RESOLUTION 15-01-2017 (REVISED)

DIGEST

Law Enforcement: Limiting the Use of Facial Recognition Technology

Adds Penal Code sections 639, 639.01, 640, 640.01, 640.02, 640.03, 640.04, 640.05, 640.06, 640.07, 640.08, 641, and 641.01 to limit use of facial recognition technology by law enforcement.

RESOLUTIONS COMMITTEE ANALYSIS

History:

Similar to Resolution 11-01-2014, which was approved in principle.

Reasons:

This resolution adds Penal Code sections 639, 639.01, 640, 640.01, 640.02, 640.03, 640.04, 640.05, 640.06, 640.07, 640.08, 641, and 641.01 to limit use of facial recognition technology by law enforcement.

This resolution would bar law enforcement from using facial recognition technology, except to identify a person who has committed or is about to commit a felony or a criminal suspect that an officer has personally encountered. It would also prohibit law enforcement's use of facial recognition technology in conjunction with DMV photos and surveillance camera images, limiting any such search to arrest photo databases only and requiring photos of suspects who are not convicted to be purged.

This resolution is related to S.B. No. 21 (Hill), which is based on Resolution 11-01-2014, and is currently pending in the Assembly. Senate Bill 21 would require local law enforcement agencies to obtain permission from their local governing body, before obtaining any surveillance technology.

The Resolutions Committee initially recommended disapproval of this resolution. The full Conference voted to approve.

TEXT OF RESOLUTION

RESOLVED that the Conference of California Bar Associations recommends that legislation be sponsored to add Penal Code sections 639, 639.01, 640, 640.01, 640.02, 640.03, 640.04, 640.05, 640.06, 640.07, 640.08, 641, 641.01 to read as follows:

§ 639

Sections 639 through 641 shall be known and may be cited as the "Face Recognition Act of 2017 (FACE OFF)"

§ 639.01

Definitions. As used in this Act—

(a) "Face recognition" means the automated or semi-automated process by which a

person is identified or attempted to be identified based on the characteristics of his or her face.

(b) "Targeted face recognition" means the use of face recognition to identify or attempt to identify a specific person as part of a specific criminal investigation

(c) "Continuous face recognition" means the use of face recognition to identify or attempt to identify groups of persons as part of a criminal investigation or general surveillance, including the use of face recognition to continuously identify persons whose images are captured or recorded by a surveillance camera.

(d) "Arrest photo database" means a database populated primarily by booking or arrest photographs or photographs of persons encountered by investigative or law enforcement officers.

(e) "California identification photo database" means a database populated primarily by photos from driver's licenses or identification documents made or issued by or under the authority of the State, or a political subdivision of the State.

(f) "State investigative or law enforcement officer" means any officer of the State or a political subdivision the State who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in the State criminal code, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.

§ 640

Use of Face Recognition by Law Enforcement

§ 640.01

Targeted Face Recognition.

(a) Arrest photo databases.—

(1) General. A state investigative or law enforcement officer shall not use or request targeted face recognition in conjunction with an arrest photo database except as provided in this paragraph 2 below.

(2) Permitted uses. A state investigative or law enforcement officer may use or request targeted face recognition in conjunction with an arrest photo database maintained pursuant to paragraph (3) (A)To identify any individual whom the officer encounters in person under circumstances which provide the officer a reasonable suspicion that the person has committed, is committing or is about to commit a criminal offense;

(B) To identify any individual whom the officer reasonably suspects has committed, is committing or is about to commit an offense punishable by imprisonment for more than one year.

(4) Any custodian of an arrest photo database used by or at the request of an investigative or law enforcement officer in conjunction with targeted face recognition shall, every six months, eliminate from that database photos of persons—

(A) Released without a charge;

(B) Released after charges are dropped or dismissed or a nolle prosequi notice is entered; or

(C) Not convicted of the charged offense.

(b) Identification Photo Databases.—Any investigative or law enforcement officer, state or federal, shall not use targeted face recognition in conjunction with a state identification photo database, or acquire in bulk the photos in that database.

§ 640.02

Continuous Face Recognition - A state investigative or law enforcement officer shall not use continuous face recognition within the State.

§ 640.03

Civil Rights and Civil Liberties - A state investigative or law enforcement officer shall not—

(a) use face recognition to create a record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual for whom the record is created or unless pertinent to and within the scope of an authorized law enforcement activity where there is reasonable suspicion to believe the individual has engaged, is engaging, or is about to engage in criminal activity; or

(b) rely on actual or perceived race, ethnicity, national origin, religion, disability, gender, gender identity, or sexual orientation in selecting which person to subject to face recognition, except when there is reasonable suspicion, relevant to the locality and timeframe, that links a person with a particular characteristic described in this subsection to an identified criminal incident or scheme.

§ 640.04

Logging of Searches. A state law enforcement agency whose investigative or law enforcement officers use targeted or continuous face recognition shall log its use of the technology to the extent necessary to comply with the public reporting and audit requirements of sections 640.05 and 640.06 of this Act.

§ 640.05

Public Reporting.

(a) In March of each year, the principal prosecuting attorney for the State, or the principal prosecuting attorney for any political subdivision of the State, shall report to the chief judge of the highest court of the State, with respect to the preceding calendar year—

(1) For the use targeted face recognition in conjunction with an arrest photo database—

(A) the number of such searches run;

(B) the offenses that those searches were used to investigate, and for each offense, the number of searches run;

(C) the arrests that resulted from such searches, and the offenses for which arrests were made;

(D) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained; and

(E) the number of motions to suppress made with respect to those searches, and the number granted or denied.

(2) In June of each year the chief judge of the highest court of the State shall release to the public, post online, and transmit to the State Legislature a full and complete report concerning the use of targeted face recognition in conjunction with arrest photo databases. A summary and analysis of the data required to be filed with the chief judge of the highest court of the State by subsection (a) of this section and sections 640.06 and subsection (b) of 640.07 of this Act.

(b) The chief judge of the highest court of the State is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsection (a)

of this section and section 640.06 and subsection (b) of 640.07 of this Act.

§ 640.06

Audits. Any state law enforcement agency whose state investigative or law enforcement officers use targeted face recognition, regardless of whether they use a system operated by that agency or another agency, shall annually audit that use to prevent and identify misuse and to ensure compliance with sections 640.01, 640.02, and 640.03 of this Act, and shall report—

(a) summary of the findings of the audit, including the number and nature of violations identified, to the chief judge of the highest court of the State, and subsequently release that information to the public and post it online; and

(b) any violations identified to the principal prosecuting attorney for the state.

§ 640.07

Accuracy and Bias Testing.

(a) Any state law enforcement agency whose state investigative or law enforcement officers operate a system of targeted face recognition shall regularly submit that system to independent testing to determine—

(1) the accuracy of the system; and

(2) whether the accuracy of the system varies significantly on the basis of race, ethnicity, gender or age.

(b) A summary of the findings of the tests required by subsection (a) shall be submitted to the chief judge of the highest court of the state, released to the public, and posted online.

§ 640.08

Enforcement.

(a) Suppression. Whenever targeted or continuous face recognition has occurred, no results from those searches and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the use of face recognition violated sections 640.01, 640.02 or 640.03 of this Act.

(b) Administrative Discipline. If a court or law enforcement agency determines that an investigative or law enforcement officer has violated any provision of this Act, and the court or agency finds that the circumstances surrounding the violation raise serious questions about whether or not the officer acted willfully or intentionally with respect to the violation, the agency shall promptly initiate a proceeding to determine whether disciplinary action against the officer is warranted.

(c) Civil Action.

(1) In General. Any person who is subject to targeted identification or attempted identification through targeted continuous face recognition in violation of this Act may in a civil action recover from the state investigative or law enforcement officer or the state or enforcement agency which engaged in that violation such relief as may be appropriate.

(2) Relief. In an action under this subsection, appropriate relief includes—

(A) such preliminary and other equitable or declaratory relief as may be appropriate;

(B) damages under subparagraph (2) and punitive damages in appropriate cases; and

(C) a reasonable attorney's fee and other litigation costs reasonably incurred.

(3) Computation of Damages. The court may assess as damages whichever is the greater of—

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $500 a day for each day of violation or $50,000;

(1) Limitation. A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

§ 641

Funding for Law Enforcement Face Recognition Systems and Research

§ 641.01

Law Enforcement.

(a) No state financial assistance or funds may be expended for the creation, maintenance, or modification of a law enforcement face recognition system unless the agency operating that system—

(1) certifies compliance with sections 640.04, 640.05, 640.06 and 640.07 of this Act;

(2) certifies that the algorithm employed by its face recognition system has been submitted for testing in the most recent Face Recognition Vendor Test administered by the National Institute of Standards and Technology;

(3) provides documentation to confirm that the agency has released to the public and posted online a use policy governing its use of face recognition and, in the case of a law enforcement agency serving a subdivision of a State, has secured approval for that policy from a city council or other body primarily comprised of elected officials.

(b) Subsection (a) shall take effect 18 months after the enactment of this Act, except for paragraph (2) of that subsection, which shall take effect five years after enactment.

(Proposed new language underlined; language to be deleted stricken)

PROPONENT: Bay Area Lawyers for Individual Freedom

STATEMENT OF REASONS

The Problem: The use of facial recognition databases by law enforcement has grown rapidly in recent years, usually conducted with minimal legal oversight beyond the requirement that searches are conducted for "law enforcement purposes." A study conducted by the University of Georgetown, *The Perpetual Line-Up: Unregulated Police Face Recognition in America,* found that half of all American adults are in a police face recognition database. Sixty-four million of these adults are law abiding citizens, who are in the database solely because they obtained a driver's license. As a result of their desire to drive a vehicle, they have now unknowingly and involuntarily become regular participants in repetitive, virtual perp walks where their faces are scanned against an unknown subject's face for a possible match. This technology allows law enforcement to compile, in effect, digital dossiers on people's actions and movements throughout creating a huge risk to personal privacy. Despite this, to date, no state has passed a law

comprehensively regulating police face recognition.

There is a real risk that police face recognition will be used to stifle free speech and lead to a society based on self-censorship. Moreover, deployment of technology that transmits facial recognition data in real-time will transform the nature of public spaces. Shockingly, Georgetown University's study found that only one law enforcement agency in the entire country expressly prohibits its officers from using facial recognition to track individuals engaging in political, religious, or other protected free speech. In April of 2016, the Baltimore Police Department used facial recognition technology to locate, identify and arrest certain people protesting Freddie Gray's death in police custody. The ability for law enforcement officers to use facial recognition technology to generate a precise, comprehensive record of a person's public movements that reflects a wealth of detail about his or her familial, political, professional, religious, and sexual associations is massively concerning. Even the most modest imagination can conjure indisputably private aspects of an individual's intrinsic nature that may be disclosed via the use of facial recognition technology: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.

As noted in the Georgetown University study, law enforcement agencies do little to ensure that the facial recognition systems they employ are accurate. "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." In fact, facial recognition technology is likely to be less accurate, but most impactful on the African American community. A study co-authored by the FBI, found that facial recognition technology may be less accurate on African Americans. Also, because the African American community is subject to disproportionately high arrest rates, members of that community will be more affected than other populations by facial recognition systems that rely on mug shot databases. Despite these findings, racially biased error rates have not been independently tested. In fact, several major providers of face recognition technology have admitted that they failed to run test on their technology, even internally, for racial biases.

The law enforcement agencies that use facial recognition technology rarely, if ever, audit the use of the technology for misuse or abuse. Police officers across the country misuse confidential law enforcement databases to get information on romantic partners, business associates, neighbors, journalists and others for reasons that have nothing to do with daily police work, an Associated Press investigation found. Through records requests to state agencies and big-city police departments, the Associated Press found that law enforcement officers and employees who misused databases were fired, suspended or resigned more than 325 times between 2013 and 2015. They received reprimands, counseling or lesser discipline in more than 250 instances, the review found. Among those punished: an Ohio officer who pleaded guilty to stalking an ex-girlfriend and who looked up information on her; a Michigan officer who looked up home addresses of women he found attractive; and two Miami-Dade officers who ran checks on a journalist after he aired unflattering stories about the department. It's not difficult to imagine how facial recognition technology could easily be abused by a rogue law enforcement officer to locate a victim of domestic violence attempting to hide from her abuser or as blackmail in an attempt to stifle our free press.

The Solution: This resolution would limit the use of facial recognition technology by law enforcement and require certain audits and reports to monitor how the technology is being used by law enforcement agencies.

IMPACT STATEMENT
The resolution does not affect any other law, statute or rule other than those expressly identified.

CURRENT OR PRIOR RELATED LEGISLATION
None known.

AUTHOR AND/OR PERMANENT CONTACT: Meaghan Zore, 391 Sutter Street, Suite 207 - San Francisco, CA 94108, voice: (415) 347-0004, email: mmzore@gmail.com

RESPONSIBLE FLOOR DELEGATE: Meaghan Zore