



March 27, 2017

The Honorable Jonathan Kreiss-Tomkins, Chair
The Honorable Gabrielle LeDoux, Vice Chair
House State Affairs Committee
Alaska State House of Representatives
State Capitol
Juneau, AK 99801

Sent by email: Representative.Jonathan.Kreiss-Tomkins@akleg.gov
Representative.Gabrielle.LeDoux@akleg.gov

Re: Follow Up to Questions Regarding HB 74

Dear Chair Kreiss-Tomkins and Vice Chair LeDoux:

We are writing to follow up on three questions that were posed to the ACLU during testimony before the House State Affairs Committee on Tuesday, March 21, 2017.

(1) Facial recognition system.

We were asked two questions generally about facial recognition on which we agreed to follow up: (1) what are the purposes for which it is being used in other states, and (2) what is the government doing with facial recognition data?

Some states have adopted facial recognition technology for general surveillance, which can be used with public video cameras. For example, facial recognition systems have been implemented in airports, including Logan Airport in Boston, T.F. Green Airport in Providence, Rhode Island, and San Francisco International Airport. In April 2016, the Baltimore Police Department used facial recognition to identify, track, and arrest certain people protesting Freddie Gray's death in police custody.¹ In 2013, Los Angeles installed 16 wireless video cameras equipped to conduct real-time facial recognition at undisclosed locations throughout the city. New York City is now looking to implement similar cameras at bridges and tunnels throughout the city.²

¹ Russell Brandom, *Facebook, Twitter, and Instagram surveillance tool was used to arrest Baltimore protesters*, The Verge, Oct. 11, 2016, available at <http://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api>.

² Harriet Taylor, *New York City wants more information on where you're going*, CNBC, Jan. 9, 2017, available at <http://www.cnbc.com/2017/01/09/new-york-city-wants-more-information-on-where-youre-going.html>.

Other states have allowed law enforcement access to their driver's license or identity card databases in order to pursue law enforcement goals, including driver's license fraud. According to a recent report by the Center on Privacy and Technology at Georgetown Law, more than half of all U.S. adults are now in a law enforcement facial recognition network through photographs that have been shared through DMV records.³ The study reported that at least 26 states allow law enforcement to run or request searches of their driver's license and identification photos.

There are a myriad of problems associated with using facial recognition in these ways. The technology is often wrong—with government reports of high rates of “false positives” (wrongly matching two different individuals) and “false negatives” (wrongly failing to match the same individual). It is less accurate than fingerprinting, particularly when used in real-time or when collecting a large amount of data at one time. There is also a real risk that this technology could be used to stifle free speech given the history of FBI and police surveillance of civil rights protests. Mug shots, not driver's license or identification photos, should be the default databases for police searches, and photographs driver's licenses or ID cards should not be shared in a way that would allow them to be subject to these kinds of databases, over which there is very little public oversight and control.

(2) Correcting Errors in the AAMVA Pointer System

There was also a question about the process for correcting errors in the American Association of Motor Vehicle Administrators (AAMVA) state-to-state pointer system. Specifically, there was testimony before the committee that there is no procedure for correcting an error by AAMVA or its subcontractors. The AAMVA index is a system that records each driver's-license and identity-card holder's name, former names, gender, place of residence, date of birth, and last five digits of their social security number, type of credential (i.e., driver's license) and credential number. Alaska has been participating in this system since January 2017.

According to AAMVA's privacy impact assessment conducted on the pointer exchange system—which was confirmed by discussions from a representative from the ACLU national office with AAMVA—there is no real recourse within AAMVA if there is an error with the data within the index. “The accuracy of the [personally identifiable information] is the responsibility of the State that contributed the pointer. Each State has their own methods for checking the accuracy of the information AAMVA asserts no ownership of the information and cannot provide individuals direct access to their records.”⁴ Therefore, “[i]ndividuals contacting AAMVA directly with requests to correct their personal information in the SPEXS pointer index will be directed to the [state driver's license

³ Stephen Gaines & Sara Williams, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Oct. 18, 2016, available at www.perpetuallineup.org/.

⁴ American Assoc. of Motor Vehicle Administrators, *State Pointer Exchange Services, Privacy Impact Assessment* §§ 2.5, 8.1 at 4 & 15 (2016), available at papersplease.org/wp/wp-content/uploads/2016/06/SPEXS-PIA.pdf.

agency] that issued the credential in question.”⁵ Only if an individual is unable to resolve an error in the state’s data may the individual contact AAMVA, through their Privacy Officer. No information about AAMVA’s Privacy Officer could be located on AAMVA’s or Alaska DMV’s website, and it is unclear how an individual would be able to correct the record if he or she is not authorized to access it.⁶

(3) Other States’ Alternatives

Finally, we were asked about alternatives to compliance with REAL ID through the two-tiered system proposed by the Governor in HB 74. Several states are currently undergoing similar discussions. There are four states deemed “noncompliant,” while 18 states have extensions, and 8, including Alaska, have limited extensions.⁷ Although this is a rapidly changing environment, we have heard from some of our colleagues in other ACLU affiliate offices in other states about the current efforts with REAL ID compliance. In Minnesota, for example, a two-tiered identification system similar to the one proposed in HB 74 was introduced, but failed after being rejected by the Senate.⁸ There are currently no other bills introduced that would allow Minnesota to become compliant. In Maine, a two-tiered system has also been introduced, with a bill that would allocate some funds to assist individuals with obtaining passport cards.⁹ In Washington, a similar two-tiered system has been introduced, and the Attorney General of that state has promised to protect the state from any unconstitutional or illegal retaliation from the administration or executive agencies if a REAL ID compliant system is not implemented.

Sincerely,



Tara A. Rich
Legal & Policy Director

cc: Representative Chris Birch, Representative.Chris.Birch@akleg.gov
Representative DeLena Johnson, Representative.DeLena.Johnson@akleg.gov
Representative Andy Josephson, Representative.Andy.Josephson@akleg.gov
Representative Gary Knopp, Representative.Gary.Knopp@akleg.gov
Representative Chuck Kopp, Representative.Chuck.Kopp@akleg.gov
Representative Chris Tuck, Representative.Chris.Tuck@akleg.gov
Representative Adam Wool, Representative.Adam.Wool@akleg.gov

⁵ *Id.* § 8.2 at 15.

⁶ *Id.* § 8.1 at 15.

⁷ U.S. Department of Homeland Security, Current Status of States/Territories (last visited March 27, 2017), available at www.dhs.gov/current-status-states-territories.

⁸ John Lauritsen, *Minnesota Senate Votes Down REAL ID Bill*, WCCO CBS Minnesota, Mar. 6, 2017, available at minnesota.cbslocal.com/2017/03/06/minnesota-senate-real-id-vote/.

⁹ L.D. 213 (128th Legis. 2017).