COLORADO LAW
UNIVERSITY OF COLORADO **BOULDER**

Colorado DMV Records & ICE: Preventing Unauthorized Disclosures

Mar. 16, 2020

Samuelson-Glushko Technology Law & Policy Clinic and Immigration Defense Clinic at Colorado Law

Conor May, Hillary Bernhardt, Bethany Reece, and Sam Thornton
Student Attorneys

Blake E. Reid and Violeta Chapin
Clinic Directors

tlpc@colorado.edu

Executive Summary

Reports have recently come to light that state motor vehicle authorities in several states, including Colorado, have assisted federal immigration authorities and specifically Immigration & Customs Enforcement (ICE), in the identification and removal of undocumented immigrants from the U.S.[1] These reports are especially concerning because they come from states that have passed legislation to allow and encourage undocumented immigrants to obtain driver licenses in order to improve road and community safety.[2] Sharing these vast photo databases is also concerning given the expanding use of facial recognition software by state and federal agencies, including immigration authorities.[3] ICE reports that it uses state data that "may assist in case completion and subsequent prosecution," but observers have expressed concern that using facial recognition to scan Division of Motor Vehicles (DMV) databases gives agents access to the faces of drivers who have not been charged with a crime or implicated in an investigation.[4]

As a state that both encourages undocumented residents to obtain driver licenses and allows for potential information sharing with immigration officials, Colorado is at the center of this issue. DMV data sharing is a serious concern for clients of the University of Colorado's legal clinics, which offer pro bono services in immigration proceedings. Accordingly, the Samuelson-Glushko Technology Law & Policy Clinic prepared this Report with assistance from the CU Law's Immigration Defense Clinic in order to examine the best practices for protecting undocumented immigrants' records in the present political climate. This Report compares these best practices with the current policies and practices of the Colorado DMV and recommends changes that could make these records more secure. Specifically, this Report looks at:

- Individual requests for information from immigration officials;
- Sharing of information using digital law enforcement databases;
- Use of facial recognition by Colorado governmental entities; and
- Policies for transparency and accountability.

We recommend that Colorado:

- Require warrants or court orders before turning over driver information to ICE;
- Limit immigration officials' access to records in digital databases;
- Limit Colorado's own use of facial recognition technology; and
- Implement audits of the relevant systems to provide transparency.

This Report also considers relevant statutes and finds nothing in state or federal law preventing the DMV from implementing these safeguards. By doing so, Colorado can support immigrant communities, improve road and highway safety, and respect the privacy of residents.

---

[1] See Natalie Delgadillo, "It's Not Just Washington. At Least Three Other States Share Drivers' Immigration Info With ICE," Governing (Jan. 18, 2018), https://www.governing.com/topics/public-justice-safety/gov-immigrant-drivers-licenses-ICE-washington.html; National Immigration Law Center, "How ICE and DMVs Share Information" (May 2016), https://www.nilc.org/ issues/drivers-licenses/ice-dmvs-share-information/.

[2] Delgadillo, *supra* note 1.

[3] *See*, *e.g.*, National Immigration Law Center, *supra* note 1; Catie Edmondson, "ICE Used Facial Recognition Software to Mine State Driver's License Databases," New York Times (July 7, 2019).

[4] Edmondson, *supra* note 3.

Table of Contents

Discussion

This Report examines two interrelated concerns raised by immigration and privacy experts in recent years. First, experts have found evidence that DMVs in many states, including those that offer driver licenses to undocumented residents, share driver license records with federal immigration enforcers to assist them in finding and deporting undocumented residents.[5] Second, facial recognition technology use by state and federal authorities that has quietly expanded over the last decade, with little or no legislative oversight.[6] Due to these two concerning trends, information voluntarily provided to the DMV by undocumented residents in order to obtain a driver's license now potentially exposes those residents to the risk of that information being used by ICE to deport them.

This Report offers several policy recommendations for the state of Colorado to better protect against this kind of information sharing. These recommendations reflect policies implemented in other states and a guide to best practices published by the National Immigration Law Center.[7] Finally, this Report outlines how these recommendations can be implemented in accordance with state and federal law.

I. Background

Over the past several years, reports have called into question how state motor vehicle authorities are using the data citizens entrust to them. Affected data include photographs of every licensed driver in the state, collected in the course of issuing driver licenses. Additionally, DMV records often include applications for licenses and registrations that contain information including where an applicant was born and what documents they used to apply.[8] Privacy advocates are particularly concerned by revelations of data sharing between departments and divisions of motor vehicles (DMVs) and federal Immigration & Customs Enforcement (ICE), in conjunction with increasing use of facial recognition technology by law enforcement.

Research and reporting have uncovered numerous instances of data sharing between state DMVs and ICE.[9] In some states, ICE employees submitted specific requests to DMVs for information.[10] In others, investigators discovered that ICE employees had direct access to DMV records through digital law enforcement databases, obviating the need to submit an

---

[5] *E.g.*, Delgadillo, *supra* note 1; National Immigration Law Center, *supra* note 1, Edmondson, *supra* note 3.

[6] *E.g.,* Claire Garvie, Alvaro Bedoya, and Jonathan Frankle, The Perpetual Line-up: Unregulated Police Face Recognition in America, Georgetown Center for Privacy & Technology (October 18, 2016); National Immigration Law Center, *supra* note 1, Beryl Lipton, "Hundreds of agencies, including the FBI have access to Ohio AG's facial recognition platform," Muckrock (May 15, 2019), https://www.muckrock.com/news/archives/2019/may/15/ohio-facial-recognition-privacy/

[7] National Immigration Law Center, *supra* note 1.

[8] Nina Shapiro, "Washington state regularly gives drivers' info to immigration authorities; Inslee orders temporary halt," Seattle Times (Jan. 12, 2018 4:16pm), https://www.seattletimes.com/seattle-news/times-watchdog/washington-state-regularly-gives-drivers-info-to-immigration-authorities-inslee-orders-temporary-halt/.

[9] *See* Delgadillo, *supra* note 1; National Immigration Law Center, *supra* note 1.

[10] *See* Delgadillo, *supra* note 1.

individualized request.[11] The National Immigration Law Center concludes that, in short, "ICE gains access to DMV information through sophisticated technological means as well as informal communications."[12]

For example, the Ohio Law Enforcement Gateway, a database compiled by the state's attorney general, which included DMV photos and records, was accessible to thousands of individuals, including FBI and ICE employees.[13] In addition to digital databases, ICE's field Enforcement & Removal Offices often have "informal relationships" with local DMVs that facilitate "ad hoc and decentralized" information sharing.[14] This practice has occurred in states that have in other respects been fairly supportive of immigrant communities and protective of their undocumented residents, often without approval from state leaders.[15]

Turning over DMV records to ICE is particularly concerning in states, like Colorado, that allow and encourage undocumented immigrants to get driver licenses.[16] Laws granting licenses to undocumented drivers ask these residents to "come out of the shadows" and obtain licenses in order to increase driver safety. These laws are premised on those residents' reasonable expectations that doing so will not increase their chances of deportation.[17] However, DMV records often contain information that could lead to a license-holder being targeted by ICE.[18] DMV employees in Washington, for example, redacted the Social Security number field on driver license documents before sharing them, but ICE was still able to use license applications to determine an applicant's place of birth and whether the applicant had used a foreign passport or other foreign document to apply for a license.[19]

Colorado Governor Jared Polis has expressed strong support for immigrant communities throughout his career, including during his current tenure as head of Colorado's executive branch.[20] The Colorado legislature recently affirmed the Colorado Roads and Community Safety Act, which grants driver licenses to undocumented residents of Colorado and appropriates funds to expand the number of facilities issuing licenses.[21] Providing this access to undocumented Coloradans without instituting safeguards to ensure that the information obtained is not used for deportation risks betraying the trust of the immigrant community, and would undermine the policy objective of improving road safety.

---

[11] *See* National Immigration Law Center, *supra* note 1; *see also* Lipton, *supra* note 6.

[12] *Untangling the Immigration Enforcement Web*, National Immigration Law Center (Sep. 2017) 16.

[13] *See* Lipton, *supra* note 6.

[14] *Untangling the Immigration Enforcement Web, supra* note 12, at 17.

[15] *See* Delgadillo, *supra* note 1.

[16] C.R.S. 42-2-501 et seq.

[17] *See, e.g.,* Rebekah Entralgo, "Colorado Governor signs bill expanding drivers' license access to undocumented immigrants," Think Progress (May 28, 2019 4:08pm), https://thinkprogress.org/colorado-governor-undocumented-immigrants-drivers-licenses-9cc426fe3e42/.

[18] Shapiro, *supra* note 8.

[19] *Id.*

[20] Chase Woodruff, "Activists Wonder Where the 'Bold, Progressive' Jared Polis Went," Westword (May 15, 2019), https://www.westword.com/news/activists-wonder-where-the-bold-progressive-jared-polis-went-11343776.

[21] Colorado SB 19-139 (2019); *see also* Entralgo, supra note 17.

Immigration advocates' fears about ICE access to DMV records are compounded by the increasing widespread use of facial recognition technology by law enforcement.[22] However, the use of facial recognition technology to scan DMV databases also creates a more generalized privacy concern. In 2016, research by Georgetown's Center for Privacy and Technology highlighted that unrestricted use of facial recognition threatens "Fourth and First Amendment principles, social norms, and police practices" by allowing citizens who have never been implicated in an investigation to be subjected to a virtual line-up without their consent.[23] In the words of Rep. Jim Jordan, the ranking Republican on the House Oversight Committee, "No individual signed off on that when they renewed their driver's license, got their driver's licenses. They didn't sign any waiver saying, 'Oh, it's okay to turn my information, my photo, over to the FBI.' No elected officials voted for that to happen."[24] Nonetheless, Georgetown found that "law enforcement face recognition affects over 117 million American adults," due in large part to mining of DMV records.[25]

The sharp increase in facial recognition software by law enforcement presents privacy concerns for all Americans, regardless of their immigration status. However, it is particularly disturbing in states that have professed support for immigrant communities and asked undocumented residents to make use of the DMV system. This technology often suffers from lack of accuracy, especially when identifying people of color.[26] These factors combine to create a situation in which an undocumented driver could voluntarily come forward at the urging of the state and apply for a license, and, as a result, could be exposed to misidentification as a result of an ongoing investigation, as well as caught in a "dragnet"[27] that allows ICE agents to examine their license application documents without prior cause.

II. Recommendations

This Report offers a number of changes to state policy that would help safeguard against misuse of DMV information and affirm Colorado's support for immigrant communities. These recommendations fall into four broad categories. First, the Division should amend DMV policies regarding record-sharing to maintain the current level of access by local police and state and federal agencies like the Colorado Bureau of Investigations and FBI, while making it harder for ICE to mine DMV data.

Second, Colorado should carefully review its participation in federal and international law enforcement databases. These databases provide valuable resources for preventing and solving crimes, but their use also offers a possible back door to immigration enforcers.

---

[22] *See generally*, Garvie et al, *supra* note 6; *see also* Claire Garvie and Laura Moy, *America Under Watch: Face Surveillance in the United States*, Georgetown Center for Privacy & Technology (May 16, 2019).

[23] *See* Garvie, et al, *supra* note 6.

[24] Drew Harwell, "FBI, ICE find state driver's license photos are a goldmine for facial recognition searches," The Washington Post (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

[25] *See* Garvie, et al, *supra* note 6.

[26] *Id.*

[27] *Id.*

Third, Colorado should review its facial recognition policies in order to make sure they are in keeping with Coloradans' privacy norms and that the policies have the support of elected officials. The public and their representatives should be aware of technology's ability to identify and surveil, and have some say in its use.

Fourth, Colorado should provide oversight and transparency by implementing audits of all of its data sharing policies and law enforcement tools, to make sure they are being used appropriately. This will help safeguard against abuse and policy violations, as well as supporting road safety by reassuring undocumented drivers regarding the security of their data should they participate in the license program.

A. Protecting Records

The first set of recommendations in this Report deal with how states can insulate DMV records from information requests by ICE. The gold standard for protecting DMV records, implemented in Washington State after reports of record sharing came to light, require ICE officials to present a warrant before transferring records.[28]

Colorado state law already prevents DMV personnel from informally sharing information with federal agencies outside of official channels.[29] Colorado law requires that any government agency seeking to obtain records must provide a requester release form.[30] This requirement includes local, state, and federal law enforcement conducting a criminal investigation, as well as immigration officials.[31] DMV policy further stipulates that the DMV only provides federal law enforcement with information pertaining to a specific investigation.[32]

In theory, then, whether an enforcer belongs to ICE, a local police force, the Colorado Bureau of Investigations, or any other agency, that official is unable to simply pick up the phone and ask the DMV to send over records. The official will be required to fill out the requester release form and submit it to the DMV, at which point the DMV office in charge of law enforcement communications will reply with the requested information.[33]

However, this request form merely requires a guarantee that the recipient will not sell or transfer the information to another person for purposes prohibited by federal law.[34] It does not require them to provide a warrant or authorization from a court or the Colorado government. A public statement from a DMV spokesperson indicates that as of January 2018, no requests had been made to the DMV regarding immigration cases.[35] However, to safeguard against the potential for future requests, Colorado should consider creating specific exceptions to state policy that protect against disclosure of DVM information to ICE. This policy should require

---

[28] *See* Delgadillo, *supra* note 1; National Immigration Law Center, *supra* note 1.

[29] C.R.S. 24-72-204(7)(b).

[30] *Id.*

[31] *Id.*

[32] *See* Delgadillo, *supra* note 1.

[33] Appendix A at 1.

[34] C.R.S. 42-1-206(1)(b).

[35] *Id.*

ICE employees to obtain a warrant or court order before the Colorado DMV will comply with record requests.[36]

Law enforcement agencies can also request image comparisons from the Colorado DMV. However, pursuant to DMV policy, image comparison requests require that the individual subject of the image comparison must relate to a case involving specific classes of felony offenses. These "Level 1" offenses include violent crimes, threats to national security, kidnapping, etc.[37] If such a request is presented, the DMV will provide a dossier on the individual, which includes their name, date of birth, height, weight, and photo.

Accordingly, ICE and other law enforcement agencies could contact the DMV and ask that the DMV run an image comparison on their behalf. However, in theory the DMV will only comply if the request pertains to a serious felony investigation.

While the Level 1 investigation requirement provides some protection against ICE exploitation of DMV's image comparison system, it does not protect against the kind of "informal" communication between ICE and the DMV documented by the National Immigration Law Center.[38] It also does not prevent protect against facial recognition errors, which could lead to an undocumented resident who has no connection to a felony investigation coming under scrutiny from ICE. Recommendations on how to prevent these scenarios are discussed below ("Internal Facial Recognition" and "Oversight & Transparency").

B. Law Enforcement Databases

Safeguarding against informal requests to the DMV does not close the potential back door offered by information-sharing databases. In order to ensure that ICE agents are not using law enforcement databases to obtain records, as occurred in Ohio, the National Immigration Law Center also recommends "ensuring that ICE access to driver and vehicle registration information through national or state criminal justice networks is regulated to the extent possible."[39]

Colorado participates in digital law enforcement information sharing databases, at least one of which (NLETS, the International Justice and Public Safety Network) is used by ICE to obtain records.[40] NLETS allows users to send queries for driver license information to participating state and federal agencies, which may include the driver's name, address, social security number, license type, and, for certain states, photo.[41] The NLETS website currently lists Colorado as a state allowing photo sharing through the National Image Sharing Program

---

[36] National Immigration Law Center, *supra* note 1.

[37] Appendix A at 1.

[38] *Untangling the Immigration Enforcement Web*, *supra* note 12.

[39] *Id.*

[40] See Colorado Crime Information Center, Colorado Bureau of Investigation Department of Public Safety (last visited November 13, 2019), https://www.colorado.gov/pacific/cbi/colorado-crime-information-center-ccic; National Immigration Law Center, supra note 1.

[41] *See* NLETS, *Users Policy Manual v. 4* 56-61 (Dec. 2013), https://www.dropbox.com/s/anb7ah55hpptasv/3%20%20NLETS%20User%20Policy%20Manual_Redacted.pdf.

(NISP) which offers member agencies "immediate, positive identification" using DMV photos.[42] Dossiers compiled by the DMV in response to individual requests are also made available via NLETS.[43]

This suggests that NLETS offers a back door for participating agencies to avoid the official request channels described in the prior section. Colorado law provides little comfort if participants in NLETS can simply query the database for photos and other DMV information, rather than submitting a requester release form.[44] This database could give ICE agents access to DMV data in larger quantities and with even fewer barriers than the current DMV request system described in the last section.[45] Giving agents at ICE's local Enforcement & Removal Office the kind of "immediate, positive identification" advertised by NLETS would seem to entirely circumvent statutory and policy protections covering DMV records.[46]

Colorado should protect against this sort of unintentional sharing via NLETS and similar databases by restricting permissions for the information uploaded to the database to exclude ICE. If the relevant permissions cannot be restricted, Colorado should ensure that DMV records of undocumented residents are not included in such databases.

Given that the state encourages undocumented residents to obtain driver licenses, its participation in the NISP program is particularly problematic. To the extent that this affects authorized sharing with other agencies like the FBI and out-of-state police, Colorado should develop alternate mechanisms for sharing that information so that only authorized users have access. This will ensure that Colorado's participation in law enforcement databases serves traditional public safety purposes by giving law enforcement officers the information they need to investigate and prevent crime, while closing a back door that ICE may use to target undocumented license-holders.

C. Use of Facial Recognition by the DMV

Finally, best practices for states include limiting the use of facial recognition technology to ensure it is not used to assist ICE, and curtailing internal use by the DMV and law enforcement without explicit approval by the legislature.[47] Given that current DMV policy only permits image comparisons in connection with Level 1 offenses, *internal* facial recognition use by the DMV (facial recognition searches conducted by DMV employees upon request, using DMV

---

[42] Appendix B; *see also* NLETS, *NISP – DL Photo Sharing* (last visited Nov. 11, 2019, 8:41pm), https://www.nlets.org/our-members/grantmaps?mapid=d26b4e70-934e-11e3-9a61-00155d003202.

[43] *See* Appendix A at 1.

[44] *See* NLETS, *supra* note 41.

[45] *See* David Minsky, "An objective to share California driver's license photos with a nationwide database is raising concerns over privacy & oversight," 16 Santa Maria Sun 3 (Mar. 25, 2015), http://www.santamariasun.com/news/12971/an-objective-to-share-california-drivers-license-photos-with-a-nationwide-database-is-raising-concerns-over-privacy-and-oversight-/ (EFF's Dave Maass describing how California joining NLETS's photo-sharing program will result in "wholesale access to DMV photos and data without a whole lot of auditing built in.").

[46] Appendix B.

[47] *See* Garvie, *supra* note 6; *see also* National Immigration Law Center, *supra* note 1.

software) should in theory be protected from exploitation by ICE.[48] However, facial recognition technology still poses broader privacy concerns for the general population, undocumented or otherwise. At minimum, the state should subject internal facial recognition use to the same audit process recommended for other information sharing, in order to ensure it is not being used to assist ICE. More broadly, Colorado should limit its own use of facial recognition until Colorado's elected representatives can grapple with the technology's privacy implications.

Georgetown's Center for Privacy and Technology concluded their 2016 study with a number of recommendations for governments.[49] These recommendations included limiting law enforcement use of facial recognition to reasonable, individualized suspicion of criminal conduct.[50] Their recommendation to limit driver license photo searches to investigations involving serious offenses resembles Colorado's current policy.[51] However, they also recommend ending all such use of DMV photos until receiving legislative approval, and obtaining court orders for individual searches.[52]

Different states and local governments have proposed a variety of measures similar to those recommended by the Center for Privacy and Technology.

- States like Washington and Massachusetts, and cities like San Francisco and Somerville, have considered or adopted full moratoria on government use of facial recognition.[53]
- The Massachusetts bill would require "express statutory authorization," including specifics about which entities are authorized to use the technology and how it will be monitored and audited, before facial recognition could be employed.[54]
- A Washington bill laid out a series of prerequisites to the moratorium being lifted, including independent third-party bias testing and a report on civil liberties issues from a taskforce including members of impacted communities.[55]
- Different legislation introduced in Washington would require legislative bodies to engage in a notice-and-comment proceeding before authorizing the purchase of facial recognition technology.[56]

These proposals reflect the kind of careful consideration that should accompany use of facial recognition by government actors.

---

[48] *See* Appendix A at 1.

[49] Garvie, *supra* note 6.

[50] *Id.*

[51] *Id*; Appendix A at 1.

[52] Garvie, *supra* note 6.

[53] S 1385 (Ma. 2019); Washington SB5528 (2019); Victoria Hudgins, "Why 4 Local Banned Facial Recognition Tech," *LawTechNews* (Nov. 25, 2019), https://www.law.com/legaltechnews/2019/11/25/why-4-local-governments-banned-facial-recognition-tech/?slreturn=20200028232554.

[54] S 1385 (Ma. 2019), https://malegislature.gov/Bills/191/S1385.

[55] SB 5528 (Wa. 2019), https://app.leg.wa.gov/billsummary?BillNumber=5528&Year=2019&Initiative =false.

[56] HB 2761 (Wa. 2020), https://app.leg.wa.gov/billsummary?BillNumber=2761&Initiative=false&Year =2019.

Short of outright moratoria or bans, other proposals would require courts to approve the use of facial recognition.[57]

- New York is considering a measure first introduced in 2019 that would require state and local agencies and contractors to obtain court authorization before collecting and maintaining records (including driver license photos) for facial recognition purposes.[58]

Other limitations being considered around the country include:

- Prohibiting facial recognition from being used as the sole basis for establishing probable cause in a criminal investigation,[59]
- Prohibiting the use of facial recognition in schools.[60]

States have a wide menu of options at their disposal when considering how and when facial recognition should be used. The most important safeguard is that the public and their representatives actively participate in making these decisions, rather than allowing this technology to expand unchecked behind the scenes.

D. Oversight & Transparency

By requiring warrants for individual requests for image comparisons from ICE, taking steps to protect access via information databases, and checking use of facial recognition technology, Colorado can ensure that it is not increasing the exposure of undocumented residents who participate in the state's driver license program. However, these records protections are only meaningful to the extent that they are enforced. Appropriate oversight and transparency protects against the kind of informal, off-the-books sharing between DMVs and local ICE offices that has been documented in other states.[61] To this end, best practices recommend states "audit and make public any information regarding DMV disclosure of driver or vehicle information." [62]

Current DMV policy states that all DMV record-sharing systems are monitored and may be audited at any time in order to ensure that records are not disclosed in violation of state law.[63] However, this policy does not require audits, or the disclosure of results to the public.

Colorado should require minimum periodic audits of these systems to ensure enforcement of current policies and the recommendations provided in this Report. Colorado should also make these policies and the results of audits public.[64] Publicity would provide an additional

---

[57] SB 5376 (Wa. 2019) (as introduced) § 7, https://app.leg.wa.gov/billsummary?BillNumber=5376&Initiative=false&Year=2019.

[58] A 01692 (N.Y. 2020), https://assembly.state.ny.us/leg/?default_fld=&bn=A01692&term=2019&Summary=Y&Actions=Y&Text=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y.

[59] HB 1654 (Wa. 2019), https://apps.leg.wa.gov/billsummary/?BillNumber=1654&Year=2019&Initiative=false.

[60] A 06787 (N.Y. 2019), https://assembly.state.ny.us/leg/?default_fld=&bn=A06787&term=2019&Summary=Y&Actions=Y&Text=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y.

[61] *Untangling the Immigration Enforcement Web*, *supra* note 12; Delgadillo, *supra* note 1.

[62] National Immigration Law Center, *supra* note 1.

[63] *See* Appendix A at 3.

[64] *See* National Immigration Law Center, *supra* note 1.

layer of accountability and oversight, as well as reassuring immigrant communities in Colorado about their safety, the security of the information voluntarily shared with the state, and would encourage confidence and trust in the undocumented driver license system.

This oversight should also include local law enforcement's access to DMV information. Colorado has already seen examples of local law enforcement voluntarily cooperating with ICE, either by holding inmates after their release date on ICE detainers,[65] or by signing agreements with ICE allowing local officers to be deputized as immigration enforcers.[66] Protecting DMV records from direct access by ICE will be ineffective if county or municipal law enforcement use their own access to help federal agencies circumvent state policy.

Similarly, a Department of Homeland Security (DHS) memo obtained by the press in February 2020 revealed that DHS personnel had considered numerous means of evading state protections on DMV records.[67] These proposals included using "friendly" states to collect otherwise inaccessible information.[68] While local law enforcement and officers in other states should not be preventing from relying on DMV records to pursue legitimate public safety purposes, the state should also exercise due care through monitoring to ensure that they are not providing ICE with a backdoor to DMV records.

III. Compliance with Existing Law

The previous sections outline the policies that Colorado *should* implement. This Report now examines the legal requirements that govern information sharing to demonstrate that Colorado *can* implement these policies without violating state or federal statutes.

A. Protecting Records

Current DMV policy states that the Division is required by state law to share information with criminal justice agencies.[69] However, while the Colorado Open Records Act and the DMV's authorizing statute *permit* sharing of DMV records with government agencies, neither law *requires* it. Colorado statutes provide the Department of Revenue with discretion in sharing of records.[70]

The Colorado Open Records Act generally prohibits the Department of Revenue from disclosing DMV records.[71] Similarly, the Colorado DMV authorizing statute generally prevents

---

[65] Kelsey Rey, "CO Supreme Court denies El Paso sheriff's appeal in ICE detainer case," Colorado Independent (April 12, 2019).

[66] Conor McCormick-Cavanagh, "ACLU Suing Teller County Sheriff Again Over Cooperation With ICE," Westword (June 27, 2019 10:47am), https://www.westword.com/news/aclu-of-colorado-suing-teller-county-sheriff-over-ice-cooperation-11390963.

[67] Hamed Aleaziz, "DHS Considered How To Punish States That Deny Access To Driver Records, A Memo Says," Buzzfeed (Feb. 10, 2020 9:01pm), https://www.buzzfeednews.com/article/hamedaleaziz/dhs-memo-drivers-records-sanctuary.

[68] *Id.*

[69] *See* Appendix A at 3.

[70] C.R.S. 24-72-207(b), 42-1-206(3.5)(b).

[71] C.R.S. 24-72-207(7)(a).

selling or releasing specific information filed with the Department of Revenue, including photographs and digitized images.[72] Both laws contain exceptions for sharing with other government actors (any government agency in the case of CORA, and criminal justice agencies in the case of Title 42).[73] However, both of these exceptions are allowances, not requirements. CORA states that the Department of Revenue "*may* allow inspection."[74]

Meanwhile, the DMV authorizing statute merely states that "nothing in this subsection [prohibiting sharing of DMV information] shall prevent" the Department from sharing information with criminal justice agencies.[75] This language merely applies to that specific prohibition. More importantly, by stating that the statute "shall not prevent" the sharing of DMV records, the state legislature's mandate allows sharing, but does not compel it.

Federal law does not require the DMV to share driver license information with immigration authorities. One federal statute and two constitutional doctrines could be construed to implicate the recommendations contained in this report: the federal law authorizing the Immigration & Naturalization Service (INS), and the doctrines of intergovernmental immunity and obstruction preemption.[76] These three potential challenges have been recently litigated in federal court.[77] A case brought by the federal government challenged several California laws, one of which prohibited local law enforcement from "'[p]roviding information regarding a person's release date or' other 'personal information,' such as 'the individual's home address or work address.'"[78] The resulting verdict did much to define the limits of state's duties to federal immigration officials.[79]

The INS authorizing statute states that, other laws notwithstanding, state and locals officials "may not prohibit, or in any way restrict, any government entity or official from sending to . . . [the INS] . . . information regarding the citizenship or immigration status, lawful or unlawful, of any individual."[80] However, the 9th Circuit ruled in 2019 that this requirement is limited to "information strictly pertaining to immigration status (i.e. one's immigration status) and does not include information like release dates and addresses."[81] Under this reading, information contained on Colorado driver licenses would not be included.

---

[72] C.R.S. 42-1-206(3.5).

[73] C.R.S. 24-72-207(7)(b); C.R.S. 24-72-207(3.5)(b); *see also* 24-72-302(3) (defining "criminal justice agency").

[74] C.R.S. 24-72-207(b) [emphasis added].

[75] C.R.S. 42-1-206(3.5)(b).

[76] United States v. California, 921 F3d 865, 873-74, 876-77 (9th Cir. 2019) (hereinafter *California*).

[77] *See generally id.*

[78] *Id.* at 876.

[79] *See generally id.*

[80] 8 U.S.C. 1373 (1996).

[81] California, *supra* note 72, at 891 (quoting United States v. California, 314 F. Supp. 3d 1077 (E.D. Cal. 2018)). The District Court questioned the constitutionality of 8 USC 1373 under the 10th Amendment, but found it unnecessary to address directly, given its inapplicability to the information in question. United States v. California, 314 F. Supp. 3d 1101 (E.D. Cal. 2018).

This litigation also saw the U.S. government invoke intergovernmental immunity. This doctrine, which arises under the Supremacy Clause of the Constitution,[82] prohibits states from directly regulating the activities of the federal government or discriminating against federal entities.[83] Finally, the United States argued that the California law was preempted by federal law under the doctrine of conflict preemption, because it "unlawfully obstruct[ed] the enforcement of federal immigration laws.[84] Under this doctrine, state laws are preempted when they "stand as an obstacle to the full purposes or objectives of Congress."[85]

However, the 9th Circuit found that neither intergovernmental immunity nor preemption compelled California to share information with immigration enforcers.[86] Rather, the court found that California's law was protected by the 10th Amendment's anti-commandeering doctrine.[87] This doctrine in many ways mirrors preemption by preventing the federal government from commandeering state legislatures or employees for federal purposes.[88]

The 9th Circuit held that anti-commandeering applied, and preemption and intergovernmental immunity did not, because the state law in question regulated state, rather than federal, activity.[89] The court recognized that "[f]ederal schemes are inevitably frustrated when states opt not to participate in federal programs or enforcement efforts" but pointed out that "the Supreme Court has implied the existence of a 10th Amendment exception to reporting requirements" concerning exchanges of information.[90]

Notably, the court reached the opposite conclusion regarding a California law that required the state's attorney general to inspect federal detention facilities.[91] This law was subjected to full intergovernmental immunity analysis because it imposed an affirmative duty on a federal program,[92] rather than merely opting out of state participation.

The recommendations proposed in this report similarly do not impose any affirmative duty on a federal program. Admittedly, this is an unsettled area of the law, and no federal court with jurisdiction over Colorado[93] has ruled on this issue. However, the requirement that federal enforcers obtain a judicial warrant in order to obtain DMV photos and information, which do

---

[82] Art. VI, clause 2.

[83] North Dakota v. U.S., 495 United States 423, 435 (S. Ct. 1990).

[84] California, *supra* note 72, at 886.

[85] Arizona v. United States, 567 U.S. 387, 399 (S. Ct. 2012).

[86] California, *supra* note 72, at 891, 893.

[87] *Id.* at 888-89.

[88] Printz v. United States, 521 U.S. 898 (S. Ct. 1997).

[89] California, *supra* note 72, at 889-90.

[90] *Id.* The court distinguished *Reno v. Condon*, in which a federal law regulating state and private actors' disclosure of DMV data survived a 10th Amendment challenge. That law "evenhandedly" regulated activities of all actors, which happened to include state agencies. By contrast, all that was at issue in *California* was whether a federal law can compel participation by state and local entities.

[91] *Id.* at 882.

[92] *Id.*

[93] The federal District Court of Colorado, the 10th Circuit Court of Appeals, or the United States Supreme Court.

not pertain directly to immigration status,[94] is subject to the same logic as the California law discussed above. This California case shows that the federal government may be willing to go to court to remove protections for undocumented residents, but it also provides a clear legal path for defending these laws. The fact that similar protections to those recommended in this report have been challenged and upheld in another jurisdiction should encourage Colorado officials. While a court challenge from federal enforcers is possible, the outcome in *United States v. California* indicates that these recommendations do not conflict with any federal laws.

B. Law Enforcement Databases

The legal framework of obligations and regulations that guides NLETS protocol is more nuanced. Nevertheless, NLETs is not intended to offer federal agencies direct access to state databases outside the context of an active criminal investigation. Colorado's interactions with NLETS are structured through the Colorado Crime Information Center (CCIC), run by the Colorado Bureau of Investigations.[95] The Bureau describes the mission of the CCIC as providing and maintaining "criminal justice information in an effort to prevent crime and protect life and property."[96]

State law defines criminal justice records as materials "made, maintained or kept by any criminal justice agency in the state for use in the exercise of functions required or authorized by law or administrative rule."[97] Criminal justice agencies, under the same statute, include "any agency of the state that performs any activity directly related to the detection or investigation of a crime."[98] Similarly, the Bureau is authorized to create and maintain computerized systems for tracking information that may be pertinent to law enforcement, including "motor vehicle information received from the department of revenue accessible to law enforcement agencies through the telecommunications network operated by the bureau."[99]

The CCIC includes vehicle registration and driver license information.[100] However, while information furnished by the DMV to law enforcement pertinent to a criminal investigation clearly falls under this definition, DMV policy confirms that access to DMV records is procedurally restricted. The DMV recognizes that "Colorado law authorizes disclosure of records and information to authorized Government agencies, but such disclosure must be tied to the agency's official duties and functions."[101] The policy goes on to outline the processes for

---

[94] *E.g.,* Shapiro, *supra* note 8.

[95] Colorado Crime Information Center, *supra* note 44.

[96] *Id.*

[97] C.R.S. 24-72-302(4).

[98] C.R.S. 24-72-302(3).

[99] C.R.S. 24-33-412(c.5); *see generally* 24-33-412.

[100] Colorado Crime Information Center, *supra* note 44.

[101] Appendix A at 1.

requesting a specific dossier from the DMV.[102] Federal case law confirms that the CCIC is not required to maintain a complete database of Colorado DMV records.[103]

CCIC cites federal statute and regulation as the basis for its rules governing use of information.[104] These federal statutes and regulations do not conflict with the recommendations contained in this Report. The cited 18 USC 2721 requires disclosure of DMV records "for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers."[105] The statute also allows that these records "*may be* disclosed . . . for use by any Government agency, including any court or law enforcement agency, in carrying out its functions."[106] However, as with the Colorado statutes cited above, this law allows, but does not require, sharing of DMV records outside of the specific instances outlined in the state.

The federal regulation cited by the CCIC gives further context to the purpose of the database, and more specifically, the limits of that purpose. The regulation, which governs criminal justice information systems, defines criminal history record information as follows:

> "[I]nformation collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations (sic), or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. *The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.*"[107]

While not directly pertinent to DMV records, this definition makes clear that the creation of a unified state and federal criminal justice information database was intended to streamline sharing of specific criminal justice records. It was not intended to give every state and federal agency maximum access to all personal data collected by government entities across the country.

---

[102] *Id.*

[103] *See* United States v. Esquivel-Rios, 786 F.3d 1299, 1309-1310 (10th Cir. 2015). ("We also find unpersuasive Mr. Esquivel-Rios' argument that CBI's operation of the CCIC database ran afoul of an FBI mandate and Colorado statute. First, he provides no support for his argument concerning a federal mandate. Second, the Colorado statute he relies on, Colo. Rev. Stat. § 24-33.5-412(1)(c.5), permits but does not require CBI to "maintain a computerized data file of motor vehicle information." Further, that provision refers to "motor vehicle information *received from the department of revenue*." Id. (emphasis added). It is undisputed here that CBI did not receive from CDOR information pertaining to temporary tags until 2012.")

[104] Colorado Crime Information Center, *supra* note 42.

[105] 18 USC 2721 (1999).

[106] *Id.*

[107] 20 CFR 20.3(d) (1999).

All of this is to say that state and federal law gives Colorado discretion. The Department of Revenue has the authority under state and federal law to create specific exceptions to prevent access by ICE to protect the privacy of undocumented license-holders in Colorado.

C. Retaliation Outside the Courts

This report concludes that Colorado would not be violating state or federal law by protecting DMV records, but that does not guarantee that there is no risk of federal retaliation. For example, after New York restricted ICE access to DMV data as part of a driver license program for undocumented residents, DHS announced that it would be forced to deny or restrict New York's access to certain programs.[108] New York residents would no longer be eligible for Custom & Border Protection's Trusted Traveler Programs, and used vehicle exports from New York "will be significantly delayed and could be costlier."[109] Five days after this policy was announced, a leaked memo from DHS indicated that the Department had "drafted a slew of plants" to retaliate against states that restricted access to DMV data.

New York and DHS are attempting to reach a compromise under which New York would give DHS access to DMV information, but would redact social security numbers to protect undocumented residents.[110] The potential for DHS retaliation should not deter Colorado from keeping promises to the undocumented population, but might inform the specifics of these policies.

Conclusion

Access to DMV records and the use of facial recognition technology can both be powerful tools for law enforcement. However, like many tools available to law enforcement, they are also susceptible to abuse. Information sharing with federal agencies can lead to a breach of trust between the State of Colorado and immigrant communities, and can undermine the legislature's actions to promote safe roads. Unrestricted use of facial recognition technology gives law and immigration enforcement the ability to conduct invisible and sweeping surveillance. This surveillance is currently not subject to oversight by voters or their elected representatives.

The goal of these recommendations is not to impede legitimate law enforcement investigations, nor to condemn facial recognition as a useful tool for combatting crime. Rather, these recommendations offer a path to bring information sharing and facial recognition into compliance with American norms of privacy and the commitments that Colorado has made to its undocumented residents. Colorado lawmakers have historically sought to balance the need to provide tools to law enforcement with the imperative to protect residents from overreach,

---

[108] Letter from Chad Wolf, Act. Director, Dept. of Homeland Security, to Mark J. F. Schroeder, Acting Comm'r, N.Y. Dept. of Motor Vehicles (Feb. 5, 2020), on file with author & available at: https://www.scribd.com/document/445799731/DHS-Letter-to-NYS.

[109] *Id.*

[110] Tobias Hoonhout, "Cuomo Agrees to Give Feds Limited Access to New York DMV Records, but Will Still Try to Prevent Immigration Enforcement," National Review (Feb. 12, 2020 11:00 am), https://www.nationalreview.com/news/cuomo-agrees-to-give-feds-limited-access-to-ny-dmv-records-but-will-still-try-to-prevent-immigration-enforcement/.

including by respecting their privacy. By implementing these recommendations, Colorado's executive branch can more effectively safeguard that balance.

Appendix A: DMV Information Sharing Policy Memo

COLORADO
Department of Revenue
Division of Motor Vehicles

Investigations Unit
Physical Address:
1881 Pierce Street
Lakewood, CO 80214

Mailing Address:
P.O. Box 173350
Denver, CO 80217-3350

MEMORANDUM

To: Jean Robinson, Legislative Liasion

From: Ted Trujillo, Deputy Director - DMV

CC: Mike Dixon, Senior Director - DMV, Flavio Quintana, Deputy Director - DMV, Ben Mitchell, Director - Driver Control,

Date: September 9, 2019

Subject: Questions Regarding ICE

Colorado law allows disclosure of records and information collected by the DMV to authorized Government agencies, but such disclosure must be tied to the agencies' official duties and functions pursuant to (24-72-302(3), C.R.S). The following is a summary of procedures involved:

ROLES & RESPONSIBILITIES

- The DMV Driver Control Section's Law Enforcement Communication Center (LECC) staff is responsible for assisting authorized agencies with requests of DMV resources that are used to aid such agency with their official duties/ functions through 24/7 communication via NLETS, E-Mail and Phone.
- The DMV Motor Vehicle Investigations Unit (MVIU) staff support the LECC with requests that are outside of the purview of the LECC, such as image comparison requests or when an agency seeks to report fraud to the DMV.

DOSSIER:
A law enforcement agency can request a dossier to assist with positive identification of a victim or subject in an investigation. A dossier includes the customer's name, DOB, height, weight, gender, address, fingerprint, signature and photo. This information is also accessible to authorized users through NLETS (CCIC/NCIC).

IMAGE COMPARISONS:
A law enforcement agency can request an image comparison for a case that is defined as a Level 1 offense. A Level 1 offense includes national security violations, homicide, kidnapping, sexual assault, robbery, aggravated assault, threats of bodily harm, extortion or threat to injure a person, sex offenses, cruelty toward children or spouse, resisting an officer and weapons and any other crimes that are felony level.

The DMV MVIU corresponds with all law enforcement agencies, to include the Department of Homeland Security (DHS).

COLORADO
Department of Revenue
Division of Motor Vehicles

Investigations Unit
Physical Address:
1881 Pierce Street
Lakewood, CO 80214

Mailing Address:
P.O. Box 173350
Denver, CO 80217-3350

MEMORANDUM

To: Jean Robinson, Legislative Liasion

From: Ted Trujillo, Deputy Director - DMV

CC: Mike Dixon, Senior Director - DMV, Flavio Quintana, Deputy Director - DMV, Ben Mitchell, Director - Driver Control,

Date: September 9, 2019

Subject: Questions Regarding ICE

Colorado law allows disclosure of records and information collected by the DMV to authorized Government agencies, but such disclosure must be tied to the agencies' official duties and functions pursuant to (24-72-302(3), C.R.S). The following is a summary of procedures involved:

ROLES & RESPONSIBILITIES

- The DMV Driver Control Section's Law Enforcement Communication Center (LECC) staff is responsible for assisting authorized agencies with requests of DMV resources that are used to aid such agency with their official duties/ functions through 24/7 communication via NLETS, E-Mail and Phone.
- The DMV Motor Vehicle Investigations Unit (MVIU) staff support the LECC with requests that are outside of the purview of the LECC, such as image comparison requests or when an agency seeks to report fraud to the DMV.

DOSSIER:
A law enforcement agency can request a dossier to assist with positive identification of a victim or subject in an investigation. A dossier includes the customer's name, DOB, height, weight, gender, address, fingerprint, signature and photo. This information is also accessible to authorized users through NLETS (CCIC/NCIC).

IMAGE COMPARISONS:
A law enforcement agency can request an image comparison for a case that is defined as a Level 1 offense. A Level 1 offense includes national security violations, homicide, kidnapping, sexual assault, robbery, aggravated assault, threats of bodily harm, extortion or threat to injure a person, sex offenses, cruelty toward children or spouse, resisting an officer and weapons and any other crimes that are felony level.

The DMV MVIU corresponds with all law enforcement agencies, to include the Department of Homeland Security (DHS).

COLORADO
Department of Revenue
Division of Motor Vehicles

Investigations Unit
Physical Address:
1881 Pierce Street
Lakewood, CO 80214

Mailing Address:
P.O. Box 173350
Denver, CO 80217-3350

MEMORANDUM

To: Jean Robinson, Legislative Liasion

From: Ted Trujillo, Deputy Director - DMV

CC: Mike Dixon, Senior Director - DMV, Flavio Quintana, Deputy Director - DMV, Ben Mitchell, Director - Driver Control,

Date: September 9, 2019

Subject: Questions Regarding ICE

Colorado law allows disclosure of records and information collected by the DMV to authorized Government agencies, but such disclosure must be tied to the agencies' official duties and functions pursuant to (24-72-302(3), C.R.S). The following is a summary of procedures involved:

ROLES & RESPONSIBILITIES

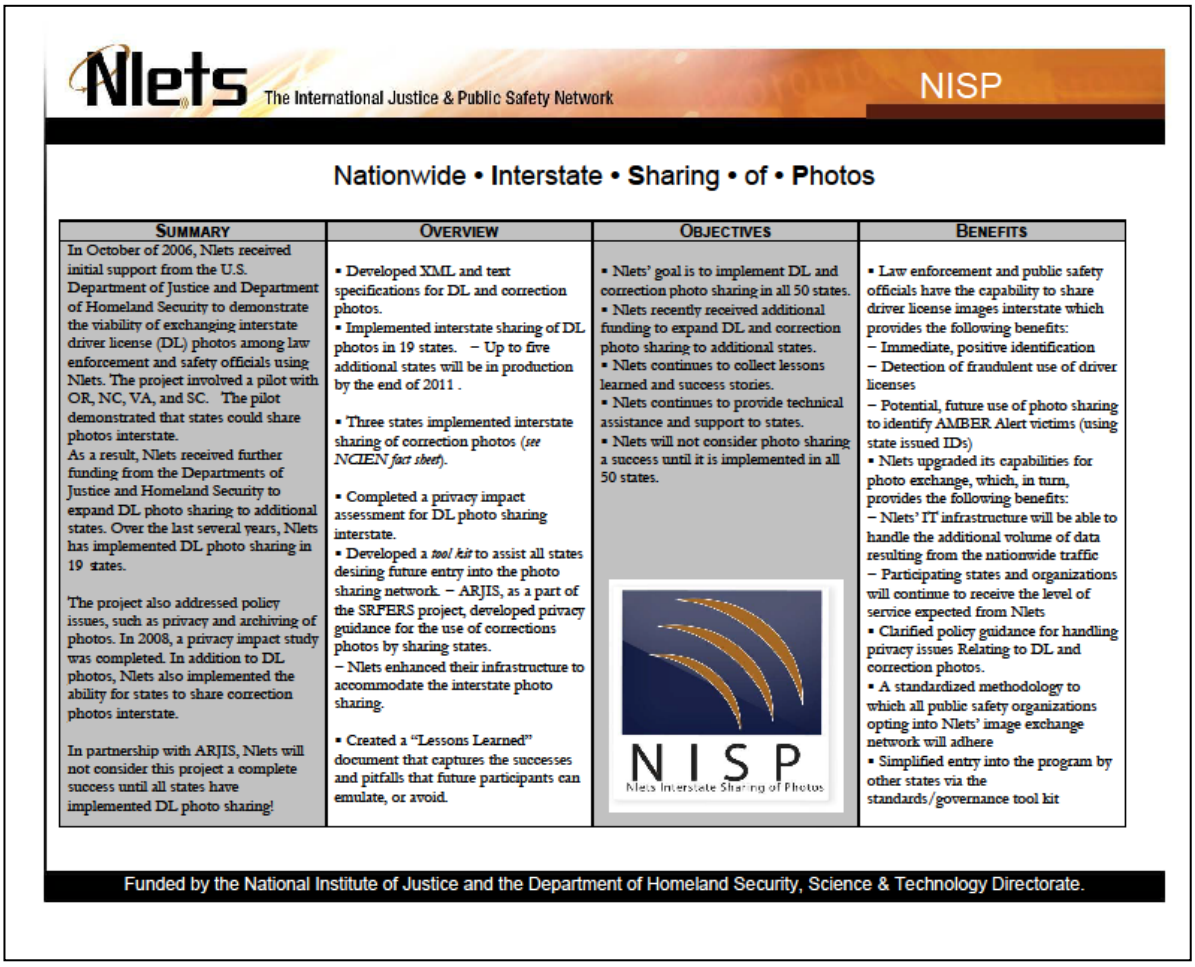
- The DMV Driver Control Section's Law Enforcement Communication Center (LECC) staff is responsible for assisting authorized agencies with requests of DMV resources that are used to aid such agency with their official duties/ functions through 24/7 communication via NLETS, E-Mail and Phone.
- The DMV Motor Vehicle Investigations Unit (MVIU) staff support the LECC with requests that are outside of the purview of the LECC, such as image comparison requests or when an agency seeks to report fraud to the DMV.

DOSSIER:
A law enforcement agency can request a dossier to assist with positive identification of a victim or subject in an investigation. A dossier includes the customer's name, DOB, height, weight, gender, address, fingerprint, signature and photo. This information is also accessible to authorized users through NLETS (CCIC/NCIC).

IMAGE COMPARISONS:
A law enforcement agency can request an image comparison for a case that is defined as a Level 1 offense. A Level 1 offense includes national security violations, homicide, kidnapping, sexual assault, robbery, aggravated assault, threats of bodily harm, extortion or threat to injure a person, sex offenses, cruelty toward children or spouse, resisting an officer and weapons and any other crimes that are felony level.

The DMV MVIU corresponds with all law enforcement agencies, to include the Department of Homeland Security (DHS).

Appendix B: National Image Sharing Program Fact Sheet[111]



Nlets The International Justice & Public Safety Network

NISP

Nationwide • Interstate • Sharing • of • Photos

SUMMARY	OVERVIEW	OBJECTIVES	BENEFITS
In October of 2006, Nlets received initial support from the U.S. Department of Justice and Department of Homeland Security to demonstrate the viability of exchanging interstate driver license (DL) photos among law enforcement and safety officials using Nlets. The project involved a pilot with OR, NC, VA, and SC. The pilot demonstrated that states could share photos interstate. As a result, Nlets received further funding from the Departments of Justice and Homeland Security to expand DL photo sharing to additional states. Over the last several years, Nlets has implemented DL photo sharing in 19 states. The project also addressed policy issues, such as privacy and archiving of photos. In 2008, a privacy impact study was completed. In addition to DL photos, Nlets also implemented the ability for states to share correction photos interstate. In partnership with ARJIS, Nlets will not consider this project a complete success until all states have implemented DL photo sharing!	▪ Developed XML and text specifications for DL and correction photos. ▪ Implemented interstate sharing of DL photos in 19 states. – Up to five additional states will be in production by the end of 2011 . ▪ Three states implemented interstate sharing of correction photos (*see NCIEN fact sheet*). ▪ Completed a privacy impact assessment for DL photo sharing interstate. ▪ Developed a *tool kit* to assist all states desiring future entry into the photo sharing network. – ARJIS, as a part of the SRFERS project, developed privacy guidance for the use of corrections photos by sharing states. – Nlets enhanced their infrastructure to accommodate the interstate photo sharing. ▪ Created a "Lessons Learned" document that captures the successes and pitfalls that future participants can emulate, or avoid.	▪ Nlets' goal is to implement DL and correction photo sharing in all 50 states. ▪ Nlets recently received additional funding to expand DL and correction photo sharing to additional states. ▪ Nlets continues to collect lessons learned and success stories. ▪ Nlets continues to provide technical assistance and support to states. ▪ Nlets will not consider photo sharing a success until it is implemented in all 50 states. NISP Nlets Interstate Sharing of Photos	▪ Law enforcement and public safety officials have the capability to share driver license images interstate which provides the following benefits: – Immediate, positive identification – Detection of fraudulent use of driver licenses – Potential, future use of photo sharing to identify AMBER Alert victims (using state issued IDs) ▪ Nlets upgraded its capabilities for photo exchange, which, in turn, provides the following benefits: – Nlets' IT infrastructure will be able to handle the additional volume of data resulting from the nationwide traffic – Participating states and organizations will continue to receive the level of service expected from Nlets ▪ Clarified policy guidance for handling privacy issues Relating to DL and correction photos. ▪ A standardized methodology to which all public safety organizations opting into Nlets' image exchange network will adhere ▪ Simplified entry into the program by other states via the standards/governance tool kit

Funded by the National Institute of Justice and the Department of Homeland Security, Science & Technology Directorate.

[111] Available at: NLETS, *Documents*, "NISP Fact Sheet" (last visited Nov. 11, 2019 8:44 PM).