March 26, 2017

The Honorable Lyman Hoffman, Co-Chair
The Honorable Anna MacKinnon, Co-Chair
The Honorable Click Bishop, Vice Chair
Senate Finance Committee
Alaska State Senate
State Capitol
Juneau, AK 99801

Sent by email: Senator.Lyman.Hoffman@akleg.gov
Senator.Anna.MacKinnon@akleg.gov
Senator.Click.Bishop@akleg.gov

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

Dear Co-Chairs Hoffman and MacKinnon, and Vice-Chair Bishop:

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 forth below. We are also submitting proposed amendments to SB 34 Version O—the Committee Substitute bill that was introduced by Senator Dunleavy and passed by the Senate State Affairs Committee—to which this testimony refers.

Alaskans' Privacy and the Federal REAL ID Act

Governor Walker 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, passport card, or military identification card.

[1] Throughout this testimony, "the REAL ID Act," "the 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.

For Alaskans who hold their privacy dear, unfortunately, the REAL ID standards include sharing information about licensees and cardholders in a multi-state database network. Each compliant state must maintain a database of information and must make that database accessible to all other compliant states. For a pilot program of 14 states including Alaska, an additional, central database was created—notwithstanding that there is no such requirement in the Act—to facilitate connections among the required databases. Furthermore, REAL ID requires that each state scan and store "identity source documents" about licensees and cardholders that Alaska currently does not store.

Such concentrations of information about Alaskans and other Americans are certain to be the target of hackers and identity thieves. Also, the mere existence of such convenient, centralized stores of identity information will undoubtedly become tempting to future government actors who prioritize expediency over privacy. Accessing data about people for purposes not contemplated when that data was first collected has become a disturbing feature of "big data" surveillance creep.

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] If Alaska is now going to move forward with compliance, the ACLU of Alaska supports the approach in SB 34 of providing residents the option of obtaining a noncompliant license or card, at a lower cost.

To better serve Alaskans' privacy interests, we further urge the legislature to ensure that every step is 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. We also urge the legislature to ensure that meaningful privacy protections are enshrined in law that distinguish compliant from noncompliant licenses and cards. We are pleased to note that the CS passed by the Senate State Affairs Committee addressed several of our concerns. To continue in the direction set forth in that CS, we share the following recommendations:

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 the Division of Motor Vehicles for a minimum of ten years.[4]

---

[2] 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).

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. For example, to the extent it is useful to a DMV official to examine an applicant's passport 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. This can be accomplished through our proposed Amendment 1, where it creates a new AS 18.65.310(n)(1).

Concerning compliant licenses and cards, Alaska should keep one—and only one—digital image of an identity document for each licensee or cardholder. Alaska should keep that digital image for only ten years and then destroy it. Specific language should be used to ensure that the documents are destroyed after ten years. This can be accomplished through our proposed Amendment 1, where it creates a new AS 18.65.310(m)(1).

Storage of Applications and Declarations

Under REAL ID, the original application and declaration for a compliant driver's license or identity card 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 (SSN), DMV should not copy or scan it but instead should retain only the original paper application. Similarly, the declaration should simply be retained without being copied. After seven years, both documents should be destroyed. This can be accomplished through our proposed Amendment 1, where it creates a new AS 18.65.310(m)(2).

Applications and declarations for noncompliant licenses and cards should also not be copied or scanned, but kept in original form only and then destroyed after seven years. This can be accomplished through our proposed Amendment 1, where it creates a new AS 18.65.310(n)(2).

Storage of Verifying Documents

Applicants may present other documents to DMV when applying for a compliant license or card—for example, a utility bill to verify 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 prohibiting the copying, scanning, or retention of these non-source documents. This can be accomplished through our proposed Amendment 1, where it creates a new AS 18.65.310(m)(2).

Similarly, for noncompliant licenses and cards, the legislature should ensure that such verifying documents are not copied, scanned, or retained. This can be accomplished through our proposed Amendment 1, where it creates a new AS 18.65.310(n)(2).

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. This can be accomplished through our proposed Amendment 1, where it creates a new AS 18.65.310(m)(3).

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 one year after the license or card expires, after which the image should be destroyed.[5] This can be accomplished through our proposed Amendment 1, where it creates a new AS 18.65.310(n)(3).

Concerning both compliant and noncompliant licenses and cards, the Governor's REAL ID bill should be amended to ensure that images of applicants' faces should not be stored in the multi-state networked database required by REAL ID. This can be accomplished through our proposed Amendment 3, where it creates a new AS 28.05.068(c)(1).

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. Such alarming, privacy-eroding programs are coming under increasing scrutiny by lawmakers nationwide. Congress held a hearing about this troubling practice as recently as last week, on March 22.[6] Last May, the U.S. Government Accounting Office issued a critical report titled "Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy."[7] 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. This was accomplished through the introduction of AS 28.05.068, added to SB 34 by the CS passed by the Senate State Affairs Committee.

---

[5] 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). 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.

[6] *Committee to Review Law Enforcement's Policies on Facial Recognition Technology*, U.S. HOUSE OF REPRESENTATIVES, FULL HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, (Mar. 22, 2017), https://oversight.house.gov/hearing/law-enforcements-use-facial-recognition-technology/.

[7] U.S. GOVERNMENT AND ACCOUNTABILITY OFFICE, (May 2016), http://www.gao.gov/assets/680/677098.pdf.

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,[8] in part to facilitate the child support provisions of AS 25.27.010.

It is important to note that SSNs are incredibly valuable to identity thieves. [9] The critical importance of securing Alaskans' privacy by not compromising their SSNs has already prompted the Legislature to insist that the numbers not be displayed on Alaskans' driver's licenses and identity cards.[10] This is a concern shared by the Social Security Administration, which endeavors to keep the public informed of the importance of keeping their SSNs secure.[11] The SSA advises:

> Identity theft is one of the fastest growing crimes in American society. The routine and often indiscriminate use of SSNs as identifiers creates opportunities for individuals to inappropriately obtain personal information. Repetitive use and disclosure of SSNs in organizational record keeping systems, multiplies the susceptibility of persons to potential identity theft. Through misuse of SSNs, individuals are subject to the danger of identity theft and its repercussions. Access to an individual's SSN can enable an identity thief to obtain information that can result in significant financial difficulties for the victim. While this can be disruptive for the individual, it can also lead to civil liability for the organization and its individual employees if someone is harmed by information that has been made available to others.[12]

The SSA goes on to "strongly urge all organizations that use SSNs as the identifier in their record keeping systems to use alternate identifiers."[13]

---

[8] AS 28.15.061.

[9] One recent report suggests that a single Social Security number can fetch $30 in a black market dossier. Jeanine Skowronski, *What Your Information Is Worth on the Black Market*, BANKRATE.COM, (July 27, 2015), http://www.bankrate.com/finance/credit/what-your-identity-is-worth-on-black-market.aspx.

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

[11] *See, e.g.,* "Identity Theft and Your Social Security Number," SOCIAL SECURITY ADMINISTRATION, SSA Publication No. 05-10064, (Nov. 2016), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf; *Avoid Identity Theft: Protect Social Security Numbers*, SOCIAL SECURITY ADMINISTRATION, PHILADELPHIA REGION, https://www.ssa.gov/phila/ProtectingSSNs.htm; *Social Security Numbers: The SSN Numbering Scheme*, SOCIAL SECURITY ADMINISTRATION, https://www.ssa.gov/history/ssn/geocard.html.

[12] *Id.*, *Avoid Identity Theft: Protect Social Security Numbers.*

[13] *Id.*

In keeping, the Legislature should prohibit SSNs, in whole or in part, from being included among the information contained in the multi-state networked database required by REAL ID, or in any index created to locate records in that database.

Our concern is not hypothetical: Alaska is one of 14 states currently participating in a pilot program—the State-to-State (S2S) Verification Service, operated by the American Association of Motor Vehicle Administrators (AAMVA)—that uses the last 5 digits of license and card holders' SSNs as an element of its identification "platform." This has already been testified to by the Department of Administration and DMV, in a February 23, 2017, presentation it gave to the Senate State Affairs Committee.[14]

Limiting use of SSNs to the last 5 digits, such as the DMV is doing with S2S, is not sufficient to eliminate the threat posed by identity thieves. Including these five digits with other personally identifiable information about people leaves those people susceptible to thieves' reconstructing the remaining 4 digits. For most Social Security cardholders, this is not a function of pure guesswork. Only since June 2011 has the SSA assigned numbers via a randomized process.[15] Until then, the first 3 digits of SSNs were directly associated with the state either in which a Social Security card was issued or, between 1973 and mid-2011, of an applicant's ZIP code.[16] Every Alaskan who obtained an SSN before 2011 almost certainly has a number beginning with 574. Knowing these 3 first digits, plus the final 5 digits, leaves only one remaining digit for an identity thief to guess.

Eliminating this privacy vulnerability can be accomplished through our proposed amendments to AS 28.05.068.

Multi-state Networked 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 retain the least amount of information in this database. We note that in the S2S pilot program being operating by AAMVA, a central index has been created containing personally identifiable information about every individual record in every networked database, even though creating such a national, centralized index is not required by the Act.

---

[14] Commissioner Sheldon Fisher, Deputy Commissioner Leslie Ridle, and DMV Director Marla Thompson, *SB 34 Driver's Licenses and ID Cards and REAL ID Act*, DEPARTMENT OF ADMINISTRATION, (Feb. 23, 2017), page 8, http://www.akleg.gov/basis/get_documents.asp?session=30&docid=12472.

[15] *See, e.g., Social Security Number Allocations*, SOCIAL SECURITY ADMINISTRATION, https://www.ssa.gov/employer/stateweb.htm; *Social Security Number Randomization*, SOCIAL SECURITY ADMINISTRATION, https://www.ssa.gov/employer/randomization.html.

[16] *Id.*, *Social Security Number Allocations*.

Specifically, the only information that must be contained in the multi-state networked database is the information contained in the data fields printed on licenses and cards, and drivers' histories. The Legislature should instruct that only this information may be included in the database. No other information should be co-mingled with it. 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. Furthermore, there is no requirement that compliant states include information about noncompliant licensees and cardholders in the REAL ID database or in any index created to locate records in that database.

These privacy enhancements can be secured through our proposed amendments to AS 28.05.068.

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 have recommended 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. The CS includes a notification requirement, which we have built upon in our proposed Amendment 1, where we recommend a new AS 18.65.310(o), and in our proposed Amendment 2, where we recommend a new AS 28.15.041(f).

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.[17] Meanwhile, there is no state interest furthered by inquiring into the immigration or citizenship status of safe drivers and or of 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. This can be accomplished through our Amendment 5 and through other technical fixes.

Conclusion

Thank you for considering our testimony. If you have any questions or if we may offer more information, please let us know. We look forward to the opportunity of ensuring that

[17] 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.

Alaskans' privacy is secured to the greatest extent possible, including under the coercive conditions established by the REAL ID Act.

Sincerely,

Eric Glatt
Staff Attorney

cc: Senator Peter Micciche, Senator.Peter.Micciche@akleg.gov
Senator Mike Dunleavy, Senator.Mike.Dunleavy@akleg.gov
Senator Natasha von Imhof, Senator.Natasha.vonImhof@akleg.gov
Senator Donald Olson, Senator.Donald.Olson@akleg.gov