JAMES DUFF LYALL
EXECUTIVE DIRECTOR

JIM MORSE
PRESIDENT

AMERICAN CIVIL LIBERTIES UNION OF VERMONT

P.O. BOX 277
MONTPELIER, VT 05601

802-223-3604
WWW.ACLUVT.ORG

May 23, 2017

Robert Ide
Commissioner
Department of Motor Vehicles
Vermont Agency of Transportation

Re: Vermont DMV's Unlawful Facial Recognition Program

Commissioner Ide:

It has come to the attention of the ACLU of Vermont ("ACLU-VT")[1] that the Vermont Department of Motor Vehicles ("DMV") is using facial recognition technology to search and share Vermonters' ID photos and other personal identifying information with a variety of "authorized entities," including an array of federal government agencies.[2]

DMV's use of this technology violates Vermont law 23 V.S.A. § 634(c), which bars DMV from "implement[ing] any procedures or processes for identifying applicants . . . that involve the use of biometric identifiers."[3] In addition, DMV's use of facial recognition technology at the request of "authorized entities" violates Vermonters' privacy and is subject to abuse. We write to demand an immediate suspension of DMV's facial recognition program.

Introduction

As a part of Act 154 of 2004, which required photo ID, 23 V.S.A. § 634(c) was adopted to address the threat to Vermonters' privacy rights posed by unchecked biometric surveillance. In fact, to assuage legislators concerns, DMV suggested § 634(c)'s

[1] Founded in 1967, the ACLU of Vermont is a nonpartisan, non-profit advocacy organization dedicated to defending the constitutional and civil rights of all Vermonters. With more than 7,500 members, ACLU-VT is the statewide affiliate of the national ACLU, which has a membership of over 1.6 million. The ACLU works to advance civil liberties through impact litigation, advocacy, and education.
[2] "Authorized entities" is not defined in the documents provided by DMV in response to the ACLU-VT's public records request.
[3] 23 V.S.A. § 634(c).

language, telling the House Transportation committee that it "would require legislative approval if [DMV] ever went to anything that looked like biometrics."[4] Since 2004, there is nothing in the legislative history or subsequent administrative record we reviewed indicating that DMV's FRS program is exempt from the requirements of that statute. To the contrary, the problems with DMV's program detailed herein demonstrate precisely why the Legislature was right to adopt the law in the first place.

Since 2004, state ID applicants must have their photograph taken and placed on their state-issued ID. DMV keeps each photograph and copies of applicant identity documents in its electronic database – the database now has over 2.6 million applicant photos.[5] Since December 17, 2012, the DMV uploads all photos and identity documents to DMV's database. Then, each night, facial recognition software ("FRS") analyzes, searches, and compares that day's applicants' faces to others already in the database. The FRS analysis, search, and comparison are done without notice to or consent from applicants. Despite the fact that the use of FRS conflicts with state law, that its effectiveness is questionable, and that there are ample alternative DMV resources dedicated to preventing fraud, officials have insisted the FRS program is necessary to address identity fraud.

But the FRS program has never been limited to fraud detection. According to documents obtained by the ACLU-VT, DMV regularly uses FRS at the request of external "authorized entities," a term not defined in the records we obtained. Specifically, external entities submit photographs or video stills of a person's face and request that they be analyzed and searched against DMV's photo database. DMV conducts the search and hands over Vermonters' photos and "any associated information stored with the photo[s]."[6] DMV records indicate the agency has responded to FRS search requests from the FBI, ICE, the U.S. State Department, and state and local police departments across the country, among many other agencies.

Further, when DMV responds to these requests, it provides photos and information of up to 50 different people whom the FRS selects as potential matches. Each person's photo and associated information in the photo "gallery" is then provided to the authorized entity without notice to or consent from the DMV applicants in the gallery.

---

[4] Testimony of Bonnie Rutledge, DMV Commissioner, to the Vermont House Committee on Transportation, January 30, 2004, LC689, CD Sheet PRA # LC676, Series 018, CD 040048.
[5] *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO Report to the Ranking Member, Subcommittee on Privacy, Technology and the Law, Committee on Judiciary, U.S. Senate, May 2016.
[6] "Associated information" is not defined in the documents provided by DMV in response to the ACLU-VT's public records request.

DMV performs FRS searches and shares Vermonters' photos and information without meaningful privacy protections. For instance, DMV does not require that a court order, probable cause, or even reasonable suspicion exist before turning over Vermonters' photos and information to external agencies. There does not appear to be any requirement that the subject person is even suspected of a crime. While you have previously stated that outside agencies would only receive applicant information if they met "stringent criteria,"[7] our analysis shows that in practice DMV rubberstamps requests without any such assessment. DMV's facial recognition search and share "criteria" lack substance and provide few, if any, protections for Vermonters' privacy.[8]

Additionally, these records indicate that DMV's facial recognition program disparately impacts racial and ethnic minorities, including migrant farmworkers and other immigrants. These groups are disproportionately targeted by search requests and research shows that these groups are more likely to be inaccurately identified by FRS. As such, they are even more likely to be caught up in unwarranted criminal investigations.[9] Moreover, the Trump administration has relaxed privacy protections for certain immigrant groups, including those on student or work visas, raising heightened concerns that DMV data on foreign document or driver privilege card ID holders provided to one federal agency will be shared with other federal agencies, such as ICE.

In addition to violating Vermont state law, raising serious privacy concerns, and disparately impacting people of color, DMV's facial recognition program lacks sufficient oversight, accountability measures, and data security practices to monitor a technology that poses significant risks for misuse, bias, and inaccuracy. For example, the only review of the program mentioned in DMV's records shows that FRS has resulted in the investigation of innocent people. In June 2013, DMV's director of enforcement wrote that after six months of FRS operation, 26 applicants were referred for fraud investigation, but nearly one third were exonerated.

Regarding data security, while the DMV claims to have constructed a highly secure applicant database, it relies on external agencies to securely store and purge shared applicant "gallery" photos and associated information. The records we received do not show evidence of an audit or review of the data security practices of external agencies before or after receiving Vermonters' personal information.

---

[7] *See* Charlotte Albright, New, Non-Mandatory Vt. Driver's License Will Be Available in January, VPR, Dec. 10, 2013, *available at* http://digital.vpr.net/post/new-non-mandatory-vt-drivers-license-will-be-available-january#stream/0.

[8] DMV records reviewed by the ACLU-VT indicate that all FRS search requests from external agencies were approved.

[9] *See* Clare Garvie, Alvaro Bedoya, & Jonathan Frankle, *The Perpetual Line-up: Unregulated Police Face Recognition in America*, Georgetown Center on Privacy & Technology, Oct. 18, 2016.

Finally, the DMV does not have any policies or procedures to ensure that the facial recognition program is not used to identify people exercising First Amendment freedoms. There is a significant potential that the facial recognition program will chill free speech or be used to retaliate against Vermonters protesting agencies that may submit FRS search requests. There is currently nothing to prevent FRS from being used to surveil religious, cultural, or political organizations.

For these reasons, we demand that you immediately discontinue the DMV's facial recognition program until its use is clearly authorized by law and in a manner that protects Vermonters' constitutional and civil rights.

Background

The ACLU-VT's concerns about DMV's facial recognition program are longstanding.[10] The program came to light in 2012, but has received scant attention. In October 2016, Georgetown Law's Center on Privacy and Technology published a national report showing that Vermont's DMV possesses millions of applicant photos, making them available to local, state, and federal agencies for facial recognition searching.[11]

On November 18, 2016, ACLU-VT sent a public records request to the DMV for all records referencing facial recognition software, systems, technologies, or operations. In response, over the course of six months, DMV provided ACLU-VT with records of facial recognition database search requests, policies and procedures, and various other documents related to the program. The following summary of DMV's facial recognition program is based on those records.

A. The creation of DMV's facial recognition program

Since 2004, Vermont statute 23 V.S.A. § 634(c) has banned the DMV from "implement[ing] any procedures or processes for identifying applicants for licenses, learner permits, or nondriver identification cards that involve the use of biometric identifiers."[12] The statute's intent was to guard against increased government surveillance, a national ID database, and other personal data-sharing that could result from Act 154's mandate that Vermonters obtain photo ID. As mentioned above, the DMV crafted and suggested § 634(c)'s language to assuage legislators'

---

[10] *See e.g.,* Ken Picard, Vermont DMV To Use Facial Recognition On All New Driver's License Photos and IDs, Seven Days, July 16, 2012, *available at* http://www.sevendaysvt.com/vermont/vermont-dmv-to-use-facial-recognition-software-on-all-new-drivers-license-photos-and-ids/Content?oid=2205087.

[11] *See* n. 9.

[12] 23 V.S.A. § 634(c)'s ban on biometric processes does not apply to commercial driver licenses pursuant to federal law 49 U.S.C. § 31308.

concerns that DMV would eventually use facial recognition technology on applicant photos.[13]

Notwithstanding § 634(c)'s clear prohibition against DMV using biometric processes and its intent to prevent the facial recognition scanning and sharing of applicant photos, in 2011, DMV submitted a U.S. Department of Homeland Security grant application to use over $900,000 in federal and state funds to procure and implement a facial recognition program.

Throughout DMV's grant application and reports, it states that facial recognition technology is for the purpose of "insuring [sic] that no individual is able to obtain more than one identification document (ID) or to obtain an ID with false information." According to DMV, FRS would enable DMV personnel "to perform high-volume screening of applicant images, reliably confirm applicants are who they claim to be, and provide effective pre- and post-issuance investigation tools."[14] DMV procured software from MorphoTrust, a defense technology contractor, and began utilizing FRS on December 17, 2012.

Nowhere in the legislative record we reviewed or in the documents provided to the ACLU of Vermont is there is any indication that DMV or other state officials addressed the conflict between DMV's implementation of a facial recognition program and 23 V.S.A. § 634(c)'s ban on DMV's use of biometrics.

B. Sharing Vermonters' photos and information with external federal, state, and local agencies

Despite DMV's federal grant reports and press statements claiming that FRS was only for the purpose of checking internal application fraud, upon the program's implementation, DMV wasted no time in immediately making its FRS available to outside law enforcement agencies. In Vermont Law Enforcement Bulletin #12-13 (12/26/2012), DMV's director of enforcement informed Vermont's law enforcement agencies that FRS was at their disposal, granting them unfettered discretion to submit photographs of any individual to be compared with those in the DMV database.

Shortly thereafter, on May 8, 2013, the DMV Commissioner signed a Memorandum of Understanding ("MOU") with the Federal Bureau of Investigation ("FBI").[15] The agreement allows the FBI to submit photos to DMV, requires DMV to do an FRS

---

[13] *See* n. 4.

[14] According to DMV records, FRS completes "biometric verification" of provided images or new DMV ID photos, comparing them to the ID photos already in the DMV database. The system "is capable of making billions of facial comparisons every night." DMV can compare "all applicant images captured on a given day against millions of stored images to quickly identify attempts at multiple identity fraud."

[15] Notably, the MOU requires Vermont DMV to "comply with its own state's privacy laws."

search of DMV's photo database, and requires that DMV provide the FBI with photos of "all possible candidates" with associated biographical information. After the information is sent to the FBI, the FBI manually analyzes, compares, and evaluates the "candidate gallery" to determine the "most-likely candidate(s)" and searches the candidate against the FBI's "Next Generation Identification Interstate Photo System" ("NGIIPS").[16]

Putting aside, for the moment, the apparent illegality of DMV's continued use of FRS, the lack of transparency in such a sophisticated surveillance program is striking. Simply put, DMV is using FRS to map and share Vermonters' faces and personal information, notwithstanding legal limits on its authority to do so and without meaningful rules or oversight, all without the knowledge or approval of impacted Vermonters.

Since December 17, 2012, DMV has run at least 126 FRS searches at the request of a variety of local, state, and federal agencies, and has shared the photos and "associated information" of potentially thousands of Vermonters with those agencies.[17] Externally-initiated FRS search requests reviewed by ACLU-VT cover a range of charges – everything from disorderly conduct and trespassing to murder. But, they also include requests where subject individuals are not charged with or even suspected of any crime. For example, in December 2016, DMV conducted an FRS search for the Vermont State Police based on an alleged "visa overstay," which is not a crime. In another instance, DMV conducted an FRS search at Vermont State Police's request for an individual believed to be involved in "suspicious circumstances," without any additional detail.

According to the records, DMV conducts similar searches at the request of multiple federal agencies. For example, in July 2016, DMV conducted an FRS search in response to an FBI-submitted photo based on nothing more than the FBI's assertion that the pictured person asked "unusual and suspicious" questions about firearms at a local Vermont gun shop. Another request from the U.S. Marshals sought an FRS search for an alleged fugitive's girlfriend based on her picture, without any allegation that the girlfriend was involved in criminal activity. Nonetheless, DMV conducted those searches and provided photos and associated information.

In 2016 and 2017, DMV also ran searches for and provided information to ICE and the Department of Homeland Security on at least five occasions. Vermont has statutorily committed to providing all driving-age residents the opportunity to

---

[16] For more information about NGIIPS, which the FBI calls "the world's largest and most efficient electronic repository of biometric and criminal history information," *see* https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi.

[17] While two FBI search requests forms were included in DMV records reviewed by the ACLU of Vermont, it is unclear whether the FBI is required to supply the standard FRS search request forms under the DMV-FBI MOU.

receive state ID, regardless of immigration status. In light of the State's policy and DMV's recent history of unlawful collaboration with federal immigration officials, the use of FRS on behalf of these agencies is especially troubling.[18]

DMV has also supplied Vermonters' photos and associated information to non-police regulatory enforcement agencies. For instance, DMV conducted a search and provided results to the Vermont Agency of Natural Resources ("ANR") based on an ANR allegation that the pictured individual was accused of AMP (acceptable management practices) violations related to logging. Similarly, at the request of the Missouri Department of Revenue, DMV conducted a database search regarding a tax fraud case and provided photos and information.

DMV's Unlawful and Unregulated Facial Recognition Program

A. The DMV's facial recognition program violates Vermont statute

Since 2004, Vermont law has banned the DMV from "implement[ing] any procedures or processes for identifying applicants . . . that involve the use of biometric identifiers."[19] The term "biometric" is defined as a type of "measurement and analysis of unique physical or behavior characteristics (as fingerprints or voice pattern)[,] especially as a means of verifying personal identity."[20] The FBI's NGIIPS website states that "the term 'biometrics' is not limited to fingerprints. It also includes palm prints, irises, and facial recognition."[21]

The DMV apparently agrees with the FBI's definition of "biometrics." In its grant reports, DMV repeatedly states that facial recognition provides "biometric verification" through a biometric process. And, in the MorphoTrust FRS Manual provided to DMV, entitled Biometric Identification System User Guide, "Biometric Identification" is defined as the MorphoTrust software that "provides automated screening of images (face and/or finger) captured during daily credential issuance."

Nevertheless, with apparent disregard for Vermont law, the DMV sought and used grant funds, instituted biometric processes, and provided unfettered database access to external agencies to do exactly what the law proscribes – use biometric identifiers to identify Vermont ID card holders when they apply for ID and when

---

[18] For the recent history of unlawful DMV collaboration with federal immigration officials, *see* Paul Heintz, Vermont DMV, State Police Play Nice With ICE, Seven Days, April 5, 2017, *available at* https://www.sevendaysvt.com/vermont/vermont-dmv-state-police-play-nice-with-ice/Content?oid=4953143; Elizabeth Hewitt, DMV Changing Application Process After Discrimination Case, VTDigger, Aug. 29, 2016, *available a*t https://vtdigger.org/2016/08/29/dmv-changing-application-process-discrimination-case/.

[19] 23 V.S.A. § 634(c).

[20] "Biometrics." *Merriam-Webster Online Dictionary* (2017), https://www.merriam-webster.com/disctionary/biometrics (last accessed May 5, 2017).

[21] *See* FBI NGIIPS website, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi.

requested by external agencies. After an extensive review of the legislative and documentary record, we can find no evidence that the legislature intended to exempt facial recognition technology from that requirement. In fact, the reviewed legislative history is entirely to the contrary, showing facial recognition identification as a primary consideration in adopting § 634(c)'s preventive bar to protect Vermonters' privacy. Because the DMV's use of FRS is unquestionably a "procedure[] or process[]" using biometrics to identify applicants, the program violates state law and must be discontinued immediately.

B. In addition to violating state law, DMV's facial recognition program raises privacy concerns and lacks oversight or other safeguards to prevent abuse

DMV's facial recognition program raises serious privacy concerns for two reasons. First, in order to receive state identification, DMV requires individuals to have their picture taken. When the photo is uploaded to the database and analyzed by FRS, it becomes much more than a picture – it becomes a "faceprint."[22] A "faceprint" is very similar to a fingerprint – both are biometric identifiers specific to each person that can be compared with others to determine identity. Of course, fingerprints can only be taken from a person through physical interaction. A faceprint can be compared with any other photograph taken with or without the individual ever knowing they are being subjected to identification. The DMV's failure to provide notice, allow an opportunity to consent or appeal FRS analysis and searching, or conform to any protective protocol or procedural requirements before accessing and sharing a person's "faceprint" violates basic privacy and due process norms.

Second, every time a database search is run, millions of "faceprints" are searched without any requirement of probable cause or reasonable suspicion that the pictured individuals have committed a crime. Unlike Vermont's fingerprint databases, which only include those individuals who have been arrested upon probable cause, or the state's DNA database of convicted felons,[23] DMV's faceprint database has no limitations. It operates as a general warrant to analyze and search a person's faceprint, and at nearly all times without probable cause or reasonable articulable suspicion that anyone has committed a crime.

---

[22] Kirill Levashov, *The Rise of a New Type of Surveillance For Which the Law Wasn't Ready*, Colum. Sci. & Tech. L. Rev., Fall, 2013, *available at* http://www.stlr.org/cite.cgi? volume=15&article=5.

[23] In 2014, the Vermont Supreme Court overturned the statutory requirements that forced all criminal defendants arraigned on certain qualifying charges to provide DNA samples to the State: "The marginal weight of the State's interest in DNA collection at the point of arraignment, balanced against the weight of the privacy interest retained by arraignees prior to conviction, persuades us to hold that 20 V.S.A. § 1933(a)(2), and associated sections, which expand the DNA-sample requirement to defendants charged with qualifying crimes for which probable cause is found, violate Chapter I, Article 11 of the Vermont Constitution." *See State v. Medina*, 197 Vt. 63, 95 (2014).The Court also noted that the Vermont Constitution holds persons themselves free from search, and therefore a person "does not forfeit [constitutional] protections with respect to offenses not charged absent either probable cause or reasonable suspicion." *Id.*

Furthermore, based on DMV's own documents, it is clear that there are few, if any, meaningful rules for searching the FRS photo database or providing information based on searches. DMV's FRS search request form explains that searches are for the purpose of "obtaining information that will advance active investigations, apprehend wanted fugitives or known or suspected terrorists, and locate missing persons." DMV also asks that external agencies provide a case number on the form. But, there is no evidence that those cases are ever reviewed, and even if they were, there is no way to know if the requestor is accurately portraying the justification for an FRS search. Regardless, DMV has apparently never denied a search request and regularly approves search requests without any evidence or even an assertion that the person in a submitted photograph has committed a crime. The lack of procedural safeguards means that any person with a Vermont ID could be the subject of an FRS database search with or without any law enforcement justification or evidence, and never know about it.

Aside from the DMV program's significant privacy implications and lack of meaningful safeguards or guidelines, there are substantial problems associated with FRS technology—including its fundamental inaccuracy. For instance, according to an Institute of Electrical and Electronics Engineers 2012 study, the FBI's facial recognition software, also created by MorphoTrust, has a 14% error rate for a dataset of 1 million photographs (and the software is 5-10% less accurate for African-Americans, women, and adults 18-30 years old).[24] The software's inaccuracy is compounded by the inherent variability in the quality of photos submitted for comparison, the enormous number of individuals' photos in a database, and common errors in human evaluation of gallery photos.

Such errors have caused significant harm to law-abiding individuals. Steve Talley, a Denver native, was twice arrested, jailed, and injured by police based on an FBI facial examiner's erroneous belief that his photo matched video stills taken from a bank robbery.[25] And, because such mistakes require the subject individuals to prove they are not the person pictured, facial recognition, in effect, turns our system of justice on its head by forcing defendants to prove their innocence.

In addition, there is a significant potential that this system will be abused. According to an Associated Press review, between 2013 and 2015, hundreds of officers across the nation have been disciplined for accessing government databases to obtain information about individuals for improper and personal reasons.[26]

---

[24] *See* n. 9.

[25] Ava Kofman, Losing Face: How a Facial Recognition Mismatch Can Ruin Your Life, The Intercept, Oct. 13, 2016, *available at* https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/.

[26] Sadie Gurman & Eric Rucker, Across US, Police Officers Abuse Confidential Databases, Associated Press, Sept. 28, 2016, *available at*

Despite these shortcomings and risks, facial recognition systems at the local and federal level have never been subject to even the most basic oversight measures. In 2016, the U.S. Government Accountability Office ("GAO") noted that the FBI has never reviewed its facial recognition data collection and investigation program, which has access to 411 million "faceprints," for misuse, abuse, or accuracy.[27] The GAO also criticized the FBI for utilizing state-based databases that have never been audited for accuracy or validity. Nevertheless, the FBI specifically refused to implement some of the GAO's recommendations. Until a formal audit of data security practices is initiated and completed by DMV, as well as external federal and state agencies seeking to search DMV's FRS database, sharing Vermonters' sensitive personal information puts Vermonters' privacy and identities at risk.

C. DMV's FRS searches disparately impact people of color

Vermont DMV's FRS searches on behalf of external agencies disproportionately involved African-Americans and Hispanics. Searches for African-Americans occurred 7 times more frequently, and searches for Hispanics were nearly 12 times more frequent, than would be expected based on their respective percentages of the Vermont driving population. Whites were searched for half as frequently as would be expected. The following chart represents information from DMV FRS search request forms:

Racial Disparities in DMV's Facial Recognition Searches				
Race/Ethnicity	# of Search Forms	% of Search Forms	% of Vermont Driving Population	Disparity Index – DMV Data
Asian	2	1.6%	2.2%	72%
African-American	16	12.7%	1.8%	705%
Hispanic	9	7.1%	.6%	1183%
White	55	43.7%	95.2%	46%
Race/Ethnicity Not Provided	44	35%	N/A	N/A

http://bigstory.ap.org/article/699236946e3140659fff8a2362e16f43/ap-across-us-police-officers-abuse-confidential-databases.

[27] *See* n. 5.

Similar racial disparities have been consistently documented in other parts of Vermont's criminal justice system, including police stops and searches and incarceration rates.[28] DMV's active participation in the disproportionate targeting of people of color is yet another example of institutional racial bias in Vermont that must be addressed.

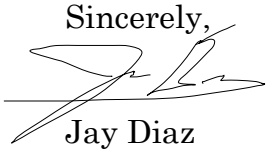
Conclusion

DMV's use of FRS violates state law. It also raises serious privacy concerns, is subject to abuse, disparately impacts Vermont's communities of color, and puts immigrant communities and First Amendment freedoms at greater risk. Even leaving aside these serious dangers, facial recognition technology's fundamental flaws and lack of safeguards undermine any justifications for its continued use.

For all of the foregoing reasons, the ACLU demands an immediate suspension of the FRS program until its use is clearly authorized by law and in a manner that protects Vermonters' constitutional and civil rights.

Please do not hesitate to contact me at jdiaz@acluvt.org or 802-223-6304 ext. 113.

Sincerely,



Jay Diaz
Staff Attorney
ACLU of Vermont

Cc: Joe Flynn, Vermont Secretary of Transportation; T.J. Donovan, Vermont Attorney General

[28] *See* Nancy Brooks & Stephanie Seguino, *Driving While Black and Brown in Vermont*, Jan. 9, 2017; Robin Weber, *Race and Sentencing in Vermont*, Report to the Vermont Legislature and Vermont Commission on Human Rights, Oct. 2015; Marc Mauer & Ryan King, *Uneven Justice: State Rates of Incarceration by Race and Ethnicity*, Sentencing Project, July 1, 2017.