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

http://www.caliberties.org/

California Facial Identification and Surveillance Privacy Act of 2018 (CalFISPA)

A Bill Proposal to the California State Legislature
Regular Session 2017-2018

MISSION

The California Civil Liberties Advocacy (CCLA) is a statewide 501(c)(4) nonprofit lobby with the goal of protecting individual rights in California. The CCLA does not peddle a national agenda and only takes a stand on national issues as they relate to California's specific needs and policies. For the 2017-2018 session, the CCLA is actively promoting legislation to enhance protections from suspicionless, dragnet, mass surveillance. The CCLA rejects the zero-sum fallacy that implementing policies that enhance civil liberties constitute a total loss for law enforcement, or that the passage of a bill enhancing law enforcement constitutes a total loss for civil liberties. Thus, the bill language that follows has been drafted in attempt to balance the needs of the people with the tools necessary for law enforcement to achieve their goals.

INTRODUCTION

The purpose of this bill proposal is to address the impending, monolithic imposition upon individual privacy and the potential for government abuses of facial recognition technology. Much of the language was patterned after model legislation provided by the Georgetown Law Center on Privacy & Technology. Section 1 establishes the title of the bill — the "California Facial Identification and Surveillance Privacy Act of 2018," definition of the terms used throughout, and permitted and prohibited law enforcement uses, along with exceptions. Section 2 establishes protections for civil rights and civil liberties protected under the United States and California Constitutions. Section 3 establishes procedures for disciplinary action and civil remedies for anyone harmed by an abuse or misuse of facial recognition technology and data.

NEED FOR STATE LEGISLATION

The CCLA first began monitoring government use of facial recognition technology in 2014. Based on our technology expert's assessment, our board of directors determined that the implementation of such technology as a threat to civil liberties was a medium risk due to the fact that the technology did not yet appear to be in widespread use. The board voted to continue monitoring the issue and take action when and if the technology became adopted by more law enforcement agencies throughout California. At the time, the board reached a consensus that widespread adoption of the technology was likely a half-decade or more away. By the end of 2016, the matter was reintroduced to the organization's Legislative Committee due to more stories popping up in the media regarding not only its use by law enforcement, but tech sector's strides in developing the technology. After examining the evidence, the Committee made a full recommendation to the directors that the CCLA begin working on a proposal to the California State Legislature.

KEY FINDINGS

- Facial recognition technology currently appears to be unregulated by California law.
- California state and local law enforcement use a shared database known as "Cal-Photo" to search for arrest records, sex offender registration, and DMV profiles.[i]

- Though not adopted due to public outcry, the California Law Enforcement Telecommunications System (CLETS) Advisory Committee (CAC) considered the expansion of "Cal-Photo's capability to share photos on a **national basis**; and, deploy facial recognition as an investigative tool."[ii]

- The United States Government Accountability Office found that the FBI failed to adhere to privacy laws and policies and had not even taken any action to ensure the accuracy of their face recognition technology.[iii]

- 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. The CCLA was unable to locate a policy on the use of the equipment.[iv]

- Law enforcement face recognition will disproportionately affect African Americans and will be less accurate when profiling African Americans.[v]

- Facial recognition presents a threat to other minority groups, especially the **LGBTQ** community.[vi]

- Facial recognition technology has the potential to reveal political views.[vii]

- Surveillance cameras used by law enforcement, in conjunction with facial recognition, could chill activities protected by the First Amendment, such as the right to peacefully assemble and protest.[viii]

- It is likely that face recognition technology and corresponding photo databases will be utilized by law enforcement agencies against undocumented immigrants and their families.[ix] [x]

CONCLUSION

The simple fact of the matter is that it typically takes years or decades for public policy to catch up with societal changes. But the vast changes in technology that we are now experiencing are causing broad and sweeping changes that are outpacing the evolution of public policy. This is similar to the challenges following the invention of the railroad in the 19th century. At a minimum, the regulations set forth in the following model language must be implemented before procedures and practices become so ingrained in corporate and government bureaucracy that it is too costly or difficult to amend at a later date.

PROPOSED LEGISLATION

BILL SUMMARY

Section One establishes when an officer can and cannot use face recognition in coordination with a court order, under probable cause, and states when any such information shall be destroyed. Exceptions include use in conjunction with emergency watchlists, arrest photo databases, and identification photo databases.

Section Two establishes protections for free speech activities and creates a tort for misuse, including targeting face recognition based on race, ethnicity, national origin, religion, disability, sex, sexual orientation, gender, or gender identity.

Section Three provides remedies for the misuse and mis-acquisition of data as evidence; any such violation shall warrant an investigation. Section Three further allocates civil relief for victims.

BILL LANGUAGE

SECTION 1. (Facial Scan Identifiers) Section _____ is added to the Penal Code, to read:

_____

(a) This section may be referred to as the "California Facial Identification and Surveillance Privacy Act of 2018."

(b) For the purpose of this section, the following definitions apply:

(1) "Facial scan identification" means the automated or semi-automated process by which an individual is identified or attempted to be identified based on the individual characteristics of his or her face.

(2) "Targeted facial scan identification" means the use of face recognition to identify or attempt to identify a specific person as part of a specific criminal investigation.

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

(4) "Arrest photo database" means a database populated primarily by booking or arrest photographs or photographs or individuals encountered by law enforcement officers.

(5) "Person" means a natural person.

(6) "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 of California, or a political subdivision thereof.

(7) "Emergency watchlist" means a highly targeted database populated by a specific individual or groups of individuals who there is probable cause to believe have committed, are in the process of committing, or are about to commit a criminal offense.

(8) "Law enforcement agency" means the Attorney General of the State of California, every district attorney, and every agency of the State of California expressly authorized by statute to investigate or prosecute law violators.

(9) "Law enforcement officer" means any officer of the State of California or a political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses as defined in the Penal Code, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.

(c) A law enforcement agency or a law enforcement officer shall not use or request targeted facial scan identification in conjunction with an arrest photo database except as provided in subdivision (d).

(d) A law enforcement agency or a law enforcement officer may use or request targeted facial scan identification in conjunction with an arrest photo database maintained pursuant to subdivision (e).

(1) To identify any person whom the officer personally encounters under circumstances which provide the officer a reasonable suspicion that the person or persons have committed, are in the process of committing, or are about to commit a criminal offense.

(2) To identify any person or persons whom the officer reasonably suspects have committed, are in the process of committing, or are about to commit a criminal offense punishable by imprisonment for more than one year.

(e) Within one year, any custodian of an arrest photo database used by or at the request of a law enforcement agency or a law enforcement officer in conjunction with targeted facial scan identification shall remove from that database photos of persons who meet the following criteria:

(1) The person was released from custody and was never charged with a criminal offense.

(2) The person was released from custody after charges were dropped, or dismissed, or where a notice of nolle prosequi was entered.

(3) The person was charged with a criminal offense and was found "not guilty."

(f) A law enforcement agency or a law enforcement officer shall not use targeted facial scan identification in conjunction with an identification photo database, or acquire in bulk the photos in that database except as provided in subdivision (g).

(1) A law enforcement agency or a law enforcement officer may use or request face recognition in conjunction with an identification photo database by an order issued pursuant to subparagraph (2).

(2) A law enforcement agency or a law enforcement officer may submit a written application to a court of competent jurisdiction for an order authorizing the use of targeted facial scan identification in conjunction with an identification photo database to identify a person or persons when a law enforcement agency or a law enforcement officer has probable cause to believe that the person or persons have committed, are in the process of committing, or are about to commit a criminal offense. The court may grant such an order in conformity with subparagraph (4).

(3) Each application for an order authorizing the use of targeted facial scan identification in conjunction with an identification photo database shall be made in writing upon oath or affirmation to a court of competent jurisdiction and shall expressly state the applicant's authority to make such application. Each application shall include the following information:

(A) The identity of the law enforcement officer making the application;

(B) A full and complete description of the person or persons that the officer is seeking to identify;

(C) A full and complete description of the photos or video footage portraying that person or persons that will be used to search the identification photo database;

(D) A full and complete statement as to whether or not other investigative procedures to identify that person or persons has been attempted or why they reasonably appear to be unlikely to succeed;

(E) The specific identification photo database or databases to be searched;

(F) The offense for which the person or persons are being charged, or are likely to be charged; and

(G) A full and complete statement of the facts and circumstances that provide the applicant probable cause to believe that the person or persons have committed, are in the process of committing, or are about to commit a criminal offense.

(4) Upon written application, a judge may enter an ex parte order authorizing or approving the use of targeted facial scan identification in conjunction with an identification photo database. The order must be based on the following determinations:

(A) There exists probable cause to believe that a person or persons have committed, are in the process of committing, or are about to commit a criminal offense.

(B) Normal investigative procedures, including the use of targeted facial scan identification in conjunction with an arrest photo database, have been attempted and have failed or reasonably appear to be unlikely to succeed.

(C) The ex parte order shall state all of the following:

(i) The identity of the state or federal law enforcement agency authorized to conduct targeted facial scan identification, and of the officer authorizing the application;

(ii) The authority under which the order is made;

(iii) A detailed description of the person or persons that the applicant seeks to identify;

(iv) The photos or video footage portraying the person or persons to be used to search the identification photo database;

(v) An order prohibiting the use of future photos or video footage not specifically listed in the application;

(vi) The identification photo database or databases to be searched;

(vii) The period of time within which the agency must execute the search, not to exceed thirty (30) days; and

(viii) The offense for which the person or persons are being charged, or are likely to charged.

(g) This section does not apply when a law enforcement agency or a law enforcement officer uses targeted facial scan identification in conjunction with an arrest photo database or an identification photo database under the following circumstances:

(1) To identify a person who is deceased, incapacitated, or otherwise physically unable to identify him or herself.

(2) To identify a person who is the victim of a crime when the officer determines, in good faith, that the person cannot be identified by any other means.

(3) To identify a person who has been lawfully arrested, or during the booking process after a lawful arrest, or during the custodial detention of such a person.

(4) When a law enforcement agency or a law enforcement officer believes, in good faith, that an emergency involving danger of death or serious physical injury to any person may occur, in which the law enforcement agency or law enforcement officer making that determination shall apply for an order approving such use within twenty-four (24) hours after the use occurred, and shall terminate immediately if the application is denied. If a law enforcement agency or a law enforcement officer fails to apply for such an order, then the all information obtained as a result of the search shall be immediately destroyed.

(h) A law enforcement agency or a law enforcement officer shall not use or request continuous facial scan identification in conjunction with an arrest photo database except as provided in subdivision (d).

(i) A law enforcement agency or a law enforcement officer may use or request continuous facial scan identification in conjunction with an arrest photo database maintained pursuant to subdivision (l).

(2) A law enforcement agency may submit a written application to a court of competent jurisdiction for an order authorizing the use of continuous facial scan identification in conjunction with an emergency watchlist. The court may grant such an order in conformity with subparagraph (4).

(3) Each application for an order authorizing the use of continuous facial scan identification in conjunction with an emergency watchlist shall be made in writing upon oath or affirmation to a court of competent jurisdiction and shall

expressly state the applicant's authority to make such application. Each application shall include the following information:

(A) The identity of the law enforcement officer making the application;

(B) The number of persons on the emergency watchlist;

(C) A full and complete description of the person or persons on the emergency watchlist, or their identities, if known, and the photos or video footage through which they have been enrolled on the emergency watchlist;

(D) A full and complete description of the nature and specific locations where continuous facial scan identification will be performed;

(E) The period of time for which the continuous facial scan identification is required to be maintained;

(F) A full and complete statement as to whether or not other investigative procedures to locate that person or persons on the emergency watchlist have been attempted or why they reasonably appear to be unlikely to succeed;

(G) A full and complete statement of the criminal offense involving imminent danger of death or serious bodily injury that are being investigated;

(H) A full and complete statement of the facts and circumstances that provide probable cause to believe that the person or persons have committed, are in the process of committing, or are about to commit a criminal offense;

(I) A full and complete statement of the facts and circumstances that provide reason to believe that an emergency situation exists that requires the use of continuous facial scan identification without delay;

(J) A court may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(4) Upon written application, a judge may enter an ex parte order authorizing or approving the use of continuous facial scan identification in conjunction with an emergency watchlist. The order must be based on the following determinations:

(A) There exists probable cause to believe that a person or persons on the emergency watchlist have committed, are in the process of committing, or are about to commit a particular offense involving imminent danger of death or serious bodily injury.

(B) Normal investigative procedures to locate the person or persons on the emergency watchlist have been attempted and have failed or reasonably appear to be unlikely to succeed.

(C) An emergency situation exists that requires the use of continuous facial scan identification without delay.

(D) The ex parte order shall state all of the following:

(i) The identity of the law enforcement agency or law enforcement officer authorized to conduct continuous facial scan identification;

(ii) The authority under which the order is made;

(iii) A detailed description of the person or persons on the emergency watchlist, or their identities, if known, and the photos or video footage through which they have been enrolled on the emergency watchlist;

(iv) The nature and specific locations where continuous facial scan identification will be performed;

(v) The particular offense, or facts and circumstances, that are being investigated;

(vi) The period of time during which such continuous facial scan identification is authorized;

(j) This section does not apply when a law enforcement agency or a law enforcement officer uses continuous facial scan identification in conjunction with an emergency watchlist under the following circumstances:

(1) When a law enforcement agency or a law enforcement officer believes, in good faith, that an emergency involving danger of death or serious physical injury to any person may occur, in which the law enforcement agency or law enforcement officer making that determination shall apply for an order approving such use within twenty-four (24) hours after the use occurred or began, and shall terminate immediately if the application is denied. If a law enforcement agency or a law enforcement officer fails to apply for such an order, then all information obtained as a result of the search shall be immediately destroyed.

SECTION 2. (Civil Rights and Civil Liberties) Section _____ is added to the Penal Code, to read:

_____

A law enforcement agency or a law enforcement officer shall not do any of the following:

(a) Use face recognition to create a record of an individual for exercising rights protected by the First Amendment of the United States Constitution, or to describe the contents, subject matter, or the time, place, and manner in which that individual exercises such rights.

(b) Use face recognition to create a record of an individual for invoking or exercising rights protected by Article I, sections 1 through 4, 8, and 13 of the California Constitution.

(c) Rely on actual or perceived race, ethnicity, national origin, religion, disability, sex, sexual orientation, gender, or gender identity in selecting which person to subject to face recognition, except where there exists probable cause to believe that the individual has committed, is in the process of committing, or is about to commit a criminal offense.

SECTION 3. (Enforcement) Section _____ is added to the Penal Code, to read:

(a) Any face recognition evidence obtained as a result of a violation of any section of this Act shall be suppressed from introduction in any trial, hearing, or any other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or any other authority of the State of California, or any political subdivision thereof.

(b) If a court or law enforcement agency determines that an investigative or law enforcement officer has violated any provision of this Act, the agency shall immediately initiate an investigation to determine whether disciplinary action is warranted.

(c) Any person who is subject to targeted identification or attempted identification through targeted continuous face recognition, or who suffers harm, as a result of a violation of this Act bring a civil action in any court of competent jurisdiction against the law enforcement agency or person who is responsible for the violation. In addition to any other sanctions, penalties, or remedies provided by law, the court may award a combination of any one or more of the following:

(1) Actual damages, but not less than liquidated damages in the amount of two thousand five hundred dollars ($2,500).

(2) Punitive damages upon proof of willful or reckless disregard of the law.

(3) Reasonable attorney's fees and other litigation costs reasonably incurred.

(4) Other preliminary and equitable relief as the court determines to be appropriate.

[i] Office of the Attorney Gen., News Release, *Attorney General Bill Lockyer, Orange County Sheriff Michael Carona and Agency Secretary Maria Contreras-Sweet Demonstrate Fast, New Photo Database* (2002), http://ag.ca.gov/newsalerts/print_release.php?id=766 (last visited Nov. 2, 2017).

[ii] Cal. Law Enforcement Telecommunications Sys. (CLETS) Advisory Comm. (CAC), Meeting Minutes 1-6 (November 21, 2013).

[iii] *FACE RECOGNITION TECHNOLOGY: DOJ and FBI Need to Take Additional Actions to Ensure Privacy and Accuracy* (Mar 22, 2017), https://www.gao.gov/products/GAO-17-489T (last visited Nov. 2, 2017).

[iv] Curtis Waltman, *California Department of Justice Spent Nearly Two Million Dollars on Controversial Facial Recognition Software*, 2017 MuckRock, Apr. 27, 2017 at (2017), https://www.muckrock.com/news/archives/2017/apr/27/california-doj-facial-recognition/ (last visited Nov. 2, 2017).

[v] Ctr. on Privacy & Tech., *The Perpetual Line-Up – Unregulated Police Recognition in America* (Georgetown Law 2016).

[vi] SAM BRAKE GUIA, *Facial Recognition Presents Threat to LGBT Community*, 2017 The Sociable, Sept. 21, 2017 at (2017), https://sociable.co/technology/facial-recognition-lgbt/ (last visited Nov. 2, 2017).

[vii] *Face-Reading AI Will Detect Politics and IQ, Expert Says,* 2017 CIO Today, Oct. 13, 2017 at (2017), https://www.cio-today.com/article/index.php?story_id=106079 (last visited Nov. 2, 2017).

[viii] Jodie Gil & Vern Williams, *How New Technology Like AI, Drones and Big Data Can Limit the First Amendment,* 2017 , Oct. 11, 2017 at (2017), http://mediashift.org/2017/10/6-new-media-first-amendment-issues-horizon/ (last visited Nov. 2, 2017).

[ix] Libby Watson, *Jason Chaffetz Wants to Use Facial Recognition to Track Immigrants,* 2017 Gizmodo, Mar. 22, 2017 at (2017), https://gizmodo.com/noted-shithead-jason-chaffetz-wants-to-use-facial-recog-1793520036 (last visited Nov. 2, 2017).

[x] Ron Nixon, *Border Agents Test Facial Scans to Track Those Overstaying Visas,* 2017 , Aug. 1, 2017 at (2017), https://www.nytimes.com/2017/08/01/us/politics/federal-border-agents-biometric-scanning-system-undocumented-immigrants.html (last visited Nov. 2, 2017).