March 13, 2017

The Honorable Mike Dunleavy, Chair
Senate State Affairs Committee
Alaska State Senate
State Capitol
Juneau, AK 99801

Sent by email: Senator.Mike.Dunleavy@akleg.gov

Re: ACLU Analysis of SB 34, Concerning the Federal REAL ID Act

Dear Chair Dunleavy:

Thank you for the opportunity to testify about Senate Bill 34, which would create a new system in Alaska for issuing driver's licenses and identity cards. The American Civil Liberties Union of Alaska appreciates the committee's hearing our concerns and considering the recommendations we set out below.

Governor Walker has introduced SB 34 in response to the demands of the Federal REAL ID Act of 2005.[1] Under REAL ID, a person who wishes to use a state-issued driver's license or identity card to enter a federal facility or to pass through a federally controlled checkpoint—for example, to enter a military base or to board a plane—will only be able to use a license or card that complies with the standards of REAL ID (a "compliant" card). Alternatively, a person without a compliant state-issued license or card could use a federally-issued form of identification, such as a U.S. passport or military identification card.

Unfortunately for Alaskans who hold their privacy dear, the REAL ID standards include sharing information about license and card holders in an unprecedented, multi-state database that will contain information about virtually every driver's license and identity card holder in the United States. Also, REAL ID will require that each state scan and store identity documents about license and card holders. Such concentrations of information about Alaskans and other Americans are certain to be the target of would-be identity thieves. It would be a one-stop shop for identity thieves. Furthermore, the mere existence of such convenient, centralized identity information stores will undoubtedly become tempting to future lawmakers and government officials who prioritize expediency over privacy. It may contribute to "surveillance state creep."

[1] Throughout this testimony, "the REAL ID Act" and "REAL ID" refer to the Federal REAL ID Act of 2005. "The Governor's REAL ID bill," in contrast, refers to Senate Bill 34 – Driver's License & Id Cards & Real Id Act.

Because of the privacy compromises imposed by the REAL ID Act, the ACLU has opposed it since its inception in Congress. Likewise, Alaska voiced its opposition by enacting Senate Bill 202 in 2008, which prohibited the expenditure of any funds to comply with REAL ID.[2] Now, after years of resistance from Alaska and many other states, and after years of temporary deadline extensions from the Department of Homeland Security, Alaska is considering moving forward with compliance. Other states are taking similar steps at this time.

If Alaska is going to move forward with compliance, the ACLU of Alaska strongly supports the approach in SB 34 of providing residents the option of obtaining a noncompliant license or card, at a lower cost. It is critical that every step be taken to minimize what documents and information are collected and stored, and to share with other states only the minimum information required by REAL ID. And in offering noncompliant licenses and cards, it is important to provide meaningful privacy protections that are not otherwise available to REAL ID license and card applicants. This is critical not least because even information about *noncompliant* license and card holders will almost certainly be included in the multi-state database of any state complying with the REAL ID Act.

Each of the ACLU's recommended changes to the Governor's bill, and the supporting reasons, are set forth below. For ease of reference, we are also enclosing a short bullet-point list of the changes described.

Storage of Identity Documents

REAL ID requires states to store a digital copy of at least one approved document used to establish the identity of a compliant driver's license or identity card holder, e.g., a valid U.S. passport, an original or certified copy of a U.S. birth certificate, or another REAL ID compliant license or card.[3] The digital image of the identity document must be kept by DMV for a minimum of 10 years.[4]

We are unaware of any current regulation or practice in Alaska requiring the copying and storage of such sensitive documents. And for good reason: it serves no purpose. To the extent it is useful to a DMV official to examine an applicant's passport, for example, in order to verify the person's identity, it is useful only while the official has the passport in hand. We recommend that current DMV practices be enshrined in the Governor's REAL ID bill for noncompliant licenses and cards, by prohibiting the copying, scanning, or storage of identity documents for those applicants.

---

[2] This is currently codified at AS 44.99.040(a)(2) ("A state or municipal agency may not use or authorize the use of an asset to implement or aid in the implantation of a requirement of . . . P.L. 109-13, Division B (REAL ID Act of 2005).").

[3] REAL ID Act, Pub. L. No. 109-13, § 202(d)(1), 119 Stat. 302, 314 (2005).

[4] *Id.* at § 202(d)(2).

Concerning compliant licenses and cards, Alaska should keep one—and only one—digital image of an identity document for each license or card holder. Alaska should keep that digital image for only 10 years and then destroy it. Specific language should be used to ensure that the documents are destroyed after ten years.

Storage of Other Documents

Under REAL ID, copies of the application and declaration for compliant driver's license and identity card holders must be kept. The REAL ID Act provides the option of storing these documents in paper, microfiche, or digital form. Because the application contains the Social Security number, DMV should not copy or scan it, but should instead retain only the original paper application. Similarly, the declaration should simply be retained without being copied. After seven years, both documents should be destroyed. The ACLU recommends adopting specific language that would ensure that only the original application and declaration are retained and that they are destroyed after the seven-year mandatory time period.

Applicants may present other documents when applying for a compliant license or card—for example, a utility bill to establish one's address of principal residence, or a W-2 form to verify one's Social Security number. Because these do not meet the REAL ID regulations' definition of "source documents," they should not be copied or scanned and should not be retained. Specific language should be added to the Governor's REAL ID bill restricting the copying, scanning, or retention of these non-source documents.

Concerning noncompliant licenses and cards, the ACLU recommends that the current kinds of records kept by DMV be enshrined in the legislation to differentiate compliant from noncompliant cards. Currently, DMV maintains a file containing the application for a driver's license or identity card, and information about the license and license-holder, such as whether the license has been suspended.[5] We believe that DMV's current practices should remain mostly unchanged, but that section 28.15.151 be amended to indicate that it applies to noncompliant license and card applicants. The one substantive change we recommend is that, instead of retaining the record for 15 years before destroying it,[6] the records should be destroyed after the same seven years required for REAL ID Act compliant cards. There is no reason to retain documents and records for noncompliant licenses and cards longer than they are retained for compliant licenses and cards.

Finally, if for any reason any of these records are kept in digital form—whether for compliant or noncompliant licenses and cards—the ACLU urges the Legislature to clarify that these documents should not be stored in the multi-state shared database.

---

[5] AS 28.15.151; 2 AAC 90.475.

[6] 2 AAC 90.475(a).

Facial Image Capture

REAL ID license and card applicants must have an image of their face captured and stored, even if no license or card is issued. The Governor's REAL ID bill should clarify that these images should be stored for no longer than required by REAL ID: five years if no license or card is issued and two years after the expiration date if a license or card is issued. After the appropriate period of time, the images should be destroyed.

Noncompliant applicants should not have images of their faces captured and stored if they do not receive a license or card. The image of the face of a recipient of a noncompliant license or card should only be retained for two years after the license or card expires, after which the image should be destroyed.[7]

Concerning both compliant and noncompliant licenses and cards, images of applicants' faces should not be stored in the multi-state shared database required by REAL ID. The Governor's REAL ID bill should be amended to ensure they are not.

Furthermore, the Legislature should explicitly prohibit DMV from being pressured to participate in federal government experiments in "next generation identification systems," such as automated facial recognition systems. The alarming existence of such an FBI endeavor was recently highlighted in a critical report from the federal Government Accounting Office (GAO), titled "Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy."[8] According to the GAO's report, Alaska's DMV is not participating in this woeful, privacy-compromising facial-recognition system. The Legislature should ensure it never does.

Social Security Numbers

The REAL ID Act requires states to collect Social Security numbers on applications for driver's licenses and identity cards and to verify the accuracy of the Social Security numbers given. Current DMV practices already include doing this,[9] in part to facilitate the child support provisions of AS 25.27.010.

It is important to note that Social Security numbers are incredibly valuable to identity thieves. The critical importance of securing Alaskans' privacy by not compromising their Social Security numbers has already prompted the Legislature to insist that Social Security

---

[7] 2 AAC 90.485(b) provides, "The department will maintain a record of the digital image and signature of a licensee or holder of an identification card, together with other data required by the department for identification and retrieval." Presumably, this is retained for 15 years pursuant to 2 AAC 90.475(a). Again, we see no compelling reason for Alaska to keep records for noncompliant license and card holders for 15 years, as currently required by 2 AAC 90.475(a), when even REAL ID compliance standards do not require records to be kept that long.

[8] U.S. Government and Accountability Office, May 2016, http://www.gao.gov/assets/680/677098.pdf.

[9] AS 28.15.061.

numbers not be displayed on Alaskans' driver's licenses and identity cards.[10] In keeping, the Legislature should similarly instruct that Social Security numbers, in whole or in part, not be included in the information contained in the multi-state shared database.

Multi-state Database Containing Information about Alaskans

REAL ID requires each compliant state to maintain certain information in a database that can be accessed by other states. It is essential that, if it opts to comply with REAL ID, Alaska only share the least amount of information in this database.

Specifically, the only information that must be contained in the multi-state shared database is the information contained in the data fields printed on licenses and cards, and drivers' histories. The Legislature should instruct than only this information may be included. No other information should be co-mingled in this database. As discussed above, there should be no Social Security numbers, in whole or in part, included in the shared database. Including Social Security numbers in the shared database is not required by REAL ID, and there is no reason to compromise Alaskans' privacy by including such sensitive information.

Additional Privacy Safeguards

We also recommend that the Governor's REAL ID bill be amended to include additional safeguards that ensure the noncompliant card option is a meaningful one. We recommend that applicants be notified that they have a choice between compliant and noncompliant licenses and cards, with a clear, meaningful description of the benefits and risks of each option. Notification should be included with applications, should be available on the DMV website, and should be included in renewal notices.

Furthermore, we urge Alaska to join the growing number of states that issue driver's licenses and identity cards without inquiring into applicants' immigration or citizenship status. Increasingly, states and cities across the United States are becoming alert to the value of issuing driver's licenses or identity cards to all residents whose identity and residency can be confirmed.[11] Meanwhile, there is no state interest furthered by inquiring into the immigration or citizenship status of would-be drivers and identity card holders. Neither DMV nor any state or local law enforcement agency is authorized to enforce federal immigration laws. There is no reason for Alaska to inquire into this aspect of an applicant's background.

---

[10] AS 28.15.11(a) ("A license may not display the licensee's social security number.").

[11] As of June 2016, 12 states, the District of Columbia, and Puerto Rico provide for the issuance of driver's licenses and identity cards without requiring applicants to establish their immigration status.

Conclusion

Thank you for considering our testimony. If you have any questions or if we may offer more information, please let us know.

Sincerely,

Eric Glatt
Staff Attorney

cc: Senator John Coghill, Senator.John.Coghill@akleg.gov
Senator Dennis Egan, Senator.Dennis.Egan@akleg.gov
Senator Cathy Giessel, Senator.Cathy.Giessel@akleg.gov
Senator David Wilson, Senator.David.Wilson@akleg.gov

Storage of Identity Documents (e.g., valid U.S. passport, U.S. birth certificate, another REAL ID compliant license or card)	
REAL ID Compliant	**Noncompliant**
• Keep only one digital image of an identity document for each driver's license or identity card holder; • Keep the digital image of an identity document for only 10 years and then destroy it.	• Prohibit copying in and retaining in any form identity-verifying documents such as passports, birth certificates, etc.

Storage of Other Documents (e.g., the application, documents establishing one's Social Security Number and principal residence)	
REAL ID Compliant	**Noncompliant**
• Retain only the original application; • Because the application contains the Social Security Number, do not copy or scan it; • After seven years, destroy the application; • Do not copy, scan, or store any other documents, including documents used to verify a Social Security Number (e.g., W-2 form, 1099 form, pay stub) or principal residence (e.g., utility bill, rental agreement, 1099 form).	

Facial Image Capture	
REAL ID Compliant	**Noncompliant**
• Store images of applicants' faces, if they do not receive a driver's license or identity card, for only 5 years and then destroy them.	• Do not store images of applicants' faces if they do not receive a license or card.
• Store images of applicants' faces, if they do receive a REAL ID or noncompliant license or card, for only 2 years after the expiration date and then destroy the images; • Do not store images of faces in the multi-state shared database; • Do not share images of faces with any other state or with the federal government, e.g., to participate in FBI endeavors to create a facial recognition system for a "next generation identification system."[1]	

[1] "Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy," U.S. Gov't and Accountability Office, May 2016, http://www.gao.gov/assets/680/677098.pdf.

Multi-State Database [2]	
REAL ID Compliant	**Noncompliant**
Only provide the information contained in the data fields printed on driver's licenses and identity cards, and drivers' histories in the multi-state database (prohibit providing Social Security Numbers, in whole or in part, images of faces, access to or copies of identity documents).	

Additional Privacy Safeguards

- Provide applicants with clear, meaningful notice of the choice between a REAL ID compliant and noncompliant driver's license or identity card; provide notice of the choice with applications, on the DMV website, in renewal notices, and wherever else it is reasonable.
- For noncompliant licenses and identification cards, provide that an applicant's date and place of birth can be verified by presenting:

  a certified original or certified copy of a U.S. birth certificate;

  a U.S. passport or passport card issued by the U.S. Department of State;

  a foreign passport;

  a resident alien, temporary resident alien, or employment work authorization document issued by DHS;

  a U.S. armed forces active duty, retiree, or reservist identification; or

  other evidence of comparable validity.
- For noncompliant licenses and identification cards, provide that proof of a valid Individual Taxpayer Identification Number—including a letter addressed to the applicant from the Internal Revenue Service, U.S. Department of the Treasury, assigning the applicant an ITIN—may be used in lieu of a Social Security Number for applicants who do not have an SSN.

[2] REAL ID Act, Pub. L. No. 109-13, § 202(d)(12) & (13), 119 Stat. 302, 314 (2005).