMV and VSP recently signed an agreement to limit access to DMV data through the Virginia Criminal Information Network to criminal justice agencies engaged in a criminal justice purpose. Because ICE and other immigration agencies primarily engage in civil immigration enforcement, there is concern that ICE would misuse the data without further regulation.[14]

HB2163 codifies and clarifies these new DMV protocols by limiting the use of DMV data over criminal justice databases to the administration of criminal justice and requiring law enforcement agencies to certify that the data will not be used for civil immigration enforcement purposes. *As such, this bill will not disrupt the ability of law enforcement agencies to use DMV data to investigate violations of federal or state criminal law while making it clear that DMV data should not be used for civil immigration purposes such as locating individuals for deportation.*

C. CODIFY BEST PRACTICE PROTOCOLS FOR PRIVATE COMPANY SALE OF DMV DATA TO PREVENT INDIRECT DATA SHARING WITH ICE (LINES 639-656)

As discussed above at Section (II)(C), hundreds of private companies purchase state DMV data in bulk and sell the information to third parties. A number of those companies sell DMV data to ICE (LexisNexis and Thomson Reuters) or to companies that then resell the data to ICE (RL Polk). HB2163 codifies existing policies and practices that DMV has already put in place in its agreements with private companies to regulate the dissemination of driver personal information and limit third party data sharing with ICE including:

- Requiring the data requester to enter into a written agreement with the DMV that states an authorized purpose for requesting the data and why the data is necessary to carry out that purpose;

- Restricts the use of the data by the requester and third parties to the purpose specified in the written agreement and no other purposes.

As discussed in section II, these bill requirements will not disrupt the ability of data brokers such as LexisNexis or RL Polk to purchase and sell DMV data. These requirements are already incorporated into existing written agreements with the DMV with which they are required to comply. In accordance with its written agreement, companies like LexisNexis can continue to access DMV data for insurance claim purposes and share that information with a third party so long as it is used for the same authorized purpose. That being said, these existing terms and conditions should be codified into law. The DMV can change their practices in the future and the regulation is critical to preventing companies that already sell DMV data to ICE from disseminating the personal information of Virginia's drivers to ICE.

D. ESTABLISH OVERSIGHT AND ACCOUNTABILITY MECHANISMS TO PROTECT PERSONAL DMV DATA FROM SECURITY BREACH AND UNAUTHORIZED USE BY THIRD PARTIES. [LINE 687-690]

HB2163 enacts audit and disclosure requirements that are critical to enforcing these limitations on data access and monitoring unauthorized use or access to DMV data. The DMV does not currently conduct audits of its agreements with private companies and government agencies for compliance. Regular audits will allow the DMV to monitor whether third parties have lawful access to the DMV database and whether the DMV's sensitive, personal information is properly protected from unauthorized use. These audits are particularly critical given the large data breaches in DMV data across multiple states in recent years. Moreover, when other states have conducted audits and investigations, agencies have found that government officials and private companies like LexisNexis have failed to comply with its agreements on data use with the DMV.

8 Acknowledgments

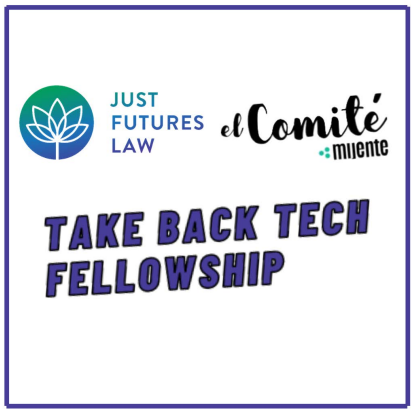
TAKE BACK TECH FELLOW
Linus Chan, University of Minnesota Law School

WRITERS
Julie Mao and Paromita Shah, Just Futures Law Professor
Linus Chan, University of Minnesota Law School

EDITORS
Diane Burkley Alejandro, Lead Advocate
ACLU People Power Fairfax
Simon Sandoval-Moshenberg, Legal Aid Justice Center

REPORT DESIGN LAYOUT
Summer Rose Wood

Mijente and Just Futures Law are joint sponsors of the Take Back Tech Fellowship program.



9 Endnotes

1 The REAL ID Act was opposed by hundreds of domestic violence organizations because of the concern that the disclosure of an individual's residential address made it easier for perpetrators to locate and harm violence survivors. See https://www.epic.org/privacy/dv/real_id_immigrant_women.pdf. The original federal Driver's Privacy Protection Act was passed because of the murder of actress Rebecca Schaeffer in which the perpetrator hired a private investigator to locate her residential address from the CA DMV. https://www.cdcr.ca.gov/insidecdcr/2020/09/03/death-of-actress-aided-by-states-failure-to-protect-data/; see also Minnesota Cop Awarded $585K After Colleagues Snooped on Her DMV Data, Wired, Jun. 21, 2019, https://www.wired.com/story/minnesota-police-dmv-database-abuse/.

2 DMVs are selling your data and making millions, documents reportedly reveal, Fox News, Sept. 6, 2019.

3 S.B. 1747B, 2019 Leg., Reg. Sess. (N.Y. 2019), https://www.nysenate.gov/legislation/bills/2019/S1747; Assemb. 4743, 218th Leg., Reg. Sess. (N.J. 2018), https://www.njleg.state.nj.us/2018/Bills/A5000/4743_I2.PDF; Washington Department of Licensing, "DOL takes immediate steps to stop disclosure of information to federal immigration authorities," Jan. 15, 2018, https://licensingexpress.wordpress.com/2018/01/15/dol-takes-immediate-steps-to-stop-disclosure-of-information-to-federal-immigration-authorities/.

4 ICE is able to obtain DMV information through VCIN because (1) VA DMV entered into a voluntary agreement with VSP that allows it to grant other government entities access to DMV data through VCIN, and (2) VSP has granted ICE access to VCIN's DMV data via the Nlets access switch.

5 This information was confirmed through FOIA.

6 Information use agreement with ICE, 2018, https://www.muckrock.com/foi/virginia-128/ice-mous-moas-virginia-department-of-motor-vehicles-76744/#file-799728.

7 VA DMV has stated that they would renew the agreement if ICE requested it.

8 See e.g. Max Rivlin-Nadler, "How ICE Uses Social Media to Surveil and Arrest Immigrants," The Intercept, Dec. 22, 20219, https://theintercept.com/2019/12/22/ice-social-media-surveillance/ (an example of an ICE raid and arrest where the agency obtained the individual's residential address through use of Thomson Reuter's data intelligence tools which pulled up information from the individual's California DMV license); Mijente, Report: Who's Behind ICE?, Oct. 2018, https://mijente.net/2018/10/whos-behind-ice-the-tech-companies-fueling-deportations/.

9 Currier, Cora, "Lawyers and Scholars to LexisNexis, Thomson Reuters: Stop Helping ICE Deport people," The Intercept, Nov. 19, 2019, https://theintercept.com/2019/11/14/ice-lexisnexis-thomson-reuters-database/ (last visited Jan. 19, 2021).

[10] Funk, McKenzie, "How ICE Picks its Targets in the Surveillance Age," The New York Times, Oct. 2, 2019, https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html (last visited Jan. 21, 2021).

[11] Simon, Morgan, "Reuters Shed Light On Family Separation, But Its Parent Company Has Nearly $50 Million In Contracts With ICE. Shareholders Want Answers," Forbes, May 14, 2020, https://www.forbes.com/sites/morgansimon/2020/05/14/reuters-reporters-shed-light-on-family-separation-behind-closed-doors-reuterss-parent-company-has-nearly-50m-in-contracts-with-ice-shareholders-want-answers/?sh=3ab23451a666; Tech companies quietly work with ICE as border crisis persists, NBC News, Jan. 21, 2021, https://www.nbcnews.com/tech/tech-news/tech-companies-quietly-work-ice-border-crisis-continues-n885176.

[12] For example, a 2016 audit by PennDOT, Pennsylvania's DMV office, indicated that LexisNexis failed to follow certain safety protocols to safeguard DMV information including disclosing driver information to a third party without obtaining PennDOT's consent and failure to provide adequate customer safeguards to ensure the security of personal information. See Commonwealth of Pa., Bureau of Audits, Report on LexisNexis Risk Solutions, Inc., (2016), https://philadelphia.cbslocal.com/wp-content/uploads/sites/15116066/2018/06/lexisnexis-report_redacted.pdf; see also Prof. Caitlin Barry, Secure Our Data: Protecting the Privacy of Pennsylvania Residents and Drivers, Sept. 2020, Farmworker Legal Advocacy Clinic, University of Villanova Law School, https://drivingpaforward.org/wp-content/uploads/2020/09/Secure-Our-Data-Hit-the-Brakes-on-Information-Sharing.-Driving-PA-Forward-2020-1.pdf; Is your DMV data safeguarded properly?, USA Today, Mar. 17, 2015; Office of the Legislative Auditor, State of Minnesota, Evaluation Report, Feb. 2013, https://www.auditor.leg.state.mn.us/ped/pedrep/ledatabase.pdf.

[13] A number of jurisdictions including New York and New Jersey have legislation that requires notification of a civil immigration request for DMV information to the subject of the request. See S.B. 1747B , Section 1 § 2(12)(A), 2019 Leg., Reg. Sess. (N.Y. 2019), https://www.nysenate.gov/legislation/bills/2019/S1747.

[14] ICE has misused other state criminal justice databases for civil immigration enforcement purposes. In October 2019, the California Attorney General denied ICE access to CLETS, the state criminal justice database operated by the Attorney General, because ICE could not certify that the agency would not use the data to enforce civil immigration law, a misuse of the state criminal justice database. "California DOJ Cuts Off ICE Deportation Officers State Law Enforcement Database," Electronic Frontier Foundation, Dec. 2019, https://www.eff.org/deeplinks/2019/12/california-doj-cuts-ice-deportation-officers-state-law-enforcement-database.