STATE OF CALIFORNIA
Franchise Tax Board

Bill Analysis

Author: Jackson	Sponsor:	Bill Number: SB 1010
Analyst: Jahna Carlson	Phone: (916) 845-5683	Amended: March 25, 2020
Attorney: Shane Hofeling	Related Bills: See Legislative History	

SUBJECT

Safety, Accountability, Freedom, and Economic Opportunity Act (SAFE Act)

SUMMARY

This bill would under the Civil Code, create the SAFE Act.

RECOMMENDATION

No position

SUMMARY OF AMENDMENTS

The March 25, 2020, amendments removed the bill's provision that would have made a nonsubstantive change to the Information Practices Act of 1977 and replaced it with the provisions creating the SAFE Act.

This is the department's first analysis of the bill and only addresses the provisions that impact the department.

REASON FOR THE BILL

The reason for this bill is to establish limits on the use of biometric information and establish reporting requirements on the collection, use, and storage of such information to protect an individual's privacy.

ANALYSIS

This bill would under the Civil Code establish the SAFE Act that would require government entities including the Franchise Tax Board (FTB) to submit a written report to the Legislature on or before March 31, 2021, that includes all of the following:

- Whether, in the past three years, the government entity has developed, acquired, possessed, accessed, used, or shared any facial recognition or other biometric surveillance system or commercial biometric database.
- The purpose of the system or database.
- The source of the system or database.

- The date of acquisition of the system or database.
- The policies and procedures governing the system or database.

The report would be required to be submitted in compliance with Government Code section 9795.

The reporting requirement would be repealed on January 1, 2025.

This bill would prohibit a government entity, including the FTB, from sharing images, recordings, or biometric information with any other person or entity for use in a facial recognition or other biometric surveillance system or commercial biometric database.

This bill would allow an individual to bring a lawsuit for damages, injunctive relief, or both, for a government entity's violation of the bill's prohibition in a court of competent jurisdiction. An individual that prevails could obtain any or all of the following remedies:

- Recovery of damages in an amount equal to or greater than $100 and less than or equal to $750 per individual per violation, or actual damages, whichever is greater.
- Reasonable attorney fees and costs.
- Injunctive and declaratory relief, as appropriate.
- Any other relief the court deems appropriate.

In determining the amount of statutory damages, the court would be required to consider one or more relevant circumstances presented by any party to the case, including the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

This bill would define a number of terms and phrases, including:

- "Biometric information" means a physiological, biological, or behavioral characteristic that can be used, singly or in combination with each other or with other information, to establish identity. Biometric information would specifically exclude a physical or digital photograph, unless used or stored for the purpose of facial recognition or other biometric surveillance.
- "Biometric surveillance system" means any computer software or application that performs facial recognition or other biometric surveillance.
- "Commercial biometric database" means a collection of biometric information that an entity other than a government entity possesses, controls, or shares alone or as part of a biometric surveillance system.

- "Facial recognition or other biometric surveillance" means either or both an automated or semiautomated process that captures or analyzes biometric information of an individual to identify or assist in identifying an individual, and an automated or semiautomated process that generates, or assists in generating, surveillance information about an individual based on biometric data. "Facial recognition or other biometric surveillance" would specifically exclude both the use of an automated or semiautomated process for the purpose of redacting a recording for release or disclosure outside the law enforcement agency to protect the privacy of a subject depicted in the recording, if the process does not generate or result in the retention of any biometric information or surveillance information and the use of a mobile fingerprint scanning device during a lawful detention to identify a person who does not have proof of identification if this use is lawful and does not generate or result in the retention of any biometric information or surveillance information.
- "Government entity" means a department or agency of the state or its political subdivision, or any person acting for or on behalf of, or at the request of, the state or its political subdivision.
- "Share" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or any other means.

Effective/Operative Date

Assuming that this bill is enacted before September 30, 2020, this bill would be effective January 1, 2021, and operative as of that date.

Federal/State Law

Federal Law

Because this bill only adds provisions to the Civil Code relating to biometric surveillance systems, a review of federal income tax law would not be relevant.

State Law

Current state law, the Information Practices Act of 1977 (IPA), declares that the right to privacy is a personal and fundamental right protected by the California Constitution and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them. The IPA applies to state government and expands upon the constitutional guarantee of privacy by limiting the collection, management and dissemination of personal information by state agencies to only what is relevant and necessary for a required or authorized purpose.

On January 1, 2020, the California Consumer Privacy Act (CCPA), enacted in 2018, took effect. The CCPA created new consumer rights relating to the access to,

deletion of, and sharing of personal information that is collected by businesses. The CCPA expanded the state's existing privacy and information security regulatory framework to cover biometric data that the CCPA broadly defines to include physiological, biological, and behavioral characteristics.

Current state law prohibits a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera, also referred to as a body camera, or data collected by an officer camera, and authorizes a person to bring an action for equitable or declaratory relief against a law enforcement agency or officer who violates that prohibition.

Implementation Considerations

The department has identified the following implementation concerns. Department staff is available to work with the author's office to resolve these and other concerns that may be identified.

The definitions of "biometric information," "biometric surveillance system," and "facial recognition or other biometric surveillance" may be more broadly interpreted than the author intends and could impact the department's ability to use behavioral analysis or biometric indicators for fraud detection and preservation of system security. For example, the definition of "biometric information" would include biometric characteristics for user access to the department's web applications and to identify and stop potential account take over, malicious use of the system, and data loss.

Technical Considerations

None noted.

Policy Concerns

None noted.

LEGISLATIVE HISTORY

AB 1215 (Ting, Chapter 579, Statutes of 2019) prohibits a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera, also referred to as a body camera, or data collected by an officer camera, and authorizes a person to bring an action for equitable or declaratory relief against a law enforcement agency or officer who violates that prohibition.

AB 2261 (Chau, 2019/2020) would enact safeguards regarding the use of facial recognition services in the state. AB 2261 is currently pending before the Assembly Appropriations Committee.

PROGRAM BACKGROUND

None noted.

FISCAL IMPACT

The department's costs to implement this bill have yet to be determined. As the bill moves through the legislative process and the implementation concerns are resolved, costs will be identified.

ECONOMIC IMPACT

Revenue Estimate

This bill as amended on March 25, 2020, would not impact state income or franchise tax revenue

This analysis does not account for changes in employment, personal income, or gross state product that could result from this bill or for the net final payment method of accrual.

LEGAL IMPACT

None noted.

APPOINTMENTS

None noted.

SUPPORT/OPPOSITION

To be determined.

ARGUMENTS

To be determined.

LEGISLATIVE STAFF CONTACT

Jahna Carlson
Legislative Analyst, FTB
(916) 845-5683
jahna.carlson@ftb.ca.gov

Tiffany Christiansen
Revenue Manager, FTB
(916) 845-5346
tiffany.christiansen@ftb.ca.gov

Annette Kunze
Legislative Director, FTB
(916) 845-6333
annette.kunze@ftb.ca.gov