http://www.caliberties.org/

California Civil Liberties Association
25 Cadillac Dr, Ste 107
Sacramento, CA 95825
(916) 426-9338

Problems with Law Enforcement Face Recognition Technology

Face recognition is becoming a problem in California and elsewhere. Technology provided by NeoFace is capable of performing over 1,500,000 searches a day.[i] According to documents provided in a California Public Records Act request, the California Department of Justice (CADOJ) spent over $2 million to purchase and implement facial recognition technology provided by NeoFace in 2016.[ii] While these public records requests reveal the type of equipment purchased and the amounts, we do not know exactly how that technology is being implemented by CADOJ; for instance, whether it is being used to track suspects in criminal investigations, or if it is being used to monitor the public at large. Toward the end of 2016, a 151-page study called *The Perpetual Line-Up* was published by the Center on Privacy & Technology at Georgetown Law, highlighting the growing problem with facial recognition technology along with recommendations for Congress and state legislatures. The following is an excerpt from that study intended to serve as a basis for a dialogue with the California State Legislature on how to address these problems in our state[iii]:

One in two American adults is in a law enforcement face recognition network.

. . . .

A. KEY FINDINGS

Our general findings are set forth below. Specific findings for 25 local and state law enforcement agencies can be found in our Face Recognition Scorecard, which evaluates these agencies' impact on privacy, civil liberties, civil rights, transparency and accountability. The records underlying all of our conclusions are available online.

- **Law enforcement face recognition networks include over 117 million American adults.**

Face recognition is neither new nor rare. FBI face recognition searches are more common than federal court-ordered wiretaps. At least one out of four state or local police departments has the option to run face recognition searches through their or another agency's system. At least 26 states (and potentially as many as 30) allow law enforcement to run or request searches against their databases of driver's license and ID photos. Roughly one in two American adults has their photos searched this way.

- **Different uses of face recognition create different risks. This report offers a framework to tell them apart.**

A face recognition search conducted in the field to verify the identity of someone who has been legally stopped or arrested is different, in principle and effect, than an

investigatory search of an ATM photo against a driver's license database, or continuous, real-time scans of people walking by a surveillance camera. The former is targeted and public. The latter are generalized and invisible. While some agencies, like the San Diego Association of Governments, limit themselves to more targeted use of the technology, others are embracing high and very high risk deployments.

- **By tapping into driver's license databases, the FBI is using biometrics in a way it's never done before.**

Historically, FBI fingerprint and DNA databases have been primarily or exclusively made up of information from criminal arrests or investigations. By running face recognition searches against 16 states' driver's license photo databases, the FBI has built a biometric network that primarily includes law-abiding Americans. This is unprecedented and highly problematic.

- **Major police departments are exploring face recognition on live surveillance video.**

Major police departments are exploring real-time face recognition on live surveillance camera video. Real-time face recognition lets police continuously scan the faces of pedestrians walking by a street surveillance camera. It may seem like science fiction. It is real. Contract documents and agency statements show that at least five major police departments—including agencies in Chicago, Dallas, and Los Angeles—either claimed to run real-time face recognition off of street cameras, bought technology that can do so, or expressed a written interest in buying it. Nearly all major face recognition companies offer real-time software.

- **Law enforcement face recognition is unregulated and in many instances out of control.**

No state has passed a law comprehensively regulating police face recognition. We are not aware of any agency that requires warrants for searches or limits them to serious crimes. This has consequences. The Maricopa County Sheriff's Office enrolled all of Honduras' driver's licenses and mug shots into its database. The Pinellas County Sheriff's Office system runs 8,000 monthly searches on the faces of seven million Florida drivers—without requiring that officers have even a reasonable suspicion before running a search. The county public defender reports that the Sheriff's Office has never disclosed the use of face recognition in Brady evidence.

- **Law enforcement agencies are not taking adequate steps to protect free speech.**

There is a real risk that police face recognition will be used to stifle free speech. There is also a history of FBI and police surveillance of civil rights protests. Of the 52 agencies that we found to use (or have used) face recognition, we found only one, the Ohio Bureau of Criminal Investigation, whose face recognition use policy expressly prohibits its

officers from using face recognition to track individuals engaging in political, religious, or other protected free speech.

- **Most law enforcement agencies do little to ensure their systems are accurate.**

Face recognition is less accurate than fingerprinting, particularly when used in real-time or on large databases. Yet we found only two agencies, the San Francisco Police Department and the Seattle region's South Sound 911, that conditioned purchase of the technology on accuracy tests or thresholds. There is a need for testing. One major face recognition company, FaceFirst, publicly advertises a 95% accuracy rate but disclaims liability for failing to meet that threshold in contracts with the San Diego Association of Governments. Unfortunately, independent accuracy tests are voluntary and infrequent.

- **The human backstop to accuracy is non-standardized and overstated.**

Companies and police departments largely rely on police officers to decide whether a candidate photo is in fact a match. Yet a recent study showed that, without specialized training, human users make the wrong decision about a match half the time. We found only eight face recognition systems where specialized personnel reviewed and narrowed down potential matches. The training regime for examiners remains a work in progress.

- **Police face recognition will disproportionately affect African Americans.**

Police face recognition will disproportionately affect African Americans. Many police departments do not realize that. In a Frequently Asked Questions document, the Seattle Police Department says that its face recognition system "does not see race." Yet an FBI co-authored study suggests that face recognition may be less accurate on black people. Also, due to disproportionately high arrest rates, systems that rely on mug shot databases likely include a disproportionate number of African Americans. Despite these findings, there is no independent testing regime for racially biased error rates. In interviews, two major face recognition companies admitted that they did not run these tests internally, either.

Face recognition may be least accurate for those it is most likely to affect: African Americans.

- **Agencies are keeping critical information from the public.**

Ohio's face recognition system remained almost entirely unknown to the public for five years. The New York Police Department acknowledges using face recognition; press reports suggest it has an advanced system. Yet NYPD denied our records request entirely. The Los Angeles Police Department has repeatedly announced new face recognition initiatives—including a "smart car" equipped with face recognition and real-time face recognition cameras—yet the agency claimed to have "no records responsive" to our document request. Of 52 agencies, only four (less than 10%) have a publicly available use policy. And only one agency, the San Diego Association of Governments, received legislative approval for its policy.

- **Major face recognition systems are not audited for misuse.**

Maryland's system, which includes the license photos of over two million residents, was launched in 2011. It has never been audited. The Pinellas County Sheriff's Office system is almost 15 years old and may be the most frequently used system in the country. When asked if his office audits searches for misuse, Sheriff Bob Gualtieri replied, "No, not really." Despite assurances to Congress, the FBI has not audited use of its face recognition system, either. Only nine of 52 agencies (17%) indicated that they log and audit their officers' face recognition searches for improper use. Of those, only one agency, the Michigan State Police, provided documentation showing that their audit regime was actually functional.

B. RECOMMENDATIONS

- **Legislators should pass laws to regulate law enforcement face recognition.**

Such laws should require the FBI or the police to have a reasonable suspicion of criminal conduct prior to a face recognition search. After-the-fact investigative searches—which are invisible to the public—should be limited to felonies.

Mug shots, not driver's license and ID photos, should be the default photo databases for face recognition, and they should be periodically scrubbed to eliminate the innocent. Except for identity theft and fraud cases, searches of license and ID photos should require a court order issued upon a showing of probable cause, and should be restricted to identity theft and serious crimes. If these searches are allowed, the public should be notified at their department of motor vehicles.

If deployed pervasively on surveillance video or police-worn body cameras, real-time face recognition will redefine the nature of public spaces. At the moment, it is also inaccurate. Communities should carefully weigh whether to allow real-time face recognition. If they do, it should be used as a last resort to intervene in only life-threatening emergencies. Orders allowing it should require probable cause, specify where continuous scanning will occur, and cap the length of time it may be used.

- **Real-time face recognition will redefine the nature of public spaces. It should be strictly limited.**

Use of face recognition to track people on the basis of their political or religious beliefs or their race or ethnicity should be banned. All face recognition use should be subject to public reporting and internal audits.

To lay the groundwork for future improvements in face recognition, Congress should provide funding to NIST to increase the frequency of accuracy tests, create standardized, independent testing for racially biased error rates, and create photo databases that facilitate such tests.

State and federal financial assistance for police face recognition systems should be contingent on public reporting, accuracy and bias tests, legislative approval—and public posting—of a face recognition use policy, and other standards in line with these recommendations.

. . . .

- **Police face recognition use should be transparent and publicly accountable.**

Many police departments have run searches of driver's license and ID photos without express legislative approval. Police should observe a moratorium on those searches until legislatures vote on whether or not to allow them.

Police should develop use policies for face recognition, publicly post those policies, and seek approval for them from city councils or other local legislative bodies. City councils should involve their communities in deliberations regarding support for this technology, and consult with privacy and civil liberties organizations in reviewing proposed use policies.

When buying software and hardware, police departments should condition purchase on accuracy and bias tests and periodic tests of the systems in operational conditions over the contract period. They should avoid sole source contracts and contracts that disclaim vendor responsibility for accuracy.

All agencies should implement audits to prevent and identify misuse and a system of trained face examiners to maximize accuracy. Regardless of their approach to contracting, all agencies should regularly test their systems for accuracy and bias.

For more information on the work that CCLA is doing to address this matter in California, please contact us at (916) 426-9338, or email us at ccla@caliberty.net.

[i] https://motherboard.vice.com/en_us/article/kbvkg3/california-spent-nearly-dollar18-million-on-controversial-facial-recognition-software <Accessed October 16, 2017>.

[ii] https://www.muckrock.com/news/archives/2017/apr/27/california-doj-facial-recognition/ <Accessed October 21, 2017>.

[iii] Georgetown Law, Center on Privacy & Technology, The Perpetual Line-Up—Unregulated Police Face Recognition in America (October 18, 2016) 2-4.