STATE DRIVER'S LICENSE DATA: BREAKING DOWN DATA SHARING AND RECOMMENDATIONS FOR DATA PRIVACY

JUST FUTURES LAW

TABLE OF CONTENTS

I. REPORT FRAMING 1

II. HISTORICAL AND LEGAL BACKGROUND 4

III. BREAKING DOWN STATE DMV DATA SHARING 7
- 1 ICE Access to the DMV Database 7
- 2 Data Sharing with Private Companies and Actors 9
- 3 Data Sharing with Law Enforcement Information Sharing Networks 11
- 4 Data Sharing within Law Enforcement Fusion Centers 15
- 5 National DMV Data Programs 17

IV. Compliance and Implementation Recommendations 19

V. READ UP! Additional Resources 22

Appendix I. Frequently Asked Questions 23

Appendix II. Suggested Steps for Identifying and Addressing State Law Enforcement Data Sharing Systems 25

Appendix III. State by State Practices 28

End Notes 29

ABOUT JUST FUTURES LAW

Just Futures Law is a women of color-led immigration lawyering project that works to support the immigrant rights movement in partnership with grassroots organizations. JFL staff have decades of experience in providing technical assistance, written legal resources, litigation and training for attorneys, advocates, and community groups in various areas of immigration law, particularly at the intersection of criminal and privacy law.

Writer: Julie Mao
Editors: Paromita Shah, Sejal Zota
Graphic Design: Luz Chavez, Mijente
Photo Credits: Fernando Lopez, Matthew Gossage, Movimiento Cosecha, Organized Communities Against Deportations, Maru Mora-Villalpando

ACKNOWLEDGMENTS

Just Futures Law would like to thank Jacinta Gonzalez of Mijente, Mizue Aizeki of the Immigrant Defense Project, Brenda Valladares of Movimiento Cosecha, Edward Hasbrouck of the Identity Project, Joan Friedland of the National Immigration Law Center, David Menninger, Maru Mora-Villalpando, Zoe Li, Angélica Cházaro, and César Cuauhtémoc García Hernández for their expertise, feedback and assistance on this report.

ENDORSEMENTS

JUST FUTURES LAW

Advancement Project

AI Now

Immigrants' Rights & Human Trafficking Program Boston University School of Law

Casa De Maryland

Center for Constitutional Rights

Center for Popular Democracy

Detainee Rights Clinic of the Binger Center for New Americans

Electronic Frontier Foundation

Fight for the Future

Georgia Latino Alliance for Human Rights

Grassroots Leadership

The Meyer Law Office

Immigrant Defense Project Immigrant

Immigrant Legal Resource Center

Legal Aid Justice Center

MacArthur Justice Center

Make the Road New Jersey

Make the Road New York

Media Justice

Mijente

Movimiento Cosecha

Organized Communities Against Deportations

Southeast Asian Resource and Action Center

University of California Irvine Law School Immigrant Rights Clinic

Washington Square Legal Services Immigrant Rights Clinic

I. REPORT FRAMING

The Department of Homeland Security (DHS) increasingly relies on big data and technology to conduct raids and deportations. As states, cities, and technology companies collect more and more data about all of us, DHS has been finding ways to access and stockpile our personal data and acquire new technologies to locate individuals and carry out its arrests and deportations.

Data from state motor vehicle license and registration departments (herein "DMV") is one of the main sources of information that Immigration and Customs Enforcement (ICE) uses for conducting immigration enforcement. This is in part because DMV data along with local criminal justice information is easy for ICE to access. In the last few years, multiple investigations by journalists, data privacy groups, and community advocates have exposed how states are sharing and selling large amounts of personal data from DMV databases to private companies and law enforcement agencies including ICE.

Disturbingly, the information from DMV databases contain some of the most sensitive information about a person—such as an individual's photo, date of birth, social security number, and home address. Sharing such data with police or private parties can have serious consequences, particularly for vulnerable communities—from domestic violence survivors, abortion health providers to civil rights activists. For immigrants at risk of deportation, it has sometimes led ICE to their doorsteps.[1]

I. REPORT FRAMING

Such broad data sharing and profit making is particularly concerning as states across the country have passed or consider passing laws granting driver's licenses to residents regardless of immigration status. These legislative efforts are the result of years of advocacy and organizing by immigrant, faith, and civil rights groups. Their struggles for permanent protection and liberation should not come at the cost of more fear and criminalization. Residents should not have to choose between the risk of police arrest and ICE transfer for driving without a license and the risk of ICE showing up at their home address.

As we look to state and local political stakeholders to protect our communities, including through expanding state driver's license eligibility, we must ask that states and localities do more to protect our personal data from corporate misuse and the immigration dragnet.

While few state laws protect an individual's DMV information from disclosure, there have been some encouraging developments. For example, recently passed driver license laws in New York and New Jersey aim to prohibit ICE from directly accessing DMV databases unless the agency has a criminal warrant. Other states have issued agency directives and are exploring legislation regulating the private sale of DMV data.[2]

Moreover, pushed by organized communities demanding accountability, cities and states are now taking action to address larger issues of data collection, data sharing, and surveillance technology, from facial recognition technology to license plate readers to flawed gang databases.

The purpose of this report and recommendations is to assist organizers, policy makers, and communities in taking collective action to protect the personal DMV data of residents, particularly in states that have passed or are currently considering laws that expand driver's license eligibility.

I. REPORT FRAMING

Some key recommendations include:

- **States Should Stop Sharing DMV Data Directly with ICE:** Many states share information from their DMV database directly with ICE. Responding to ICE requests for DMV data such as a driver's license photo and residential address is voluntary. Many states and localities already have laws and policies to limit sharing of addresses, school information or other sensitive personal data with ICE. Localities should consider similar laws for DMV data.

- **States Should Stop Selling DMV Data to Private Companies:** States should consider limiting the sale of DMV data to corporations that will turn around and sell our information for profit. Our data should not be for sale. Moreover, it allows ICE to bypass data protections placed on direct access to DMV data by simply buying it from these companies.

- **States Should Stop Sharing DMV Data with ICE through National, Regional or Local Law Enforcement Data Exchanges and Fusion Centers:** Many states are part of voluntary national, regional or state law enforcement data exchanges that allows partnering law enforcement agencies to query its state DMV data. Sometimes, ICE can be a partnering agency in these data exchanges. States should modify their data sharing through these law enforcement exchanges to limit DMV data sharing with ICE. States should also place restrictions on the use of DMV data by other participating law enforcement agencies in the data exchange.

Additionally, to provide context for our findings and recommendations, we have broken down our report into four main sections:

1. BRIEF HISTORICAL AND LEGAL OVERVIEW OF DATA SHARING AND REAL ID ACT:

In order to understand what drives state data sharing and our policy recommendations, we provide a brief history of data sharing and the REAL ID Act.

2. BREAKING DOWN DMV DATA SHARING FINDINGS AND RECOMMENDATIONS:

We take a deeper dive into five DMV data sharing findings and recommendations.

3. COMPLIANCE AND IMPLEMENTATION RECOMMENDATIONS

We provide a number of recommendations on enforcing these data privacy laws. Oversight and auditing of DMV data sharing by state agencies will be key to ensuring that privacy protections actually happen.

4. APPENDIX

We provide an Appendix for policymakers, organizers, and advocates that includes a Frequently Asked Questions two-pager discussing key questions such as retaliation from the Trump Administration and Steps for Identifying State Law Enforcement Data Sharing Systems.

Through this report, our goal is to equip readers with the ability to spot the issues in your specific state and provide key solutions. While our report does include sample legislation and drafting considerations, we do want to emphasize that there is no one size fits all "model policy". We recognize the difference in each state's data system structures, policing practices, immigration enforcement, and political climate. We hope this report serves as a starting point for a collaborative movement towards greater data privacy. Though we do not know all the ways that immigration authorities, police, or private actors might attempt to obtain personal information, we hope to supplement our report and recommendations as we learn more information on these technology and information systems.

II. HISTORICAL AND LEGAL BACKGROUND

a. Data Sharing and Selling

Law enforcement data sharing is as old as policing itself. But the method of data sharing and the scale of data collection has changed dramatically in light of new data storage and surveillance technologies. Since the 1960s, states have been sharing DMV data with other states and federal agencies through national, regional and state criminal justice information systems such as the National Law Enforcement Telecommunications System (NLETS) also known as Nlets.[3]

Since 9/11, state and federal government data surveillance and sharing has greatly accelerated with the expansion of the Department of Homeland Security (DHS) which has provided grant money to states to purchase surveillance technology, update data collection information systems, and establish fusion centers where local law enforcement agencies can coordinate information sharing across state agencies and the federal government.

In the 1990s, as states started digitizing its records, states began selling the personal data of residents in their DMV databases to private companies, which would then sell the information to third parties.[4]

Unfortunately, federal laws have fallen far short of protecting the privacy of drivers and motor vehicle registrants. Congress passed the Driver Privacy Protection Act (DPPA) in 1994, intending to regulate the sharing of DMV information by states. The law was passed after growing reports of private vigilantes using DMV data to track down and harass domestic violence survivors, abortion providers and patients, and celebrities.[5]

But the DPPA still permits the sharing of DMV database information with government agencies and its contractors among other permissible uses.[6] Furthermore, the law does not restrict states from sharing DMV data with private companies who go on to sell the data as long as the companies certify that the information will be used for a permissible purpose—such as use by any government agency.[7] Thus, it is up to local and state policy and legislative bodies to step up to pass laws and regulations to strengthen privacy protections around their residents' personal information.

> *"The selling of personally identifying information to third parties is broadly a privacy issue for all and specifically a safety issue for survivors of abuse, including domestic violence, sexual assault, stalking, and trafficking...For survivors, their safety may depend on their ability to keep this type of information private." Quote from Erica Olsen, Director of Safety Net at the National Network to End Domestic Violence for "DMVs Are Selling Your Data to Private Investigators," Motherboard, Sep. 6, 2019*

b. REAL ID LAW

Passed in 2005, the federal REAL ID Act limited the rights of immigrants in a number of ways from asylum to judicial review of deportation orders to acceptance of state identity documents for federal purposes.[8]

One of the law's sections requires that states restrict the issuance of identification documents such as driver's licenses and state identity cards to U.S. Citizens or those with legal status IF the documents are used for a federal purpose (e.g., accessing a federal building). However, the Act permits states to create driver's licenses and identity cards that are non-REAL ID compliant for residents to use for a state purpose such as driving.[9]

After the passing of the REAL ID Act, many states such as Washington, Utah, California, and Nevada enacted laws creating a separate non-Real ID driver's license or identity card for individuals who could not prove their citizenship or legal status. Unfortunately, almost as soon as states established non-REAL ID licenses, many of these states gave law enforcement agencies, including ICE, access to this information because of existing data sharing arrangements. To date, 15 states and the District of Columbia and Puerto Rico have passed laws that issue non-REAL ID driver's licenses or state identification documents.[10]

It is important to understand what the REAL ID Act does and does not require. We list some of the most relevant requirements to this report below:

1. REAL ID LICENSE APPLICANT'S INFORMATION IS SENT TO DHS'S SAVE SERVICE.[11]
In order to obtain a REAL ID compliant card, the REAL ID Act requires that the DMV office share an applicant's information with the DHS's SAVE service to verify lawful immigration status for noncitizens at the REAL ID application stage. Note: this query of SAVE is not required for non-REAL ID cards.[12]

2. STATE MAINTENANCE OF A DMV DATABASE:
The REAL ID Act requires that states maintain a motor vehicle database that contains all data fields printed on drivers' licenses and identification cards and drivers' histories. Note: states have interpreted this data retention provision to apply to both REAL ID and non-REAL ID compliant cards.

3. STATE-TO-STATE SHARING OF DMV DATA:
The REAL ID Act and regulations require that states share DMV data with other states for verification purposes.[13] States have interpreted this data sharing requirement to include sharing both REAL ID and non-REAL ID compliant cards in the DMV database. *See* Section III(5) for a discussion of this data sharing including concern that the federal government may attempt to acquire access to this data sharing system.

4. THE REAL ID ACT DOES NOT REQUIRE THAT STATES SHARE THEIR DMV DATABASES WITH THE FEDERAL GOVERNMENT.
Of course, a number of states share their DMV databases with ICE and other law enforcement agencies voluntarily, and there is concern that the DHS is attempting to obtain this data through other means which we will discuss in this report at Section III(3)-(5).

c. ICE Use of DMV Data

ICE seeks drivers' license and motor vehicle registration information for its enforcement actions, including home and worksite raids. ICE considers DMV data more reliable than its own databases for surveillance and targeting purposes.[14] There are a number of ways ICE and other immigration enforcement agencies use DMV data.

1. RESIDENTIAL ADDRESS INFORMATION

ICE uses residential address information from DMV records for a last known address in order to conduct home raids. As ICE explains in its own words, "ICE uses DMV data primarily to assist in locating its priority targets (e.g., by obtaining the address of record)."[15]

2. PHOTOGRAPHS

ICE uses photos from DMV records for raids and to "verify" identities using facial recognition programs. ICE uses driver's license photos during raids to surveil and arrest the targeted individual.[16] Additionally, recent investigations have revealed that ICE is scanning large amounts of state driver's license photos through facial recognition software to match and verify identities.[17] Lastly, ICE is building technology and surveillance infrastructure that can use photos to locate individuals using surveillance cameras and real-time facial recognition software. ICE is already purchasing and installing surveillance cameras in streetlights.[18]

4. MOTOR VECHICLE REGISTRATION INFORMATION

ICE can use motor vehicle registration information combined with license plate reader data to obtain time and location mapping of an individual's driving routes. Many city police departments have installed automatic license plate readers on patrol cars and major corridors and high traffic areas of the city. Oftentimes, other law enforcement agencies including ICE can access the license plate reader data through regional sharing systems and networks. Having access to license plate reader data and a person's vehicle registration information, ICE can connect individual names to their license plate numbers.[19] This would allow ICE to track and record an individual's movement in real time. Additionally, motor vehicle registration information also contains residential addresses that could then be used to conduct home raids.

III. BREAKING DOWN STATE DMV DATA SHARING

Below we breakdown the major ways that states share DMV data with law enforcement and private companies, and outline key law or policy recommendations for protecting the data privacy of residents in DMV databases.[20]

Note: while these recommendations may be relevant to protecting the data privacy of individuals with non-REAL ID compliant licenses given the risk of information being used for immigration enforcement, these recommendations can and should apply to DMV data generally, unless explicitly stated.

1. ICE ACCESS TO THE DMV DATABASE

For years, states such as Washington, Vermont, Nevada, Utah, Virginia, North Carolina, and Georgia have granted local and federal law enforcement agencies, including ICE, access to information from the DMV database.

This information sharing may happen in a number of different ways depending on the state. Communities should be on the lookout for the following data sharing methods:

- DMV grants direct user access of the DMV database to ICE. This means that ICE can automatically query the database based on certain search terms.[21]
- DMV shares information in response to an ICE request for information on a specific individual. For example, ICE emails a DMV officer requesting information based on certain identifiers and the DMV officer sends back case-specific records.
- DMV shares DMV data in bulk with ICE. Bulk data means the state puts all the DMV data into a file or set of files, so that ICE can acquire all the data with a few downloads.

ICE may also have access to DMV data through a state's criminal justice data system or some other local, state, regional or national law enforcement data sharing system. *See* Section III (3).

Fortunately, in response to organized communities, investigative reporting, and public outcry, a number of states have limited DMV data sharing with ICE including:

- New York and New Jersey: laws explicitly limit law enforcement access to information from the DMV database for immigration enforcement purposes absent a court order, criminal warrant, or valid subpoena.[22]
- Washington State: an executive order places data sharing limits on all state databases and a licensing agency policy restricts responses to ICE case-by-case requests absent a criminal warrant, court order, or valid subpoena.[23]
- California: law limits release of documents used to provide identity or residency except in response to a subpoena for individual records in a criminal proceeding or a court order, or in response to a law enforcement request to address an urgent health or safety need if the law enforcement agency certifies in writing the specific circumstances that do not permit authorities time to obtain a court order.[24]

III. BREAKING DOWN STATE DMV DATA SHARING

RECOMMENDATION:
States should only provide ICE access to their DMV databases if the agency can produce a criminal warrant, court order or valid[25] subpoena for a particular individual.

PRO-TIPS:
We recommend bill drafters consider legislation that is immigration neutral or avoids singling out federal immigration enforcement. Legislation that restricts the sharing of data unless there is a narrow, criminal proceeding exception provides for a more comprehensive data protection policy and recognizes that many communities along with immigrants are concerned about data sharing and privacy.

We recommend defining criminal proceeding exceptions as law enforcement investigations accompanied by a criminal warrant, court order, or valid subpoena. We caution against loose definitional language or an exceptions clause that allows access to the DMV data simply when ICE can unilaterally assert a "criminal nexus" or based on an individual's prior criminal history. Requiring a criminal warrant, court order or valid subpoena is a clearer way of distinguishing between criminal and civil enforcement.

Note: *Limiting direct ICE access to the DMV database should be treated as a preliminary step to protecting DMV data. As explained below, ICE and DHS have a number of workarounds through third party actors.*

Maru Mora-Villalpando is a long-time immigrant rights organizer in Washington State. Maru came to the attention of ICE because agents had been surveilling her activism. In 2017, ICE was able track down Maru's home address to place her in deportation proceedings using address information provided by the Washington State Department of Licensing (DOL).

In the State of Washington, the DOL provided DHS agents with two access points to its DMV data. First, it signed a user agreement with ICE and CBP for direct access to its DMV database called DAPS. Second, DOL responded to case-by-case requests for information from ICE. Pursuant to a Governor's order issued in January 2017, the agency terminated ICE and CBP's user access contracts to DAPS. But DOL continued to respond to ICE case-by-case requests for information. In 2018, after strong community push back including Maru's case, DOL issued a policy limiting staff from responding to ICE requests for information.

2. DATA SHARING WITH PRIVATE COMPANIES AND ACTORS

Even if a state database prohibits ICE from directly accessing the database, ICE can obtain the data through a private-sector workaround. This is possible because state governments have a long-standing practice of sharing and selling their DMV data to private companies for commercial purposes.

Over the years, states such as New Jersey, Washington, California, New York, Texas and Vermont have made millions of dollars from selling the information of residents in their databases including names, dates of birth, and addresses to private entities such as data brokers, private investigators, and insurance companies.[26] For example, the State of Washington collects close to $30 million a year from its Department of Licensing selling driver and vehicle records to some 35,000 private companies.[27]

There are a number of ways that states sell data to private actors:

- Bulk data or contract sales: DMV sells license and registration data through a procurement process and signs an agreement with the company for sale and use of bulk data. Bulk data refers to putting all data into a file or set of files, so that all of the data can be acquired with a few downloads.

The California DMV made $51 million dollars in 2019 selling its data to private companies including to data brokers. One recipient is LexisNexis which has a multimillion-dollar contract with ICE for use of its search platforms.[28]

- Pay per search: a private actor applies to DMV to use its online DMV search platform and signs an agreement. Private actor is charged per search of the database. Search account holders must have a DPPA permissible use for every search performed and DMV monitors their compliance through an audit program.

- Over-the-counter queries: private actor visits a State or County DMV office to purchase a driver license record.

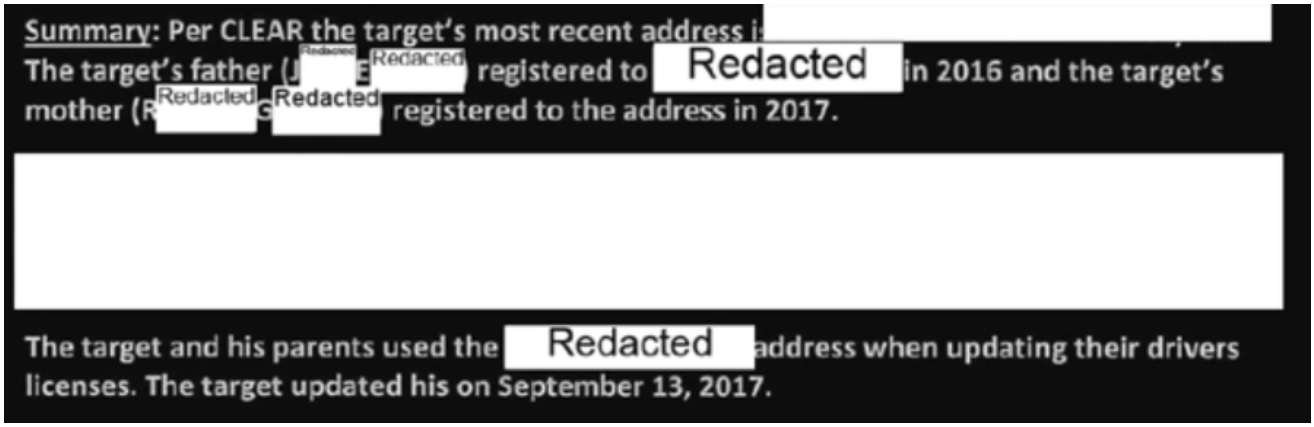
It is important to note that while federal laws require that states share DMV information to private actors under limited circumstances relating to manufacturer safety and recalls, vehicle emissions, and theft, the sharing and selling of DMV data by states to private companies is otherwise voluntary.

Once these private companies obtain this DMV data, they can turn around and sell or license the data to ICE and other entities. This arrangement allows ICE to circumvent restrictions imposed by state laws or policies such as those in New Jersey and New York limiting direct ICE access to the database. Data brokers pose a particular threat to data security.

Data brokers (also called information reseller, information broker, data aggregator) are companies that stockpile large amounts of personal information, public record information, online history, social media, or other information about people and sell that data to law enforcement and other private actors.[29] LexisNexis, Thompson Reuters, TransUnion, and Acxiom are some of the most notable ones. We know that at least LexisNexis and Thompson Reuters sell their data to ICE for use in immigration enforcement.[30]

III. BREAKING DOWN STATE DMV DATA SHARING

Excerpt of ICE intelligence report confirming ICE's use of Thompson Reuters's CLEAR database to pull driver's license and motor vehicle registration data in California to find the address of an individual and his family.[31]



RECOMMENDATION:
In order to plug this private sector loophole, we recommend that states pass legislation that limits data sharing with private parties except as required by federal law.[32]

Our data should not be for sale. Organized communities have moved cities and states to consider and pass data privacy laws to limit corporate data collection.[33] States should consider limiting the sale of DMV data to corporations that profit from our information. Some states alternatively have considered continuing to sell information to private companies but restrict the use and sharing of information for immigration enforcement purposes. We caution that this limited use model is seriously susceptible to misuse particularly when private companies are reselling data to other companies and states have limited auditing and compliance capacity.

PRO-TIPS:
Bill provisions stating that DMV information is not subject to disclosure under public record law may not be sufficient for protecting against third party disclosure. As stated above, there are a number of ways that states share DMV data with private actors. State disclosure to commercial data brokers such as Thomson Reuters or LexisNexis usually involve bulk data transfers or a procurement process, not a public records request or pay per search process.

Want to know what companies or individuals have purchased your state's DMV data? File a state public records request with the state agency that responds to requests for DMV data. This is usually a state's office for driver's license and motor vehicle registration information. The agency likely retains a list of data purchases for the last few years.[34] Additionally, the federal Driver Privacy Protection Act requires resellers of DMV data to retain a list of person(s) or entities that receive the data for a period of 5 years and must make such records available to the motor vehicle department upon request.

3. DATA SHARING WITH LAW ENFORCEMENT INFORMATION SHARING NETWORKS

For decades, ICE's main source for DMV information was through national, regional, and state criminal justice databases and information sharing systems. One of ICE's major sources of DMV data is the National Law Enforcement Telecommunication System (NLETS), now referred to as Nlets, which is a national information sharing network and message switching service.[35] Founded in 1966, Nlets is structured as a non-profit corporation that is owned and governed by 54 law enforcement agencies that make up its principal customers.

Nlets contains various data exchange arrangements including state DMV data. ICE and its predecessor agency (INS) has had access to Nlets, including its DMV data, since before DHS was created in 2003. Nlets DMV data exchange allows ICE to automatically query the state driver's license and vehicle registration databases of any participating state on a case by case basis.[36]

At last survey, law enforcement in all 50 states share vehicle registration and driver's license information to some extent with each other through Nlets as well as with various federal agencies, including ICE.[37]

Excerpt of email correspondence between DHS and White House obtained through FOIA by the National Immigration Law Center confirming that ICE has access to DMV data via Nlets.[38]

From: (b)(6),(b)(7)(C)
Sent: Tuesday, March 04, 2014 06:04 PM Eastern Standard Time
To: (b)(6),(b)(7)(C) Sobel, Ted
Cc: (b)(6),(b)(7)(C)
Subject: Re: NYT: California Driver's License Program Hits an Unexpected Snag

Law enforcement (including ICE) has access to DMV data, primarily through NLETS. But that is on a case by case basis - not bulk.

Its separate from the REAL ID provisions and existed before 9/11.

Nlets continues to be a major source of DMV data, allowing ICE to obtain residential address and photo information to conduct raids and deportations.

III. BREAKING DOWN STATE DMV DATA SHARING

Below is an excerpt from an ICE intelligence report describing how Nlets was used to pull driver's license information and locate the targeted individual in California.[39]

> Targeting Specialist at NCATC searched multiple databases, including USCIS's Central Index System (CIS), Computer Linked Application Information Management System the National Law Enforcement Telecommunications System (NLETS), National Criminal Information Center (NCIC) databases, and other commercial databases to produce targeted information for use by the Los Angeles field office. For this case, driver's license information was received from NLETS, an information-sharing system that links together state, local, and federal law enforcement, justice, and public safety agencies, which revealed driver's license application activity after Mr [redacted] date of removal. On or about June 16, 2017, a lead product

It is important to understand that state participation in Nlets, along with many other national or regional data exchanges, is voluntary. States can choose not to share information or limit the type of information shared through Nlets. Some states have already chosen not to share certain information, such as driver's license photos, through Nlets.[40]

PRO-TIPS:

Each Nlets member state designates a state agency as the Nlets System Agency (NSA). This designated agency is responsible for maintaining operational surveillance over the state end of the line and for providing information distribution services in and out of the Nlets network. Essentially, this is the agency that would implement limitations on data sharing through Nlets. Nlets lists each member's NSA contact on its website.[41] *See Appendix II for more details.*

III. BREAKING DOWN STATE DMV DATA SHARING

Beyond Nlets, there are a number of national, regional, and state law enforcement sharing networks that allow DMV data sharing with ICE. Many of these are criminal legal system data exchanges. Some of these information systems even allow for two-way automated information sharing with ICE, meaning ICE can query the data of law enforcement agencies participating in the data sharing network and vice versa.[42] While not specifically designed for the sharing of DMV data, these exchanges may contain personal information obtained from state DMVs. Law enforcement agencies or organizations with database information sharing agreements with ICE include:

- National Data Exchange (N-DEx): N-DEx is an FBI-maintained database containing crime incidents, criminal investigations, arrests, bookings, incarcerations, parole and/or probation reports from contributing state, local, tribal, and federal law enforcement and criminal justice entities.

- San Diego Automated Regional Justice Information System (ARJIS): ARJIS is a criminal justice network that shares information among justice agencies throughout San Diego and Imperial Counties.

- AZLink (Arizona): AZLink is a collaboration between four regional law enforcement "hub" data centers for the various regions (Central, Eastern, Northern and Southern) in the state of Arizona.

- T-DEx (Texas Department of Public Safety Texas Data Exchange): TDEx is a data repository containing information from law enforcement agencies in the state of Texas. It allows participating agencies to access the state's driver's license and motor vehicle registration data.[43]

- LInX NW (Law Enforcement Information Exchange Northwest): This is a data and information sharing network sponsored by the Naval Criminal Investigative Service (NCIS) and the U.S. Attorney's Office for the Western District of Washington state.

- LInX HR (Law Enforcement Information Exchange Hampton Roads): this is a data and information sharing network sponsored by NCIS and law enforcement agencies in the Tidewater region of Virginia.

- LInX CR (Law Enforcement Information Exchange Capital Region): this is a data and information sharing network sponsored by NCIS and several law enforcement agencies in the District of Columbia, Maryland, and Virginia metropolitan area.

- LInX SoCal (Law Enforcement Information Exchange Southern California): this is a data and information sharing network sponsored by NCIS and several law enforcement agencies in the southern region of California.

- LASD (Los Angeles Sheriff's Department): LASD operates the Incident Reporting Information System (IRIS), an information sharing data system which consolidates LASD's records management, citation, jail information, and dispatch systems.

III. BREAKING DOWN STATE DMV DATA SHARING

Recommendation:
Limit DMV information sharing with ICE through law enforcement data systems and require other law enforcement agencies with access to the state's DMV data to certify that it shall not use the data for immigration enforcement purposes.

As previously discussed, states are not required to share DMV data such as residential addresses or photos with the federal government.[44] The States of New York and California have already taken action to limit DMV information sharing through its criminal justice data systems with ICE.

For example, in 2017, California passed Senate Bill 54 which requires that the State Attorney General publish guidance, audit criteria, and training recommendations that limit the use of state and local law enforcement databases for immigration enforcement "to the full extent practicable and consistent with federal and state law."[45] In October 2019, in light of SB 54 and community advocacy, the California Department of Justice revoked ICE Enforcement and Removal Operations's access to CLETS, a state criminal justice database operated by the California Department of Justice in which DMV data could be queried.[46] Additionally, during the same month, regional database ARJIS cancelled its user agreements with ICE and implemented a number of changes to the database including removal of immigration records and deletion of immigration status inputs.[47]

In New York, prior to the implementation of its expanded driver's license law, the state ended ICE's access to DMV data through its e-JusticeNY Integrated Justice Portal, an access point to various criminal justice-related databases as well as DMV records.[48]

We understand that it can be challenging to navigate through the large web of state and local data collection systems and networks to identify those that can query DMV data and grant such access to ICE. In Appendix II, we provide suggestions to organizers, community advocates and policymakers on how to implement this recommendation.

4. DATA SHARING WITHIN LAW ENFORCEMENT FUSION CENTERS

Fusion Centers are law enforcement operations hubs for information sharing between local, state, federal and private entities - sharing everything from tax records, financial records and criminal records to driver's license information. These centers are usually local or state-owned and receive support from federal partners in the form of staffing, training, technical assistance, and IT support to establish connectivity between local and federal data systems.[49] Their primary federal partner is DHS.

Since their creation in 2006, fusion centers have had a documented history of civil rights abuse and troubling surveillance, from racial profiling to surveillance of protesters to religious discrimination.[50]

Photo of Maryland Fusion Center from Getty Images

Obviously, fusion centers are a vulnerability for DMV data privacy as the purpose of fusion centers is to coordinate information sharing across various local and federal law enforcement databases and staff. For one, ICE could be a direct partnering law enforcement agency of the center, and therefore staff the center or have access to the databases of other partnering law enforcement agencies. Second, even if ICE is not a partnering agency, staff of the fusion center could share information with ICE upon ICE requests to run queries.[51]

III. BREAKING DOWN STATE DMV DATA SHARING

Case example: The Boston Regional Intelligence Center (BRIC) is a fusion center operated by the Boston Police Department. The Department of Homeland Security is a partnering agency and staffs the fusion center with at least one analyst. Recent litigation confirmed that ICE was able to obtain information on high school students because Boston Public School's incident reports, which are accessible to the Boston Police Department, is shared through the BRIC Fusion Center with partnering agencies.[52]

"In a typical fusion center, an FBI agent might be sitting next to a state highway patrol officer. They don't merely share space, they share databases and techniques" Janet Napolitano, DHS Secretary, 2009, CNN.

RECOMMENDATION:

We recommend the following two steps to addressing fusion center access to state DMV databases.

First, research the fusion centers in your state: find out which fusion center(s) operates in your city, county or state, particularly what law enforcement agency operates the center and what are the partnering law enforcement agencies. Fusion Centers are operational in all 50 states, Puerto Rico, Guam, and the U.S. Virgin Islands. The DHS website provides a complete list.[53]

Second, consider the following options for addressing vulnerabilities with the DMV database depending on the operating structure of the fusion center after identifying which law enforcement agency is responsible for operating the fusion center:

- Enact a local law or policy limiting the fusion center staff from granting ICE or other federal immigration authorities access to information in DMV database or responding to ICE requests for fusion center staff to run queries and share information in the DMV database absent a criminal warrant, valid subpoena, or judicial order.

- Require other local or federal agencies with access to the fusion center database to certify that they will not use the DMV data to enforce federal immigration law. The purpose of requiring this certification is to address ICE attempts to access data through other law enforcement proxies. A common fusion center database is COPLINK. *See* Section IV for certification language.

- Require regular auditing, documentation of ICE requests and responses, and certifications by other law enforcement agencies.

5. NATIONAL DMV DATA PROGRAMS

There are two national data systems which allow states to share DMV data with each other: (1) the State Pointer Exchange Services (SPEXS) which hosts the State-to-State (S2S) Verification Service and allows states to access both REAL-ID and non-REAL-ID compliant card information and (2) the National Driving Registry which provides more limited information on drivers whose licenses have been suspended or revoked or have been convicted of a serious traffic violations.

RECOMMENDATION:
We recommend that participating states closely monitor these state-to-state databases for DHS or other federal law enforcement agency actions to obtain this data. In the case of SPEXS, states should limit the amount of data retained by SPEXS and require the operator AAMVA to notify the state should a third-party attempt to access its DMV data to the extent possible. Additionally, states can require user certifications from other states limiting the use of its data for federal immigration enforcement purposes. States have a lot of authority over how these databases operate given that they are primarily created for state use. Lastly, we recommend states consider imposing penalties for misuse or unauthorized access of the data.

- **State-to-State Sharing Requirement in the REAL ID Act**

Under the REAL ID Act, states are required to maintain a DMV database containing data for both REAL-ID and non-REAL-ID compliant cards and share the database with other states. *See* Section II. In practice, the only mechanism available that satisfies this state-to-state data sharing mandate is participation in the State-to-State (S2S) Verification Service which is accessed through the State Pointer Exchange Services (SPEXS).

Both data systems are operated by a non-governmental entity, the American Association of Motor Vehicle Administrators (AAMVA), a private entity consisting of the directors of each state DMV office. SPEXS functionally operates as a limited DMV database and is hosted by a private commercial cloud service. While S2S is a data exchange, AAMVA requires states upload some DMV data onto SPEXS in order to conduct its state-to-state queries. As of 2015, the information retained by SPEXS appears to be limited to driver's license holder name, date of birth, gender, and social security number, not address or photo.[54] But this may change. To date, 27 states contribute their DMV data to the S2S Verification Service.[55]

We do not believe that DHS or its component agencies have access to SPEXS or its S2S service. And to be clear, state participation in this data exchange is in itself completely voluntary. DHS has certified states that do not participate in this service as REAL ID Act compliant. But this is an area of emerging practice. While the REAL ID Act does not require that states share their DMV databases with the federal government, there has been some concern by privacy experts that federal agencies could compel AAMVA or its commercial hosting provider to share the SPEXS database to effectively create a federal DMV database.[56]

III. BREAKING DOWN STATE DMV DATA SHARING

On a related note, the Department of Justice recently issued a memorandum on January 27, 2020 that purportedly outlines a number of ways that it could create end runs around states that limit DHS's direct access to its DMV data.[57] One of the ideas includes asking "friendly" states to share the DMV data of "uncooperative states" that do not share the data with DHS based on this state-to-state sharing requirement. For a discussion of other DOJ tactics listed in the memorandum, please see Appendix I.

- **National Driving Registry (NDR)**

The NDR is a computerized database of information on drivers who have had their licenses revoked or suspended, or who have been convicted of serious traffic violations, such as driving while impaired by alcohol or drugs. The purpose of NDR is to provide state DMV offices and other federal agencies that license motor vehicle operators with centralized access to information on "problem drivers." States use this information to make driver license issuance decisions.

NDR is operated by the National Highway Traffic Safety Administration (NHTSA), within the Department of Transportation (DOT). States have access to the information through AAMVA. State participation is optional; and state DMVs maintain access and security controls to their own systems.

It is important to understand what information is and is NOT stored in NDR. State DMVs provide NDR with a relevant individual's full name, other names used, date of birth, sex, and driver license number. Some state DMVs do choose to share social security numbers, height, weight, and eye color. However, NDR does not disclose the content of a driver's record, photo, or residential address. Such information would still need to be obtained directly from the state DMV office or through other means.

We do not know at this time if ICE has regular access to NDR. According to NDR's Privacy Impact Assessment, some federal agencies are allowed to send case-by-case requests for information to the NDR. These include agencies that employ motor vehicle operators, FAA for airman medical certifications, FRA (and railroads) for locomotive operators, Coast Guard for merchant mariners and servicemen, and NTSB and FMCSA in connection with accident investigations.[58]

IV. COMPLIANCE AND IMPLEMENTATION RECOMMENDATIONS

Below we breakdown the major ways that states share DMV data with law enforcement and private companies, and outline key law or policy recommendations for protecting the data privacy of residents in DMV databases.

Note: while these recommendations may be relevant to protecting the data privacy of individuals with non-REAL ID compliant licenses given the risk of information being used for immigration enforcement, these recommendations can and should apply to DMV data generally, unless explicitly stated.

Compliance monitoring is critical to enforcing data privacy laws, particularly given the technical nature of state data and information management systems. Without proper mechanisms for oversight and review, it is hard to know whether state and local agencies are implementing data sharing limitations and complying with limited use agreements. Below are a number of recommendations for monitoring state compliance with data privacy protections.

1. ENACT ROBUST AUDITING, REPORTING, AND NOTIFICATION REQUIREMENTS FOR DMV OFFICES AND STATE AND LOCAL AGENCIES TO ENFORCE COMPLIANCE

Robust reporting and auditing of DMV and state and local enforcement agencies is necessary for ensuring long-term compliance with data protection policies. There have been a number of instances where states have passed strong laws on paper limiting data sharing or use, but faced significant implementation challenges at the agency or database level.

For one, even when the use of a state government database is clearly delineated, the database can be vulnerable to misuse if there is not a robust auditing system in place. For example, the California Law Enforcement Telecommunications System (CLETS) is clearly intended for use in criminal related investigations. However, an investigation conducted by the Electronic Frontier Foundation found hundreds of violations of CLETS's use agreement by law enforcement, such as using the database to vet potential dates or spying on former spouses.[59]

Moreover, localities often do not know how many databases exist, are unfamiliar with their data use and sharing practices, or lack the technical understanding to implement the changes.

For example, in 2017, the Governor of Washington State issued an Executive Order explicitly prohibiting state agencies from sharing personal information with ICE. Yet, the state DMV office continued to respond to ICE requests for information in its DMV database for nearly a year after the order's issuance, and only stopped in mid-2018 as a result of advocates and journalists exposing its collaboration with ICE.[60]

Now, the Washington State Department of Labor issues user data agreements that add the following use restriction language: "Licensee is strictly prohibited from using Data for purposes of investigating, locating, or apprehending individuals for immigration related violations." [61]

In another example, the California Values Act passed in 2017 and limited state law enforcement from using resources to assist in immigration enforcement. Specifically, it required that the State Attorney General publish guidance to ensure to the "fullest extent practicable" that state and local law enforcement databases are not used to enforce immigration laws. It was only in October 2019, after years of advocacy efforts, that the California Attorney General denied ICE access to its CLETS database.

Now, California DOJ recommends that the following certification language be added to criminal misuse warnings on the login screens of state databases: "Federal, state or local law enforcement agencies shall not use any non-criminal history information contained within this database for immigration enforcement purposes. This restriction does not pertain to any information regarding a person's immigration or citizenship status pursuant to 8 U.S.C. 1373 and 1644."[62]

Here are a number of recommended reporting and monitoring requirements for state agencies to ensure compliance with limitations on DMV data sharing:

- Require the DMV to notify an individual if the office releases an individual's information to a law enforcement agency.[63]
- Require state and federal agencies with access to the information in the DMV database to certify on an annual basis that they do not use or share the information for immigration enforcement purposes.
- Require an annual audit of state and federal agency use of the DMV data by a neutral state agency.[64]
- Require the DMV and other state agencies with access to information in the DMV database to (1) document all requests from immigration agency for DMV information, (2) document all responses from state agencies to these requests, (3) publish public reports routinely on the requests and response, and (4) designate an oversight board to hold hearings and follow-up on reports.[65]

2. CONSIDER A PRIVATE RIGHT OF ACTION FOR VIOLATIONS OF DATA PROTECTIONS LAWS

Including a private right of action in a data privacy law allows individuals to bring claims for violations of the data law in a court and receive money damages (and possibly civil penalties, or money paid as a punishment) and attorneys' fees. A private right of action allows individuals to bring private enforcement actions to ensure compliance with the law.

A number of federal and state privacy laws have a private right of action including the Driver Privacy Protection Act, the Fair Credit Reporting Act (FCRA), and the Illinois Biometric Information Privacy Act.

3. CREATE A LIMITED DOCUMENT RETENTION POLICY FOR NON-REAL ID APPLICATIONS AT THE DMV OFFICE

DMV offices should consider limiting the types of information requested at the application stage and have a limited document retention policy on sensitive identity documents related to the application process.

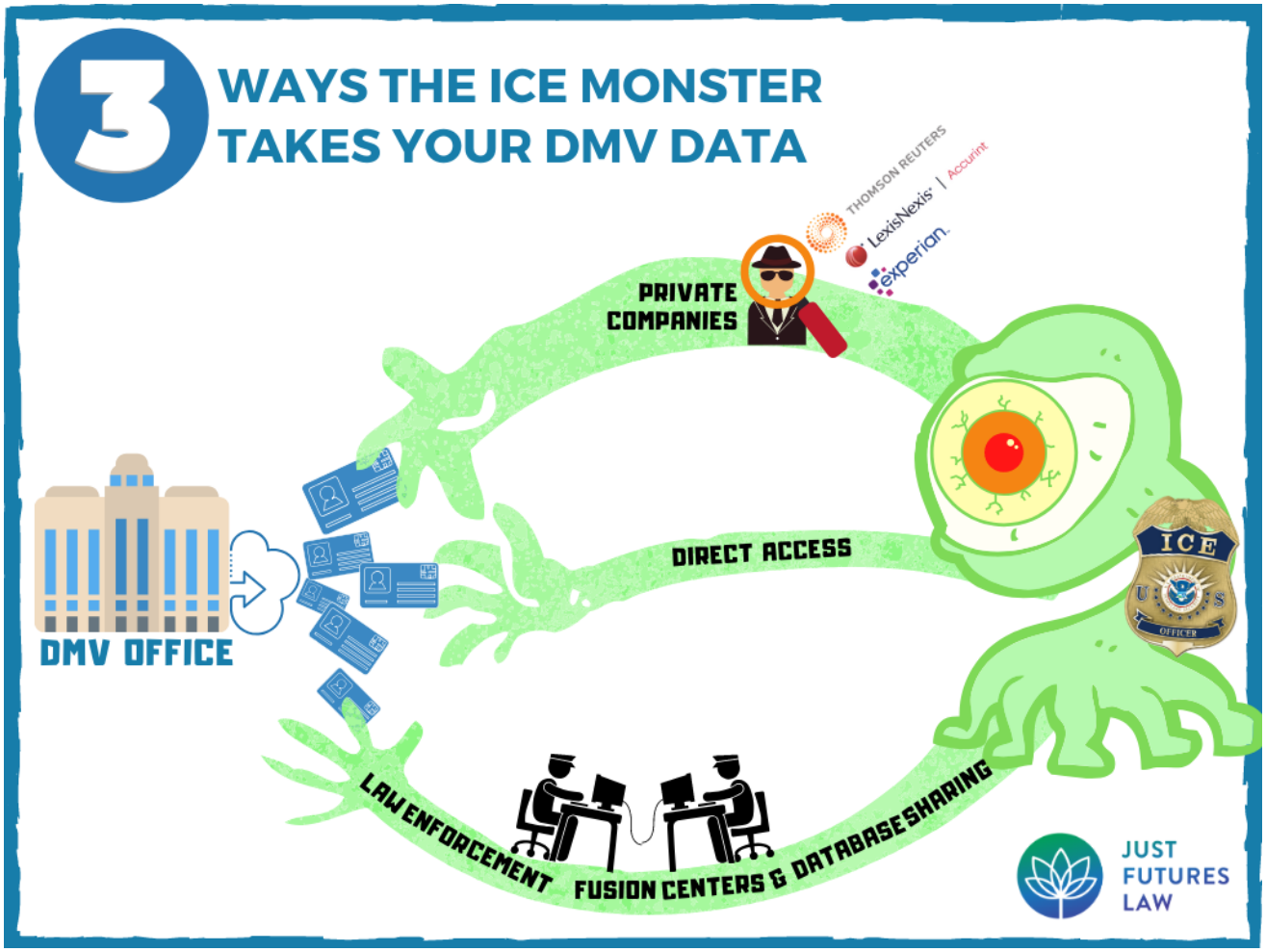
Limiting data collection at the front end avoids the need to limit data sharing at the backend. This is good practice for any agency or office that handles sensitive data such as information related to date of birth, SSN numbers, birth certificates, etc.[66]

Remember there is no federal law that requires that DMV offices to collect information on a person's nationality, place of birth, or immigration status for issuing state driver's licenses or identification cards that are non-REAL ID compliant. For example, in 2018, the State of Washington's driver's license office stopped requiring information on place of birth during the application process.[67]

Note: A state policy that simply does not collect immigration or nationality information is insufficient by itself to protect privacy. When ICE searches for DMV information, ICE likely already has information about immigration status and is rather searching for location or photo information to create a raid target list. ICE has huge data sets on individuals that it suspects of immigration violations from its own databases or other sources.

V. READ UP! ADDITIONAL RESOURCES

- Just Futures Law, Mijente, and UCI Immigrant Rights Clinic, Take Back Tech Toolkit, July 2019.
- Mijente, IDP, and NIPNLG, Who's Behind ICE? The Tech Companies Fueling Deportations, Aug. 23, 2018.
- Driver's Licenses, National Immigration Law Center, last updated Feb. 2020.



APPENDIX I. FREQUENTLY ASKED QUESTIONS

1. WHAT ARE CONSIDERATIONS FOR ORGANIZERS AND COMMUNITIES STILL DECIDING WHETHER TO TAKE ON A NON-REAL ID DRIVER'S LICENSE CAMPAIGN IN OUR STATE?

For those weighing whether to take on a campaign to expand state driver's license eligibility consider:

> Campaigns for decriminalization of driving without a license: One of the biggest concerns for individuals who drive without a license is the risk of police arrest, imprisonment, and significant fines. For immigrants, there is the additional risk of ICE transfer through the police traffic stop or jail. In recent years, in response to community organizing and campaigns, a number of municipalities have decriminalized driving without a license and other low-level offenses. These campaigns may be particularly relevant if you operate in a region or political climate where limiting data sharing between local and federal immigration authorities is a hard lift or prohibited by state law. For example, in the wake of SB 4, a Texas state law prohibiting localities from passing policies to limit collaboration with ICE, Austin City Council passed the Freedom City law directing its police department to stop arresting individuals for misdemeanors which includes driving without a license amongst other low-level offenses.[68]

Campaigns to address data privacy in state data collection: organizers and communities should consider passing data protection laws before tackling expanding DMV license eligibility. Immigrant groups are not alone in concerns around government and corporate surveillance and overreach. Consider joining with privacy and criminal justice advocates in building an intersectional coalition to pass data privacy protections addressing vulnerability in state DMV data, amongst other privacy concerns.

2. THE DAMAGE IS DONE, WHAT CAN MY STATE DO TO REMEDY THE DATA THAT WAS ALREADY SHARED WITH ICE OR OTHER PRIVATE COMPANIES?

For those in states which have already passed non-REAL ID driver's license laws without sufficient data protections, you can implement the above recommendations prospectively, either in the form of amending the legislation or advocating for the relevant agencies to issue policy orders, guidance or procedures.

When it comes to the sale of DMV data to private parties, some state governments are examining how they can claw back their DMV data from private companies since states own their DMV data and can end and limit its use except when required by federal law. In some cases, states have revised their use agreements with private companies to restrict companies from using the data for the purpose of immigration enforcement. For example, Washington State has modified its user licensing agreements with existing private companies to limit the use of information for immigration enforcement purposes and conducts regular audits.[69]

APPENDIX I. FREQUENTLY ASKED QUESTIONS

3. WHAT ABOUT RETALIATION? SHOULD WE BE CONCERNED THAT THE TRUMP ADMINISTRATION COULD RETALIATE AGAINST STATES FOR LIMITING ICE ACCESS TO DMV DATA LIKE IN CASE OF NEW YORK STATE?

Communities who have resisted ICE by passing policies limiting collaboration have been fighting Trump retaliation for years--whether it be in the form of threats of raids, losing federal funding, or lawsuits.

In late January, according to Buzzfeed, the Department of Justice issued an internal memorandum to the DHS outlining a number of ways that it could pressure states into sharing DMV data or create end runs around states that limit DHS's access to its DMV data.[70] Tactics include getting the DMV data through a more friendly state since states are required to share data, potentially issuing broad subpoenas for drivers' licenses information, and more retaliatory tactics such as closing down DHS offices, refusing to accept their state identification for certain federal purposes, and cutting TSA PreCheck services.

In February 2020, the Trump Administration did retaliate against NY State's driver's license law by canceling future enrollments into its Global Trusted Traveler's program. However, just a few days later, the NY State Attorney General's Office responded by filing a federal lawsuit to stop this retaliatory action.[71]

The best defense is an organized one. Local and state elected officials and community stakeholders should be ready to defend its laws and policies through the press, litigation, community mobilization, and popular education. Many grassroots, local, and state-level groups have been fighting similar retaliatory behavior from DHS for more than a decade, particularly those working around local police and jail data sharing with ICE. Look to those immigrant and criminal justice groups for strategies around litigation, messaging, and education.

APPENDIX II. SUGGESTED STEPS FOR IDENTIFYING AND ADDRESSING STATE LAW ENFORCEMENT DATA SHARING SYSTEMS

We understand that it can be challenging to navigate through the large web of state and local data collection and storage systems. Below we provide suggestions to organizers, community advocates and policymakers on how to implement this recommendation.

- Step 1: Identify the national, regional, and state law enforcement data sharing systems to which your state contributes DMV data.

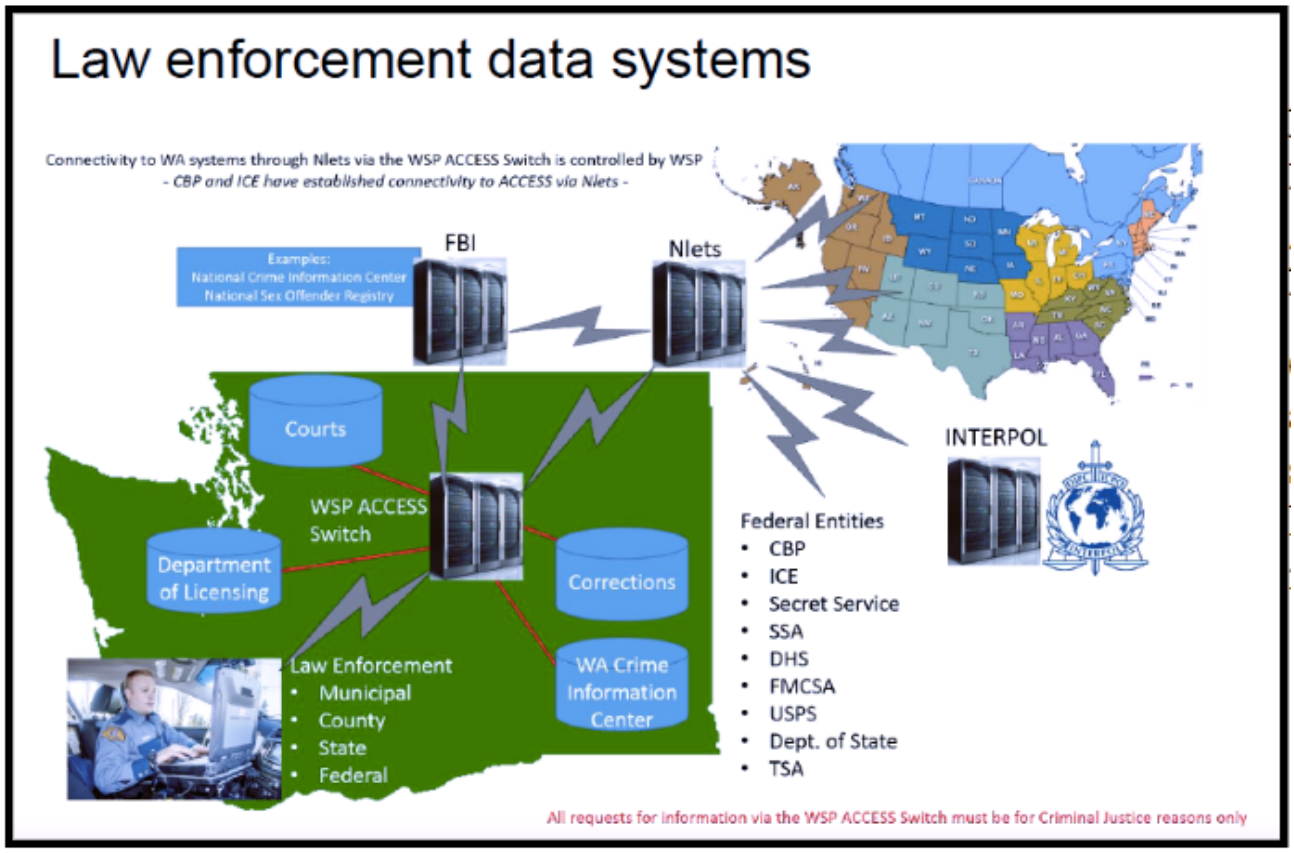
Here, the obvious data network to start investigating is Nlets since all 50 states, the District of Columbia and Puerto Rico participate in it. Other suggestions for database identification include asking questions and meeting with your state DMV office, state or local elected officials, local or state information technology office, and filing public records requests.

- Step 2: Identify which state agency is the "switch" or information access point to the data sharing system(s).

If a state or local government contributes data to a national, regional or state law enforcement data sharing system, there should be a state agency (usually a law enforcement agency) that manages access to and from the data sharing system It is important to identify the specific agency or office that manages the access point because that is the office which would have the most knowledge about the data sharing network and would implement restrictions on data sharing with the network. The agency is not necessarily the DMV office and could be a law enforcement agency such as the state police, criminal investigations bureau or state Department of Justice.

PRO-TIP:
Nlets lists each state's point of contact for data sharing with Nlets.[72] It is usually the state patrol, public safety department or state bureau of criminal investigation.

APPENDIX II



An example of how Nlets worked in Washington State in June 2018. It identifies the Washington State Police (WSP) as the designated access agency to sharing state data including license and registration information with Nlets.[73]

- Step 3: Identify whether ICE has access to the data sharing system.

We suggest asking the relevant state agencies for any data agreement(s) between ICE and the relevant agency and any data agreements between the state agencies and the data sharing system. We also suggest filing public records requests and reviewing DHS's Privacy Information Assessments which often publish the state and local databases to which ICE and other federal immigration agencies have access.

APPENDIX II

- Step 4: Ask your state or local government to limit with whom the law enforcement agency shares information, the type of information shared, and the use of such information by other law enforcement agencies.

State agencies can cancel their data sharing agreements with ICE and modify its agreements with the law enforcement agencies to restrict the use of its data for immigration enforcement purposes. Additionally, states can limit the type of information that it collects such as place of birth, and that it shares through the data sharing system such as photos.

For example, California DOJ recommends that the following language be added to criminal misuse warnings on the login screens of state databases: "Federal, state or local law enforcement agencies shall not use any non-criminal history information contained within this database for immigration enforcement purposes. This restriction does not pertain to any information regarding a person's immigration or citizenship status pursuant to 8 U.S.C. 1373 and 1644."[74] *See* also Section IV.

Auditing and certification for other state law enforcement agencies are critical to enforcing other law enforcement compliance with these use limitations. *See* Section IV.

APPENDIX III. STATE BY STATE PRACTICES

CHART OF STATE BY STATE PRACTICES HERE

END NOTES

[1] John Dillon, "For Undocumented Immigrants, Getting A Driver's License Could Spell Trouble With ICE," Northwest Public Broadcasting, Jan. 1, 2019, https://www.nwpb.org/2019/01/01/for-undocumented-immigrants-getting-a-drivers-license-could-spell-trouble-with-ice/.
[2] *See e.g.* Xander Landen, "Scott tells Vermont DMV to stop giving private investigators personal data," VT Digger, Dec. 6 2019, https://vtdigger.org/2019/12/06/scott-tells-dmv-to-stop-giving-private-investigators-personal-data/.
[3] NLETS website, available at: https://www.nlets.org.
[4] The Driver's Privacy Protection Act of 1993: Hearing on H.R. 3365 Before the Subcomm. on Civil & Constitutional Rights of the H. Comm. on the Judiciary, 103rd Cong. (1994); *Taylor v. Acxiom Corp.*, 612 F.3d 325, 336 (5th Cir. 2010) (summarizing legislative background on the DPPA).
[5] *Id.*
[6] 18 U.S.C. §2721(b)(1) ("For use by any government agency, including any court or law enforcement agency, in carrying out its functions…"); *see also* 18 U.S.C.§§ 2721 (b)(2)-(b)(14) (permitting use of information by a business to verify the accuracy of personal information, any insurer or insurance support organization, or any licensed private investigative agency or
licensed security service, among others).
[7] 18 U.S.C. §2721 (b)(1)-(14); *Graczyk v. West Pub. Co.*, 660 F.3d 275 (7th Cir. 2011).
[8] *See* Pub. L. No. 109–13, 119 Stat. 231, 302 (2005) (codified at 49 U.S.C. § 30301 note) (the Act).
[9] *See* § 202(d)(11).
[10] "States Offering Driver's Licenses to Immigrants," National Conference of State Legislatures, Feb. 6, 2020, https://www.ncsl.org/research/immigration/states-offering-driver-s-licenses-to-immigrants.aspx.
[11] The Systematic Alien Verification for Entitlements Program database (SAVE) is administered by US Citizenship and Immigration Services. SAVE is a system that enables states to verify a person's immigration status because states make some benefits contingent upon
immigration status. See USCIS, "Welcome to the Systematic Alien Verification for Entitlements Program," https://www.uscis.gov/save.
[12] *See* § 202(c)(3)(C).
[13] *See* § 202(c)(12) ("Provide electronic access to all other States to information contained in the motor vehicle database of the State").
[14] U.S. Gov't Accountability Office, GAO-05-204, Alien Registration: Usefulness of a Nonimmigrant Alien Annual Address Reporting Requirement Is Questionable (2005), available at https://www.gao.gov/products/gao-05-204.
[15] National Immigration Law Center, DOCUMENTS OBTAINED UNDER FREEDOM OF INFORMATION ACT: How U.S. Immigration & Customs Enforcement and State Motor Vehicle Departments Share Information, fn 20, available at https://www.nilc.org/wp-content/uploads/2016/05/batesp401.pdf.
[16] Sergio Flores & Tom Jones, "DMV Confirms ICE Has Limited Access to AB 60 License Information," NBC San Diego, Feb. 20, 2019, https://www.nbcsandiego.com/news/local/dmv-confirms-ice-has-limited-access-to-ab-60-license-information/3225/.
[17] Drew Harwell and Erin Cox, "ICE has run facial-recognition searches on millions of Maryland drivers," Washington Post, Feb. 26, 2020 (ICE has the ability to run facial recognition software across the Maryland Image Repository System database which contains the information of 7 million drivers); Drew Harwell, "FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches," Washington Post, July 7, 2019 (state officials in Utah, Washington, and Vermont run facial recognition software across its DMV data based on ICE request and provided photo)
[18] Justin Rohrlich & Dave Gershgorn, "The DEA and ICE are hiding surveillance cameras in streetlights," Quartz, Nov. 9, 2018, https://qz.com/1458475/the-dea-and-ice-are-hiding-surveillance-cameras-in-streetlights/.
[19] For more information on automatic license plate readers, please see Electronic Frontier Foundation, "Street Level Surveillance: Automated License Plate Readers (ALPRs)," Aug. 28, 2017, https://www.eff.org/pages/automated-license-plate-readers-alpr.
[20] *Supra* 13.

END NOTES

[21] For example, ICE conducted more than 100,000 queries of the Washington State driver's license database Driver and Plate Search (DAPS) within a 2-year period. See McKenzie Funk, "How to Reverse Engineer an ICE Investigation," Oct. 13, 2019; https://mckenziefunk.substack.com/p/how-to-reverse-engineer-an-ice-investigation.
[22] 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/S3500/3229_R1.PDF
[23] Washington Governor's Executive Order 17-01, Feb. 23, 2017 https://www.governor.wa.gov/sites/default/files/exe_order/eo_17-01.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/.
[24] Cal. Veh.Code § 12801.9 (West 2019), available at http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=12801.9&lawCode=VEH.
[25] A subpoena may command an individual to produce documents or testify at a particular legal proceeding but must comply with federal criminal or civil law or processes governing subpoenas to be valid and enforceable. At times, ICE has issued administrative subpoenas but they may not comply with federal criminal or civil law or processes.
[26] *See* e.g. Joseph Cox, "DMVs Are Selling Your Data to Private Investigators," MotherBoard, Sep. 6 2019, https://www.vice.com/en_us/article/43kxzq/dmvs-selling-data-private-investigators-making-millions-of-dollars; Xander Landen, "Scott tells Vermont DMV to stop giving private investigators personal data," VT Digger, Dec. 6, 2019, https://vtdigger.org/2019/12/06/scott-tells-dmv-to-stop-giving-private-investigators-personal-data/; New York State Department of Motor Vehicles, "Sharing your information," https://dmv.ny.gov/dmv-records/sharing-your-information.
[27] McKenzie Funk, "We're not just a public-safety agency. We're very much a data-sharing agency," Oct. 4, 2019, https://mckenziefunk.substack.com/.
[28] Cora Currier, "Lawyers and Scholars to LexisNexis, Thomson Reuters: Stop Helping ICE Deport People," The Intercept, Nov. 14, 2019, https://theintercept.com/2019/11/14/ice-lexisnexis-thomson-reuters-database/; Joseph Cox, "The California DMV Is Making $50M a Year Selling Drivers' Personal," Motherboard, Nov. 25, 2019, https://www.vice.com/en_us/article/evjekz/the-california-dmv-is-making-dollar50m-a-year-selling-drivers-personal-information; Commercial Requester Account Instructions/Applications, California State DMV, rev. Jun. 2018, https://www.dmv.ca.gov/portal/wcm/connect/3e1d525d-0c4c-46a2-a540-3c0714010999/inf1133.pdf?MOD=AJPERES (allowing the sale of bulk data to private companies as long as the private company certifies that data will be used for a permissible purpose under the DPPA, which includes any use by a law enforcement agency).
[29] Lois Beckett, "Everything We Know About What Data Brokers Know About You," ProPublica, June 13, 2014, https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.
[30] Currier, *supra* 26.
[31] Max Rivlin-Nadler, "How ICE Uses Social Media to Surveil and Arrest Immigrants," The Intercept, Dec. 22, 2019, https://theintercept.com/2019/12/22/ice-social-media-surveillance/.
[32] According to the Driver Privacy Protection Act (DPPA) and other federal laws referenced at 18 U.S.C. §2721(b), some federal laws do require certain driver's license data be disclosed for use in connection with motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle recalls, or advisories to carry out the purposes of titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 U.S.C. § 1231 et seq.), the Clean Air Act (42 U.S.C. § 7401 et seq.), and chapters 301, 305, and 321–331 of title 49. We believe that the DPPA should be read as the state must disclose driver's license and registration records for reasons in §2721(b), but may disclose for uses in (b)(1) – (b)(14) at its own discretion. In other words, DPPA does not require states to disclose information for uses under (b)(1)-(b)(14) or occupy the entire field. State driver's license and motor vehicle information is historically regulated by the states; and states can and have enacted laws that further restrict information use unless federal law (here 18 U.S.C. §2721(b)) explicitly requires information sharing.
[33] *See e.g.* The Illinois Biometric Information Privacy Act; Just Futures Law, Mijente, and UCI Immigrant Rights Clinic, Take Back Tech Toolkit, July 2019, at 10, https://justfutureslaw.org/wp content/uploads/2019/07/Tech-Policy-Report_v4LNX.pdf (examples of state and local laws that prohibit private and government data collection).
[34] *See* Xander Landen, "How Vermont's DMV makes millions of dollars selling personal information," VT Digger, Nov. 25, 2019, https://vtdigger.org/2019/11/25/how-vermonts-dmv-makes-millions-selling-personal-information/ (provides a list of private purchasers of a state's DMV data obtained via public records request).
[35] *See* National Immigration Law Center, DOCUMENTS OBTAINED UNDER FREEDOM OF INFORMATION ACT: How U.S. Immigration & Customs Enforcement and State Motor Vehicle Departments Share Information, fn 17, available at https://www.nilc.org/issues/drivers-licenses/ice-dmvs-share-information/#_ftnref17.

END NOTES

[36] U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Law Enforcement Information Sharing Service (LEIS Service) (2019), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-leiss-july2019_0.pdf.
[37] See NLETS website, https://www.nlets.org/.
[38] Powerpoint, Nlets Overview, Aug. 16, 2019, available at https://www.nlets.org/nlets-resources/library.
[39] Records are derived from discovery in a federal reentry prosecution and on file with writer.
[40] NISP - DL Photo Sharing, Oct. 2, 2019, https://www.nlets.org/.
[41] *See* TLETS Operation Manual, rev. 2014, at 11 (with writer); NLETS, "Members," https://www.nlets.org/our-members/members.
[42] *Supra* at 36.
[43] Texas Law Enforcement Telecommunications System Operation Manual, rev. 2014.
[44] NB: there are federal laws prohibiting states from specifically restricting the sharing of immigration status or citizenship pursuant to 8 U.S.C. §§ 1373, 1644. *See* Immigrant Legal Resource Center and Washington Defender Association, "FAQ on 8 USC § 1373 and Federal Funding Threats to 'Sanctuary Cities,' " Feb. 13, 2007.
[45] S.B. 54 § 7284.4(b), 2017 Leg., Reg. Sess. (Cal. 2017), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB54.
[46] Sara Hussain, "California DOJ Cuts Off ICE Deportation Officers from State Law Enforcement," Electronic Frontier Foundation, Dec. 18 2019, https://www.eff.org/deeplinks/2019/12/california-doj-cuts-ice-deportation-officers-state-law-enforcement-database. Prior to this decision, in early 2019, the California Department of Justice (DOJ) issued a rule labeling immigration enforcement as an unauthorized use of the CLETS database; David Maas, "California Now Classifies Immigration Enforcement as "Misuse" of Statewide Law Enforcement Network," Electronic Frontier Foundation, May 17, 2019, https://www.eff.org/deeplinks/2019/05/california-now-classifies-immigration-enforcement-misuse-statewide-law-enforcement
[47] SANDAG Pub. Safety Comm., "ARJIS Update: California Senate Bill 4," Meeting Minutes, Dec. 20, 2019, https://www.documentcloud.org/documents/6573875-SANDAG-Public-Safety-Committee-Dec-20-2019.html#document/p33.
[48] Mizue Aizeki, Personal communication, Immigrant Defense Project, Feb. 25, 2020; "eJusticeNY," Division of Criminal Justice Services, https://www.criminaljustice.ny.gov/ojis/ejusticeinfo.htm; "Reforms Include Giving Law Enforcement in the Field Access to DMV Data Using a Secure Internet Portal," Sept. 12, 2012, https://www.governor.ny.gov/news/reforms-include-giving-law-enforcement-field-access-dmv-data-using-secure-internet-portal
[49] U.S. Dep't of Homeland Security, Handout: State and Major Urban Area Fusion Centers, (2012), https://www.dhs.gov/sites/default/files/publications/Fusion%20Centers%20Handout_0.pdf.
[50] Dia Kayyali, "Why Fusion Centers Matter: FAQ," Electronic Frontier Foundation, Apr. 7, 2014, https://www.eff.org/deeplinks/2014/04/why-fusion-centers-matter-faq#9; Michael Price, "National Security and Local Police," Brennan Center for Justice, 2013, https://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf; Michael German and Jay Stanley, "What's Wrong With Fusion Centers," ACLU, Dec. 2007, https://www.aclu.org/files/pdfs/privacy/fusioncenter_20071212.pdf.
[51] Austin Police Dep't, Austin Freedom Cities Reports(2019), http://www.austintexas.gov/sites/default/files/files/Police/Resolution_74_Q3_July-Sep_2019_110619.pdf
[52] Blanca Vasquez Toness, "Newly released records point to evidence that Boston student information was shared with immigration agency," Boston Globe, Jan. 6, 2020, https://www.bostonglobe.com/metro/2020/01/06/newly-released-records-point-evidence-that-boston-student-information-was-shared-with-immigration-agency/i05fbo8PeFiF7OnyoYm4XP/story.html.
[53] U.S. Dep't of Homeland Security, "Fusion Center Locations and Contact Information," https://www.dhs.gov/fusion-center-locations-and-contact-information (list of fusion centers).
[54] Edward Hasbrouck, "How the Real ID Act is Creating a National ID Database," Papers Please, Feb. 11,2016, https://papersplease.org/wp/2016/02/11/how-the-real-id-act-is-creating-a-national-id-database/; Jim Harper, "DHS Lies, State Power Dies," Cato Institute, Feb. 5, 2016, https://www.cato.org/blog/dhs-lies-state-power-dies.
[55] AAMVA, "SPEXS Participation," https://www.aamva.org/State-to-State/.
[56] Edward Hasbrouck, "How the Real ID Act is Creating a National ID Database," Papers Please, Feb. 11,2016, https://papersplease.org/wp/2016/02/11/how-the-real-id-act-is-creating-a-national-id-database/; Jim Harper, "DHS Lies, State Power Dies," Cato Institute, Feb. 5, 2016, https://www.cato.org/blog/dhs-lies-state-power-dies.

END NOTES

[57] Hamed Aleaziz, "DHS Considered How To Punish States That Deny Access To Driver Records, A Memo Says," BuzzFeed, Feb. 10, 2020, https://www.buzzfeednews.com/article/hamedaleaziz/dhs-memo-drivers-records-sanctuary.
[58] U.S. Dep't of Transp., Nat'l Highway Traffic Safety Admin., Privacy Information Assessment: National Driver Registry, (2003), https://www.transportation.gov/individuals/privacy/pia-national-driver-register#Shares; Department of Transportation; National Driver Register, NDR, 65 Fed. Reg. 19,548 (Apr. 11, 2000) https://www.govinfo.gov/content/pkg/FR-2000-04-11/pdf/00-8505.pdf Office of the Attorney General.
[59] Dave Maass, "Misuse Rampant, Oversight Lacking at California's Law Enforcement Network," Electronic Frontier Foundation, Nov. 18, 2015, https://www.eff.org/deeplinks/2015/11/misuse-rampant-oversight-lacking-californias-law-enforcement-network.
[60] *Supra* 22.
[61] *See* Wash. State Dep't of Licensing, DOL Data Sharing, Presentation to the Joint Transportation Committee, May 17, 2018 http://leg.wa.gov/JTC/Meetings/Documents/Agendas/2018%20Agendas/May%202018%20Meeting/DOL.pdf.
[62] *Supra* 47.
[63] S.B. 1747B , Section 1 § 2(12)(A), 2019 Leg., Reg. Sess. (N.Y. 2019), https://www.nysenate.gov/legislation/bills/2019/S1747 ("No Later than three days after such request, notify the individual about whom such information was requested, informing such individual of the request and the request and the identity of the agency that made such request").
[64] Off. of the Leg. Auditor, Law Enforcement's Use of State Databases: Key Facts and Findings, Minn. Leg., Feb. 2013, https://www.auditor.leg.state.mn.us/ped/2013/ledatabasesum.htm.
[65] *See e.g.* Austin Police Dep't, Council Resolution Reporting Requirements 20180614-73 & 74, https://www.austintexas.gov/page/council-resolution-reporting-requirements-20180614-73-74; see Austin City Council, Resolutions 20180614-073 and 20180614-074 (Freedom Cities), https://www.austintexas.gov/department/city-council/2018/20180614-reg.htm.
[66] This limited document retention policy may only apply to non-REAL ID compliant cards as REAL ID Act requires source documents to be retained for 7 or 10 years. § 202(d)(2).
[67] *Supra* 22.
[68] *See* Austin City Council, Resolutions 20180614-073 (Item 73) and 20180614-074 (Item 74), June 14, 2018, https://www.austintexas.gov/department/city-council/2018/20180614-reg.htm.
[69] *Supra* 61.
[70] *Supra* 57.
[71] N.Y. Att'y Gen., "Attorney General James Files Lawsuit Against Trump Administration Over Assault On New York Travelers," Feb. 10, 2020, https://ag.ny.gov/press-release/2020/attorney-general-james-files-lawsuit-against-trump-administration-over-assault.
[72] *Supra* 41.
[73] *Supra* 61.
[74] *Supra* 47.