State Level Considerations for Data Sharing of Undocumented Immigrants: Access to DMV Record Information

The recent controversy around the possible addition of a citizenship question to the 2020 Census has created many questions regarding the privacy of immigrant's personal data and the various risks and benefits of providing such information for government records. While there are not many risks at the federal level associated with sharing data and participating in the Census, it is important to be aware of possible state-related issues.

One such possible state issue involves the application of undocumented immigrants for driver's licenses and learner's permits. While many states require proof of citizenship to apply for a driver's license, several have now recognized the significant benefit[1] of creating a separate type of driver's license specifically for those who might not be able to provide documentation to prove that they are a United States citizen or those who are undocumented.

In certain instances, there could be a risk that the information given by undocumented immigrants in pursuit of a driver's license may be shared with the Department of Homeland Security (DHS). It is possible that DHS could use this information provided in the course of an enforcement action.

Please read below to learn more about this issue and whether your state may be affected.

1. Does your state allow undocumented immigrants to apply for drivers' licenses?

The following states allow undocumented immigrants to apply and may have information sharing vulnerabilities:

1. California
2. Colorado
3. Connecticut
4. Delaware
5. Hawaii
6. Illinois
7. Maryland
8. New Mexico
9. Nevada
10. New Jersey
11. New York
12. Oregon
13. Utah
14. Vermont
15. Washington
16. District of Columbia
17. Puerto Rico

2. Does your state have specific legislative protections against the sharing of personal information of immigrants who applied for a drivers license?

While some states[2] have enacted specific legislative protections against the sharing of personal information of immigrants who apply for a license, most do not have any such protections. The lack of specific legislative protections leaves individuals' information vulnerable to being potentially acquired in some manner by the Department of Homeland Security, who may have the opportunity to use that information in immigration enforcement actions. This remains a significant concern, since in many cases this sort of action is directly opposed to the legislative intent of allowing undocumented immigrants to apply for driver's license.

If there are no specific legislative or administrative protections, it should be assumed that there is at least some risk that DHS will gain access to DMV records either through voluntary info-sharing, biometric technology, or another non-judicial administrative method

3. How could DHS gain access to this information?

DHS uses a large range of techniques in order to gain identification Department of Motor Vehicle information. A large portion of information sharing occurs through simple data exchange between departments. Many states have no legislative or policy restraints against DMV employees providing personal information upon request to DHS officials. This leads to info-sharing, available at the simple request of ICE.

a. Statutorily Mandated Info-Sharing Protocols:Some states even have statutorily mandated info-sharing protocols. For instance, Utah, which requires undocumented immigrants to provide fingerprint information when applying for a license, requires that the Bureau of Criminal Identification shall provide notice to ICE of any new or existing criminal history record or new or existing warrant information contained in the state database, which matches with fingerprint information found in the DMV records.

b. Free Access to DMV Databases: Utah, Washington and Vermont have been currently give free access to DMV databases. (There is special concern in Washington, where free access to information is being given despite Governor Inslee's executive order[3] prohibiting state agencies from helping to enforce federal immigration laws.)

c. Facial Recognition Technology: At least three states that offer driver's licenses to undocumented immigrants, ICE officials have utilized facial recognition technology[4] to comb through DMV records in order to gain immigrants' information. They use this information primarily to find any potential duplicates of applications, which may lead to evidence of a person's lack of status. However, there are significant concerns with this technique. Not only is it a serious invasion of privacy, but government studies of facial recognition technology[5] confirmed that age, gender, and racial bias was present in some facial recognition algorithms. The current system used by CBP has not been tested by the National Institute for Standards and Technology (NIST) for these biases.[6] This means that the technology DHS is utilizing has the potential to mark dozens or even hundreds of false positives with virtually no oversight.

4. What can be done to protect the information of those who applied for drivers' licenses?

The most effective way to satisfy these concerns are to include statutory protections against information sharing with or data mining by the Department of Homeland Security. This solution is already beginning to be embraced by states: New York, for example, recently implemented strict privacy laws surrounding the DMV information of immigrants.

5. In advocating for legislation to ensure the privacy of immigrants' personal information   contained in DMV records, here are some important questions to consider:

(a.) Does the legislation preclude all information given in an application for a non-commercial driver's license or learner's permit, or the renewal of either, from being considered a public record?

(b.) Does the legislation apply to any portion of any record retained by the commissioner in relation to a non-commercial driver's license or learner's permit application or renewal application, or is the legislation more specific?

(c.) In order for information to be accessed, does the legislation require a lawful court order, subpoena, or judicial warrant signed by an Article III judge? Or only an administrative subpoena? (This may be especially important, as DHS officials often use administrative subpoenas in order to gain personal information. Administrative subpoenas are not judicially approved and need only be signed by any immigration official. Accordingly, there is virtually no oversight of the use of such information.)

(d.) Does the legislation include a restriction against the sharing of information that identifies whether the type of driver's license or learner's permit that a person holds either meets federal standards for identification or does not meet federal standards for identification?

(e.) Does the legislation require that the DMV and its employees shall not disclose or make accessible in any manner records or information that he or she maintains, to any agency that primarily enforces

immigration law or to any employee or agent of such agency, unless the commissioner is presented with a lawful court order or judicial warrant signed by a judge appointed pursuant to article III of the United States constitution?

(f.) Does the legislation require that, if such a judicial warrant or court order is obtained, that the person whose records are acquired by immigration officials be notified of the request and the identity of the agency that made such request? This will help an immigrant to prepare in case of an adverse enforcement action.

(g.) Does the legislation require that any person or entity that receives or has access to records or information from the department to certify to the commissioner, before such receipt or access, that such person or entity shall not (i) use such records or information for civil immigration purposes or (ii) disclose such records or information to any agency that primarily enforces immigration law or to any employee or agent of any such agency?

If the answer to any of these questions is "no", these are the areas where legislative protections should be considered in order to provide for a more thorough protection of applicants' privacy.

Endnotes

1 For information about these benefits, please consult CLINIC's backgrounder, available at https://cliniclegal.org/resources/state-and-local/drivers-license-backgrounder
2 The states which have at least some basic form of information protections are California, Hawaii, New York, and New Jersey. As of February 28, 2020, Maryland has also introduced legislation considering information protection. However, some of these protections are stronger than others, and the appropriate legislation should be consulted for more specific information. However, some of these protections are stronger than others, and the appropriate statutes should be consulted for more specific information.
3 https://www.seattletimes.com/seattle-news/politics/inslee-signs-order-limiting-states-involvement-in-immigration-enforcement/
4 https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html
5 https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf
6 https://homeland.house.gov/imo/media/doc/020620%20BGT%20Statement.pdf

JUSTICE FOR IMMIGRANTS

we are one family under God