Date of Hearing: March 26, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1281 (Chau) – As Introduced February 21, 2019

SUBJECT: Privacy: facial recognition technology: disclosure.

SUMMARY: This bill would require a business in California that uses facial recognition technology (FRT), as defined, to disclose that usage in a physical sign that is clear and conspicuous at the entrance of every location that uses FRT. Specifically, **this bill would**:

1) Require that any business that utilizes FRT to disclose that usage in a physical sign at the entrance of every location that uses FRT.

2) Define "clear and conspicuous" to mean in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols and other marks that call attention to the language.

3) Define "FRT" to mean a software application used to automatically identify individuals from a digital image or video frames.

4) Provide that a violation of the bill shall be considered unfair competition pursuant to existing law, and that one violation shall occur for each day the required disclosure is not made.

EXISTING LAW:

1) Provides, under the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const. art. I, Sec. 1.)

2) Provides, pursuant to the California Consumer Privacy Act (CCPA), effective January 1, 2020, that a business that collects personal information (PI) must inform the consumer at or before the time of collection, the category and purpose of the PI that is to be collected. (Civ. Code. Sec. 1798.100(b).)

3) Defines various terms for purposes of the CCPA, including the following, among others:

   - "PI" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Specifies that PI includes, but is not limited to, certain types of information if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household. Among these is "biometric information." (Civ. Code. Sec. 1798.140(o)(1)(E).)

   - "Biometric information" means an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the

iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information. (Civ. Code. Sec. 1798.140(b).)

4) Generally protects consumers from unlawful, unfair and fraudulent business practices under California's Unfair Competition Law (UCL). (Bus. & Prof. Code Sec. 17200, et seq.)

5) Provides, pursuant to the UCL, that a business that fails to comply with the provisions of the act be subject to fines not to exceed $2,500 for each violation. (Bus. & Prof. Code. Sec. 17206.)

FISCAL EFFECT: This bill has been keyed nonfiscal by the Legislative Counsel.

COMMENTS:

1) **Purpose of the bill**: This bill seeks to enhance consumer choice by requiring businesses that use FRT notify consumers of this usage prior to a consumer entering a commercial establishment. This is an author-sponsored bill.

2) **Author's Statement**: According to the author, "[f]acial recognition technology (FRT) is becoming ever more present throughout businesses in California. It can be used to prevent retail crime, find missing persons, and even diagnose diseases. However, concerns about privacy and use of the information are increasing. Individuals are not currently informed [when] FRT being used on them, nor do they know how long the information is held or how it is used. AB 1281 would simply make consumers aware of which California businesses are using FRT by requiring each business to disclose the use of the technology with a physical sign at its entrance."

3) **The widespread use of FRT**: FRT is passive and universal, meaning that by simply walking into range of an FRT system (camera), a person's biometric information is captured. Thus, it is not necessary to complete a transaction or to otherwise actively engage with a business in order to have your personal information stored and used by that business.

   That is not to say, however, that FRT does not present potential utility for its adopters and the public as whole. Operationalizing FRT in the sphere of public safety can offer a tremendous decrease in the cost of security oversight and in enforcement accuracy (though the utility is arguably limited by identified bias, discussed more in Comment 4, below). FRT also allows users to unlock their phones without a password, alerts individuals when a friend uploads their picture to social media, and allows business to identify and address repeat customers and offer them better service. In the future, FRT could be used to increase businesses' advertising efficiency, help law enforcement find missing persons, or even allow consumers to skip the checkout line at the grocery store. Thus, whether it is law enforcement, schools, or business, FRT has the potential to lead to noticeable improvements.

   That being said, FRT also has the potential to undermine an individual's right to privacy at the same time that it offers the promise of utility to entities employing it. Defining the appropriate balance between privacy interests and competing public policies can be difficult to define. Californians have enshrined the right to privacy in the state Constitution and as a state, California has consistently been an example to other states through its prioritization of

its residents' right to privacy. Specifically, since the right to privacy was expressly provided in the state Constitution in 1972, the Legislature has continued to flesh out how this fundamental right is protected. The Confidentiality of Medical Information Act limits the disclosure of patients' medical information absent their consent. The Computer Spyware Act prohibits an unauthorized person from knowingly installing or providing software on another's computer, as specified. (Civ. Code Sec. 56 et seq. and Bus. & Prof. Code Sec. 22947 et seq.) California also has specific privacy protections for victims of domestic violence, elder and dependent adult abuse, stalking, and human trafficking, and similarly provides address confidentiality for elected and public officials despite the public's interest in transparency. (Gov. Code Sec. 6205 et seq. and Gov. Code Sec. 6254.21.) The CCPA, enacted in 2018 to protect the privacy of consumers' PI when in the possession of businesses, represents the most recent example of a long and pioneering history of placing privacy above all but the most serious concerns.

However, while there are a host of laws that protect the PI of Californians, including some that cover biometric information which would necessarily include certain applications of FRT, there are currently no statutes in place that directly govern the use of FRT more broadly in California. By requiring every business that uses FRT in California to disclose that usage to consumers, regardless of the business's size, this bill arguably increases consumer awareness substantially with minimal impact on the business themselves. In turn, by having awareness, consumers can make more informed choices about where they shop, and have a better appreciation that their biometric information is being collected and potentially used by businesses.

As highlighted in a recent article by national American Civil Liberties Union (ACLU) privacy and policy experts, *Are Stores You Shop at Secretly Using Face Recognition on You?*, a recent ACLU survey directly asked 20 of the largest brick and mortar store operators in the United States if they currently utilized FRT. Only one affirmatively denied using it and one verified they in fact did use FRT, claiming they use it specifically to prevent theft and identify shoplifters. The other 18 stores refused to answer the question at all. (Bitar & Stanley, *Are Stores You Shop at Secretly Using Face Recognition on You?*, ACLU (Mar. 26, 2018) <https://www.aclu.org/blog /privacy-technology/surveillance-technologies/are-stores-you-shop-secretly-using-face> [as of Mar. 19, 2019].) As stated by the ACLU experts:

> At this point, customers may understand intellectually that their movements in stores are captured on video — although most stores place them in domes made of smoked glass for no reason other than to hide the cameras from customers (who might find the swiveling, zooming lenses therein to be spooky and actually gain a realistic sense of the extent to which they are being watched). Most customers also probably expect that most camera feeds, most of the time, are not being monitored — and that if they are, nothing is done with the video footage that is collected, so long as nothing dramatic is captured.
>
> But I think [it is] fair to say that most customers do not think that they are being subject to a perpetual lineup, scrutinized by face recognition technology to see if they resemble anyone that a company security service has decided to put on a watch list. They do not expect that their faces are being captured, retained, connected to their real-world identity (for example when they use a credit card at checkout), and combined with information about their income, education, demographics, and other data. They do not expect that their every footstep, hand motion, and gaze will be analyzed by computers and filed away

> to give insight into their shopping habits, patterns, and preferences, and shared among different companies, data brokers, and advertisers. They do not expect that they are subject to the risk of being misidentified as someone in a database of suspected criminals, fugitives, terrorists, or whatever other blacklists stores may be using or begin using in the future. They [do not] expect that all these intimate details about their behavior will become accessible to government agencies through legal demands or voluntary sharing.
>
> And if those things are happening, I think most customers would want to know about it. (*Id.*)

As stated by the ACLU in response to the reported implementation of FRT by Ohio state officials without any debate, FRT raises "difficult issues, but the first steps are clear. We need to shine more and brighter lights in all the shadowy corners of state surveillance. We probably won't like what we find, but we can't fix a problem we don't know exists." (Crockford, *Ready, fire, aim: Ohio officials implement statewide face recognition program without a whiff of public debate,* ACLU (Sep. 3, 2013) < https://www.aclu.org/blog/national-security/privacy-and-surveillance/ready-fire-aim-ohio-officials-implement-statewide> [as of Mar. 19, 2019].) While this bill applies to private businesses, the same can arguably be said about shining a light on business practices so Californians can be informed at the places they visit.

4) **Second order issues with FRT**: While FRT may present great potential in terms of utility, these benefits do not come without risk. There are a number of concerns as to how it is currently operationalized, which stand to undermine the benefit of the technology's utility if not addressed. A recent New York Times article cites specific issues with Amazon's[1] FRT system that shows it consistently underperforms when used to accurately identify people with darker completions and of different genders. (Harwell, *Amazon facial-identification software used by police falls short on tests for accuracy and bias, new research finds,* The Washington Post, (Jan. 25, 2019) <https://www.washingtonpost.com/technology/2019/01/25/amazon-facial-identification-software-used-by-police-falls-short-tests-accuracy-bias-new-research-finds/?utm_term=.0c266b980812 > [as of Mar. 20. 2019].) This is an example of how, despite the pervasiveness of this technology, it is still in its developmental infancy. FRT systems are learning systems that are only as good as their programing. In other words, the technology generally improves as it is given more information. As data sets get larger, the technology will improve and hopefully become more accurate, reducing concerns related to bias. This is all the more reason for people to make an informed choice before ever exposing themselves to systems that collect and potentially retain their biometric information for unknown purposes.

5) **Bill would allow for more effective implementation of obligations and rights under the CCPA**: The CCPA requires that businesses inform consumers about the type of PI a business collects about them, and defines PI to include biometric information. In turn, the CCPA defines "biometric information" to include, among other things, "imagery of the iris, retina, fingerprint, [and] face[.]" (Civ. Code Sec. 1798.140 (b) and (o).) As such, this information clearly encompasses data collected by FRT.

---

[1] These types of bias issues have been identified in other proprietary FRT systems. Amazon just happens to be one of the most successful businesses in the field and thus open to more direct scrutiny.

The CCPA separately defines "business" as a legal entity, as specified, that is organized or operated for profit, that collects consumers' PI, and that satisfies one or more specified thresholds:

- having an annual gross revenue in excess of $25,000,000; or,
- alone or in combination, annually buying, receiving for the business's commercial purposes, selling, or sharing for commercial purposes, alone or in combination, the PI of 50,000 or more consumers, households, or devices; or,
- deriving 50 percent or more of its annual revenues from selling consumers' personal information. (Civ. Code Sec. 1798.140(c).)

Notably, this definition does not distinguish between businesses that operate online and those that are a traditional brick and mortar type-establishment. Since FRT enables the collection of biometric information, a plain reading of the relevant statutes would require both types of businesses (if they satisfy the criteria established by the CCPA) that use FRT, to disclose that information to consumers once CCPA becomes operative, on January 1, 2020. For businesses that operate online, this disclosure could be made on their internet website. However, the mechanism by which brick and mortar stores notify consumers may not be as apparent to the consumer on the outset of their visit to the brick and mortar store. By requiring this disclosure to be made at the *entrance* of brick and mortar stores, this bill would remove any ambiguity for both the brick and mortar store collecting such personal (biometric) information and for the consumer, thereby helping ensure that the store complies with the CCPA's notice requirements, and protecting consumers from unwittingly participating in the use of FRT.

Regarding the mandatory disclosure under this bill, the California Retailers Association (CRA) argues for a delayed implementation of "September 1, 2020, which would provide a year's notice for the industry to become aware of the new law, and to have the signs printed and posted. Without such an amendment, the effective date will be January 1, 2020, providing only [three] months notice if the Governor signs the bill."

To ensure clarity and ease any confusion for any businesses subject to the overlapping requirements of this bill and the CCPA, the author offers the following amendment that would delay the effective date of this bill to July 1, 2020. This, as opposed to the September date suggested by CRA, would better coincide with the CCPA, which prohibits the Attorney General from bringing any enforcement actions under that act until six months after its final regulations are published, or July 1, 2020 (whichever date is sooner). .

Author's amendment:

Delay implementation of AB 1281 until July 1, 2020.

6) **Small business usage of FRT**: This bill would require all businesses that use FRT to disclose that usage to customers, regardless of size. As noted in Comment 5, above, the CCPA only applies to businesses of a certain size or that otherwise cross specific PI collection thresholds. However, with FRT use becoming more widespread as the barriers to entry become smaller, coupled with the apparent utility in FRT systems, its inevitable adoption by smaller businesses becomes more of an immediate reality.

Californians are entitled to privacy under the state constitution, and the concern of FRT undermining that privacy right exists regardless of the business's size. Recognizing this, this bill correctly keeps that fundamental right in mind while balancing the costs associated with compliance for small businesses. Arguably, this bill places a very small obligation on business possible: simple notification. That obligation, however, should help Californians better exercise their rights and make informed choices.

7) **Potential issues of enforceability**: As drafted, failure to comply with the requirements of this bill would constitute an unfair business practice, which would subject a business of a civil penalty of up to $2,500 under the state's Unfair Competition Law (UCL). (Bus. & Prof. Code Secs. 17200 et seq. and 17206.) CRA, in opposition, argues that mandated signage grows every year and that the enforcement mechanism in this bill should be saved for more serious offensives. CRA writes:

> Prop 65 warnings, beverage recycling locations, return policies, hours of operation alcoholic beverage applications, solicitation policies – all appear on store entrances. We respectfully suggest that enforcement of a new sign positing requirement should not be through Section 17200 of the Business and Profession Code. The Unfair Business Practices Act [the UCL] should be reserved for more serious violations such as weights and measures overcharges, anti-competitive acts, scanning violations, etc. The inadvertent absence of a sign at one location, whether by oversight, or accidental falling down of the sign, or a customer removing the sign, even if a sign remains posted at other entrances, should be a lesser violation.
>
> [CRA suggests] the following alternative: "The first and second violations shall result in a notice of violation, and any subsequent violation shall constitute an infraction punishable by a fine of twenty-five dollars ($25) for each day the business i[s] in violation, but not to exceed three-hundred dollars ($300) annually." This is the enforcement approach used in the straws-upon-request bill enacted last year by the Legislature, and also found in AB 161 this year.

Estimating the impact on business to comply with this bill is difficult in the abstract. The costs associated with designing and displaying a sign will surely vary from business to business based on their preferences and structure. However, as CRA points out in their letter, these same businesses have been routinely asked to prominently place signage advising patrons of their various rights and of specific safety concerns mandated by Proposition 65. Thus, it is likely that most businesses will be familiar with the process of complying with the requirements of this bill and already have mechanism in place to do so. That being said, a civil penalty of up $2,500 per violation under the UCL may not provide courts with enough flexibility to fairly address violations of small businesses in comparison to violations of larger businesses. At the same time, the proposed $25 per day violation suggested by CRA may not be sufficient to incentivize compliance, particularly by larger businesses.

Accordingly, the author offers the following amendment that would limit the penalty to up to $75 per day, but never to exceed $7,500 annually or one percent of the business's net income. Arguably, this should create a penalty structure that, while not being overly punitive, still incentivizes businesses big and small to comply with the provisions of the bill. Staff also notes that this proposal, allowing for prosecution by public attorneys and providing

for the distribution of the judgments, are consistent with various statutes under existing law. (*See e.g.,* Civ. Code Sec. 1745.5.)

Author's amendment:

On page 2, strike lines 20-23 and insert the following:

(c) (1) Any person who fails to comply with subdivision (a) shall be liable for a civil penalty up to seventy five dollars ($75) for each violation, not to exceed seventy five hundred dollars ($7,500) annually or one percent (1%) of the business's net income, whichever is higher, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General, by any district attorney, county counsel, city attorney, or by a city prosecutor in any city having a full-time city prosecutor, in any court of competent jurisdiction.

(2) If the action is brought by the Attorney General, one-half of the penalty collected shall be paid to the treasurer of the county in which the judgment was entered, and one-half to the General Fund. If the action is brought by a district attorney, the penalty collected shall be paid to the treasurer of the county in which the judgment was entered. If the action is brought by a city attorney or city prosecutor, one-half of the penalty shall be paid to the treasurer of the city in which the judgment was entered, and one-half to the treasurer of the county in which the judgment was entered.

8) **Prior legislation**: AB 375 (Chau, Ch. 55, Stats. 2018) enacted the CCPA to ensure the privacy of Californians' PI through various consumer rights.

SB 1121 (Dodd, Ch. 735, Stats. 2018) ensured that a private right applied only to the CCPA's section on data breach and not to any other section of the CCPA, as specified, corrected numerous drafting errors, made non-controversial clarifying amendments, and addressed several policy suggestions made by the AG in a preliminary clean-up bill after the passage of AB 375.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

California Retailers Association

Analysis Prepared by: David Watson / P. & C.P. / (916) 319-2200