Date of Hearing: May 5, 2020

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 2261 (Chau) – As Introduced February 14, 2020

AS PROPOSED TO BE AMENDED

SUBJECT: Facial recognition technology

SUMMARY: This bill would establish a comprehensive legal framework governing the use of facial recognition technology (FRT) by public and private entities, including requiring opt-in consent for the enrollment or disclosure of an individual's facial information, requiring probable cause that an individual committed a serious criminal offense to enroll without consent, requiring independent assessment of accuracy and discriminatory performance of FRT, prohibiting denial of service on the basis of withholding consent for collection or disclosure of facial information, and requiring that decisions informed by FRT are subject to meaningful human review. Specifically, **this bill would**:

1) Require a controller to obtain consent from an individual before enrolling an image or facial template in a facial recognition service (FRS) used in a physical premise open to the public, and prohibit denying access to or service from a physical premise open to the public on the basis that an individual has exercised their right to withhold consent for enrolling facial information in an FRS.

2) Permit a controller to enroll an image or facial template of an individual in an FRS for a security or safety purpose without first obtaining consent from that individual only if all of the following requirements are met:

    - the controller has probable cause to believe that the individual has committed, or attempted to commit, a serious criminal offense;

    - a database used by an FRS for recognition, verification, or persistent tracking of individuals for a security or safety purpose is only used for that purpose and maintained separately from any other databases maintained by the controller;

    - the controller removes the facial information as soon as there is no longer probable cause to believe that the individual has committed, or has attempted to commit a serious criminal offense;

    - the controller reviews a database used for a security and safety purpose at least twice per year to remove facial templates that are more than three years old, or that the controller no longer has probable cause to believe the individual has committed, or has attempted to commit, a serious criminal offense; and

    - the controller establishes an internal process whereby individuals may correct or challenge the decision to enroll the image of an individual in an FRS for a security or safety purpose.

3) Prohibit a controller from knowingly disclosing personal data obtained from an FRS to a person or agency unless any of the following are true:

    - The disclosure is pursuant to the consent of the individual, and their consent for disclosure was not a requirement for the provision of a service.

    - The disclosure is required by federal, state, or local law in response to a court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or grand jury subpoena.

    - The controller has a good faith belief that the disclosure is necessary to prevent or respond to an emergency involving danger of death or serious physical injury to a person.

    - The disclosure is made to the National Center for Missing and Exploited Children, in connection with a report submitted thereto.

    - The disclosure is made between a controller and a processor to provide an FRS, as long as the engagement is governed by a contract between the controller and processor that is binding, and that sets out mandatory processing instructions.

4) Provide an individual with the rights to confirm if a controller has enrolled an image or facial template of that individual in an FRS used in a physical premise open to the public, to correct or challenge a decision to enroll that facial information for a security or safety purpose, to have their facial information deleted from an FRS used in a physical premise open to the public, and to withdraw consent to enroll their facial information in an FRS at any time.

5) Require a controller to provide a conspicuous and contextually appropriate notice whenever an FRS is deployed in a physical premise open to the public, that includes the purpose for which the FRS is deployed and information about where individuals can obtain information about the FRS, including policies on how individuals can exercise any rights that they have with respect to the FRS.

6) Require that a controller using an FRS to make decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals ensure that those decisions are subject to meaningful human review, as defined.

7) Prohibit an agency from using an FRS to engage in ongoing surveillance unless that use is in support of law enforcement activities or may provide evidence of a serious criminal offense, and either of the following is true:

    - a search warrant has been obtained to permit the use of the FRS for ongoing surveillance; or

    - the agency reasonably determines that ongoing surveillance is necessary to prevent or respond to an emergency involving imminent danger or risk of death or serious physical injury to a person, written approval is obtained from the agency's director or the director's designee before using the service, and a search warrant is obtained within 48 hours after the ongoing surveillance begins.

8) Expressly prohibit an agency from applying an FRS to an individual on the basis of the individual's religious, political, or social views or activities, the individual's participation in a particular noncriminal organization or lawful event, or an individual's actual or perceived race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity, sexual orientation, or other characteristic protected by law.

9) Prohibit an agency from using an FRS to create a record describing an individual's exercise of rights guaranteed by the First Amendment of the U.S. Constitution or by Section 2 of Article I of the California Constitution unless the use is specifically authorized by applicable law, is pertinent to and within the scope of an authorized law enforcement activity, and there is probable cause to believe the individual has committed, is committing, or is about to commit a serious criminal offense.

10) Require a processor that provides FRSs to make available an application programming interface or other technical capability, chosen by the processor, to enable controllers or third parties to conduct legitimate, independent, and reasonable tests of those services for accuracy and unfair performance differences across distinct subpopulations, as defined.

11) Require a processor to implement a plan to mitigate identified performance differences identified pursuant to 10).

12) Require a processor that provides FRS to prohibit, in the contract by which the controller is permitted to use the FRS, the use of the FRS by a controller to unlawfully discriminate under federal or state law.

13) Require a controller to test the FRS in operational conditions and take reasonable steps to ensure best quality results by following all reasonable guidance provided by the developer of the FRS before deploying an FRS.

14) Require a controller using an FRS to, at a minimum, conduct annual training of all individuals that operate an FRS or that process personal data obtained from the use of FRS, which includes the capabilities and limitations of the FRS, procedures to interpret and act on the output of the FRS, and, to the extent applicable, the meaningful human review requirement for decisions pursuant to 6).

15) Require a controller to respond to a request made by an individual to exercise rights enumerated in 4) within 30 days of receipt of the request, with a possible 60 day extension of that period depending on the complexity and quantity of requests being processed.

16) Permit a controller to refuse to comply with a request pursuant to 12) if the request is manifestly unfounded or excessive or if the controller is unable to determine using reasonable efforts that the request is being made by the individual to whom the request pertains.

17) Specify that, if a controller refuses to comply with a request pursuant to 13) on the grounds that the request is manifestly unfounded or excessive, the controller shall bear the burden of demonstrating that the request is manifestly unfounded or excessive, and shall be liable to the individual for court costs and reasonable attorneys' fees if the controller fails to demonstrate as such.

18) Require an agency using or intending to develop, procure, or use an FRS to produce an accountability report for that system, to be updated every two years and subject to public review and comment, including, but not limited to, clear and understandable statements of all of the following:

    - The name of the FRS, vendor, version and a description of its general capabilities and limitations.

    - Any type of data inputs that the FRS uses when it is deployed, how that data is generated, collected, and processed, and the types of data the system is reasonably likely to generate.

    - A description of any purpose or proposed use of the FRS, including any decision it will be used to make or support, and its intended benefits.

    - A clear use and data management policy including how, when, why, and by whom the FRS will be deployed or used, measures taken to minimize inadvertent collection of additional data beyond that necessary for the specific purpose that FRS will be used, data integrity and retention policies applicable to the data collected, additional rules governing the use of the FRS, data security measures applicable to the FRS, training procedures for the use of FRS, testing procedures for the FRS, a description of potential impacts on civil rights and liberties, including impacts on privacy and disparate impacts on marginalized communities as well as specific steps the agency will take to mitigate these impacts and prevent unauthorized use, and the agency's procedures for receiving and responding to feedback.

19) Require an agency to communicate the accountability report prepared pursuant to 15) to the public at least 90 days before the agency puts the service into operational use, and to post the report on the agency's internet website.

20) Require an agency that uses an FRS to prepare and publish an annual report disclosing the extent of the agency's use of FRSs, an assessment of compliance with the terms of the accountability report, any known or reasonably suspected violations of the accountability report, and any recommended revisions to the accountability report for the next update.

21) Require, by the officer who executed a warrant authorizing ongoing surveillance using an FRS, submission of the warrant to the DOJ, and notice to the individual who was tracked, within 10 days following the expiration of the period of surveillance authorized by the warrant.

22) Require that on or before January 1, 2023, and at least biennially thereafter, the California State Auditor conduct an independent audit of state and local agencies deploying FRS in order to evaluate compliance with the provisions of this bill, and to make a report based on that audit available to the public.

23) Confer exclusive authority to enforce the provisions of this bill on the Attorney General.

24) Provide that a controller or processor the provisions of this bill is subject to an injunction and liable to a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation.

25) Define, for the purposes of this bill, the following terms: accountability report, agency, consent, controller, enroll, facial recognition service, facial template, identified or identifiable natural person, meaningful human review, ongoing surveillance, persistent tracking, personal data, publicly available information, process, processor, recognition, security and safety purpose, and serious criminal offense.

26) Makes Legislative findings and declarations relating to the privacy and civil liberties risks of FRSs and to their utility.

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) Until January 1, 2023, prohibits a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera. (Pen. Code Sec. 832.19(b).)

3) 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).)

4) 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).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the bill**: This bill seeks to create a comprehensive, workable legal framework for the use of FRT by both public and private entities that is protective of the privacy and civil liberties of individuals while preserving the utility of the technology. The bill limits the use of FRS to circumstances in which the individual provides consent, except for a very limited

set of safety and security purposes, and requires extensive performance testing and accountability reporting for its use. This bill is author sponsored.

2) **Author's Statement of Criticality**: In response to the unique constraints the COVID-19 crisis has placed on the legislative process, this Committee elected to focus attention this session on bills that address only the most urgent issues and issues critical for an efficient recovery from the pandemic. In order to prioritize bills that require immediate attention, the Committee asked the author of each bill to provide a Statement of Criticality explaining the applicability of one or more of the following criteria to that bill:

   - the bill addresses a problem that was created by, or has been significantly exacerbated by, the ongoing public health crisis due to COVID-19, or the response thereto;

   - the bill addresses an urgent problem that presents a threat to the safety and security of Californians and must be resolved immediately; or

   - the bill makes a technical change to an existing program or function that must be immediately adopted to preserve the utility of that program or function.

   In response, the Author writes:

   > Currently, governments across the globe are turning to technology to spread public health messages, render benefits, and increase access to health care in an effort to save lives in response to the COVID-19 pandemic. According to Amnesty International, the rush by government entities to combat this disease is expanding the use of technology to track individuals and entire populations, and "if left unchecked and unchallenged, these measures have the potential to alter fundamentally the future of privacy and other human rights." As it relates to FRT, tech companies in the United States are reportedly in talks with the U.S. Government to "use their data gathering and data location tools to track virus transmission trends," including Clearview AI, as reported by U.S. News. The report highlights the use of FRT, like Clearview AI, "to identify anyone who's been in contact with an infected person – similar to how tech companies responded in the U.S. after 9/11 with the passing of the Patriot Act, paving way to mass surveillance." Another example of how biometric technology is evolving during the COVID-19 pandemic is its use as a screening system. CSO Online recently reported that Athena Security, whose technology detects guns, is now offering a screening system, equipped with thermal cameras, to detect fevers and alert surrounding customers of someone potentially carrying coronavirus; a product it is pitching to grocery stores, hospitals and voting locations and deploying at government agencies, airports and fortune 500 companies.
   >
   > This year, ten other states have introduced legislation that would regulate, ban or study facial recognition systems, as reported by Axios. On March 31, 2020, Washington State became first in the nation to regulate, comprehensively, the use of FRT by government agencies. The time has come for California to establish a robust FRT law that applies equally across the board in its use by businesses and public entities, and strikes a balance between social responsibility and market success. If action is not taken now, it will become increasingly costly and difficult to implement these regulations since more entities will have developed FRT infrastructure without consideration for these limits.

The Committee agrees that the issues addressed by this bill are timely and critical under the current circumstances. During times of crisis, history has demonstrated that civil liberties and privacy rights are often temporarily suspended for the alleged public interest, only for those intrusions to become permanent. Already, several foreign nations have adopted highly invasive behavioral monitoring in order to track and control the spread of COVID-19. In this country, serious discussions relating to the implementation of contact tracing have bordered on severe invasions of privacy and personal liberty, including suggestions of geolocation tracking and compulsory monitoring of biometrics through cellular devices. Though these technologies have yet to be implemented, facial recognition technology is already in use among law enforcement agencies and private businesses, and the current crisis is likely to augment the role such surveillance technology is permitted to play. It is thus imperative that the Legislature recognize the potential applications and sizable risks posed by FRT at this time, and implement a comprehensive framework to limit its use in a manner that does not stifle innovation and efficiency. The current circumstances are likely to accelerate the ongoing process of developing an essentially unregulated facial recognition technological infrastructure across public and private entities. The transition to remote society necessitated by shelter-in-place orders, for instance, requires the use of technologies with the potential to constantly collect facial information, especially with the growing popularity of online video chat platforms. To stem this expansion, and to implement a comprehensive framework to regulate this technology before such regulation would be infeasible, the Legislature must engage in this conversation immediately. As such, the Committee sees this bill as addressing an immediate issue exacerbated by the COVID-19 crisis.

3) **Facial recognition technology (FRT)**: Facial recognition technology (FRT) refers to the use of automated devices to identify or verify a person from a digital image by determining whether two images of faces represent the same person. FRT consists of two component processes: face detection, or locating a face within a photo, and face identification, or the matching of facial information to an image or images in a specified database that link to identifying information. FRT relies on the use of biometrics, the statistical analysis of measurements of biological data, in order to compare these images, reducing complex images to numerical values that represent key facial measurements that distinguish individuals.

Recent revolutions in computer science, namely in the fields of artificial intelligence and machine learning, have dramatically increased computational power, and have resulted in seismic improvements in the efficiency, accuracy, and scale with which FRT can be implemented.[1] According to a 2018 report from the National Institute of Standards and Technology, the most accurate commercial facial recognition algorithms in 2018 produced twenty times fewer errors than the most accurate algorithms tested just five years prior.[2] These algorithms have improved the speed and ease with which facial information is collected, analyzed, and compared, and have reduced the sensitivity of FRT to confounding variables, such as differences in lighting, angle, age, and expression.[3] As a result, not only can modern FRT be applied on an unprecedented scale - the FBI face recognition unit's

---

[1] *National Institute of Standards and Technology,* "Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification," P. Grother, M. Ngan, K. Hanaoka, *U.S. Department of Commerce,* Nov. 26, 2018, http://doi.org/10.6028/NIST.IR.8238.
[2] "FRVT Part 2," *supra* at fn. 1.
[3] *Ibid.*

database consists of over 400 million photos of up to 125 million Americans - but it can also be used to identify individuals in real-time from surveillance video feeds.[4]

These technological advances have revealed new applications for FRT in a variety of sectors and circumstances. Still, the ability to identify individuals on a large scale, potentially in real time, has significant implications for our fundamental rights to privacy and free expression. Extensive research has also indicated disparities in performance of FRT depending on characteristics of the subjects, with generally poorer performance when identifying people of color and women, as well as entrenchment of existing cultural biases based on the particulars of training data and algorithmic designs.[5] Though FRT retains ample promise as an emerging technology, it is imperative that California adopts a regulatory approach that is mindful of these shortcomings and prioritizes the maintenance of civil liberties guaranteed by the State and Federal Constitutions governing its residents.

4) **Applications of FRT**: FRT has several applications, both current and prospective, that offer utility for technological efficiency, safety, and security. Most frequently, discussions about the use of FRT take place in the context of law enforcement, where it can be used for surveillance and identification of perpetrators or suspects of criminal activity. Responses to public records requests by Georgetown Law's Center for Privacy & Technology suggest that at least 52 state and local law enforcement agencies surveyed are now using, or have previously used or obtained, FRT, indicating extensive adoption that precedes any substantive regulation of the manner in which it is used.[6]

   FRT in the law enforcement context has various applications. For example, it can assist in identifying an individual who either refuses or is unable to identify themselves, in determining whether an apprehended individual matches photos from unsolved crimes or has outstanding warrants, or in obtaining a list of candidates for further investigation based on a photo or video still of a suspect from a security camera, smartphone, or social media post. Most controversially, the use of face identification for real-time video surveillance allows law enforcement to extract faces from live video feeds to identify, passively, any individual within a given area in order to determine the locations of missing persons or suspects of interest. Currently, real-time face recognition is computationally expensive, but the rate of advancement of this technology suggests that it could become more pervasive in the coming years.[7]

   The applications of FRT extend beyond the law enforcement context, as well. For example, FRT can limit access to secure facilities in a manner similar to fingerprint scanners or iris scanners. Such technology is already in widespread use for authorizing access to smartphones, as Apple has provided for the use of highly sophisticated FRT to unlock their devices in the past several iterations of their operating system.[8] Beyond security uses, social

---

[4] *Center on Privacy & Technology*, "The Perpetual Line-Up: Unregulated Police Face Recognition in America," *Georgetown Law*, Oct. 18.2016, https://www.perpetuallineup.org.
[5] *National Institute of Standards and Technology*, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," P. Grother, M. Ngan, & K. Hanaoka, *U.S. Department of Commerce*, Dec. 2019, https://doi.org/10.6028/NIST.IR.8280
[6] "The Perpetual Lineup," *supra* at fn. 5.
[7] *Ibid.*
[8] See, e.g., Yoni Heisler, "Infrared video shows off the iPhone X's new Face ID feature in action," *BGR*, Nov. 3, 2017, https://bgr.com/2017/11/03/iphone-x-face-id-video-infrared; Yoko Kubota, "Apple iPhone X Production Woe

media outlets, such as Facebook, have used FRT to alert users when photos of them are uploaded, whether or not the user is tagged in those images, and to suggest user tags for images.[9] A research report conducted by *Component* assessing the market for FRT predicts that the commercial facial recognition industry in the United States alone will be worth over $7 billion by 2024.[10]

5) **Privacy concerns with FRT**: Because FRT is capable of passively identifying virtually any individual in a recording or real-time feed, and without that individual's knowledge, the expanding adoption of FRT in both the public and private sectors has come under scrutiny for its implications for individual privacy. FRT poses particularly serious threats to privacy because it is, at present, minimally regulated. In response to concerns relating to the lack of regulation of FRT, the California Legislature passed AB 1215 (Ting, Ch. 579, Stats. 2019), which placed a three year moratorium on the use of any biometric surveillance system, including FRT, in connection with police-worn body cameras. Apart from this measure, however, the use of FRT is generally unregulated, and it is unclear how existing privacy protections apply to the use of FRT. While law enforcement collection of biometric information (e.g. mouth swabs, fingerprinting, etc.) typically constitutes a "search" subject to certain protections under the Fourth Amendment, FRT, which can collect biometric information passively, does not require the physical seizure of that biometric information, and is thus categorically unique.[11] Federal district courts in California have held that an individual's reasonable expectation of privacy extends to records of their movements revealed by cell-site location information, and that a warrant must be approved for obtaining this information, indicating that a physical search is not necessary for the Fourth Amendment to apply.[12] However, no state or federal court has yet ruled on the application of Fourth Amendment protections to the use of FRT.

   Other applications of FRT include tracking the behavior of an individual over time by identifying and compiling when an individual is in front of a given recording device/feed, or identifying individuals in public without their knowledge. These capacities raise concerns that adoption of FRT could spell the end of public anonymity. Already, a New York Times exposé revealed that a company specializing in FRT, *Clearview AI*, has aggregated over three billion images scraped from publically accessible media, including Facebook, YouTube, and Venmo, to create a database of online identities matched with images of those individuals that can be used for facial recognition.[13] *Clearview AI* has allegedly provided this service to over 600 law enforcement agencies, allowing identification of virtually any individual in an image so long as that individual maintains an online presence.[14]

Sparked by Juliet and Her Romeo," *The Wall Street Journal*, Sep. 27, 2017, https://www.wsj.com/articles/apple-iphone-x-production-woe-sparked-by-juliet-and-her-romeo-1506510189.

[9] Tom Simonite, "Facebook Creates Software That Matches Faces Almost as Well as You Do," *MIT Technology Review*, Mar. 17, 2014, https://www.technologyreview.com/s/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do.

[10] *Component*, "Facial Recognition Market," Jun. 2019, https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html.

[11] "The Perpetual Line-Up," *supra* at fn. 4.

[12] *Carpenter v. United States* (2018), 585 U.S. ___.

[13] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, Jan. 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[14] *Ibid.*

One can imagine highly invasive public uses of this technology by a regime that places surveillance cameras in all public areas to constantly aggregate information on the behavior of individuals, and sort that information by identity. In effect, application in this manner would create a database of where each person was, what their actions were, and who they were with any time they enter a public space. In conjunction with private technology in the home, e.g. one's smartphone, the same FRT could expand this database to include the behavior of that individual in private. This use of FRT for surveillance is already becoming commonplace in China, in which a vast network of over 300 million public-facing closed circuit surveillance cameras, coupled with advanced FRT, has been used to monitor its population for criminal conduct or dissident behavior.[15] China's government aims to couple the video data collected by these surveillance cameras with other personal data collected on citizens, including criminal and medical records, travel bookings, online purchases, and social media comments, to create a comprehensive government profile of each citizen.[16] Such invasive use of this technology highlights the potential for FRT to be used in manners that disregard personal privacy and suppress the exercise of expressed fundamental rights championed by the United States as a whole and California in particular.

6) **First Amendment concerns with FRT**: It is currently unclear how the First Amendment of U.S. Constitution, which protects the freedoms of speech and assembly, applies to the use of FRT. In 1958, the Supreme Court held in *NAACP v. Alabama* that compelling the NAACP to disclose the identities of its members would likely hinder the ability of those members to advocate for their beliefs, and in 1960, the Supreme Court held in *Talley v. California* that a law prohibiting the anonymous distribution of pamphlets violated the First Amendment.[17] Taken together, these decisions indicate that the courts support an interpretation of the First Amendment that protects *anonymous* speech, which would presumably extend to the use of FRT to identify individuals exercising their freedoms of speech and assembly. However, the unequivocal protection of anonymous speech under the First Amendment has not always been the position of the Court. For instance, in *Laird v. Tatum* (1972), the Supreme Court held that military surveillance of public meetings did not have an "inhibiting effect" on the expression of First Amendment rights unless it created immediate danger of direct injury.[18] Several subsequent cases have used this decision to permit police photography of public demonstrations.[19]

   While such surveillance may be permissible, the courts have not weighed in on whether passive identification of the individuals surveilled during public demonstrations crosses the line into unconstitutional chilling of free speech and assembly. The use of FRT to disclose the identities of all individuals demonstrating for a given cause, as in *NAACP v. Alabama*, has the potential to hinder the ability to advocate for beliefs. In 2015, the FBI admitted to conducting surveillance flights over Ferguson and Baltimore during protests of police use of force, and that the Department of Homeland Security has reportedly surveilled protests by

---

[15] Simon Denyer, "China's watchful eye," *The Washington Post*, Jan. 7, 2018, https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance.
[16] *Ibid.*
[17] *NAACP v. Alabama* (1958) 357 U.S. 449; *Talley v. California* (1960) 362 U.S. 60.
[18] *Laird v. Tatum* (1972) 408 U.S. 1.
[19] E.g. *Donohoe v. Duling* (1972) 465 F.2d 196,202; *Phila. Yearly Meeting of Religious Soc'y of Friends v. Tate* (1975) 519 F.2d 1335, 1137-38.

Black Lives Matter, an activist group focused on police brutality and discrimination.[20] This makes clear that the broad application of FRT to surveil political demonstrations could be particularly problematic. A 2011 Privacy Impact Assessment by the Department of Homeland Security, the FBI, and several state police agencies, in discussing the capacity for FRT to compromise anonymity in a manner inconsistent with the First Amendment, explicitly recognized that "surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition."[21]

7) **Bias concerns with FRT**: Extensive research has determined the presence of biases in various forms of artificial intelligence, and recent reports indicate that FRT is no exception.[22] Studies have reported order-of-magnitude elevations in false positive rates (i.e. the number of images determined incorrectly to match an image in a database) for Asian vs. Caucasian faces and for African American vs. Caucasian faces. Additionally, those same studies reported lower false negative rates (i.e. the number of times an image did not matched to an image of the same individual that existed in a database) for African American vs. Caucasian faces.[23] These racial disparities in FRT performance could have resounding implications for racially biased law enforcement, particularly given the direction of the effects. For instance, if FRT is relied on for identifying criminal suspects from images, higher false positive rates and lower false negative rates for African American faces are likely to lead disproportionately to unwarranted investigation and arrest of African American individuals, who are already subjected to this form of discrimination. In other words, the biases existing in FRT have the potential to exacerbate and legitimize existing racial discrimination.

   Despite substantial increases in overall accuracy in the past several years, a 2019 report published by the National Institute of Standards and Technology reaffirmed the prevalence of problematic biases in commercially available FRT algorithms.[24] The report detailed the performance of 126 FRT verification algorithms in matching 442,019 images from 24 countries with a database of 441,517 different individuals from the same countries. The report identified several problematic biases in commercially available FRT algorithms, including highest false positive rates for West and East African and East Asian faces, and lowest false positive rates for Eastern European faces. The report noted, however, that several of the algorithms developed in China reversed this effect, with East Asian faces showing the lowest false positive rates. The report also found higher false positive rates for women relative to men, and in the elderly and children compared with middle-aged adults. While the report encouragingly demonstrated that the most accurate algorithms were also the least biased between demographic groups, these results are nonetheless cause for concern, as consequences of their shortcomings seem to weigh most heavily on demographic groups

---

[20] Eric Tucker, "Comey: FBI used aerial surveillance above Ferguson," *Associated Press,* Oct. 22, 2015, http://www.salon.com/2015/10/22/comey_fbi_used_aerial_surveillance_above_ferguson; George Joseph, "Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson," *The Intercept*, Jun. 24, 2015, https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson.

[21] The International Justice and Public Safety Network, "Privacy Impact Assessment: Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field," Jun. 30, 2011, p. 016632.

[22] "The Perpetual Line-Up," *supra* at fn. 4.

[23] Phillips et al., *An Other-Race Effect for Face Recognition Algorithms*, 8 ACM Transactions on Applied Perception, 14:1, 14:5 (2011).

[24] "FRVT: Part 3," *supra* at fn. 5.

already most vulnerable to discrimination. The perception that automated technology is entirely objective in its performance, even in the face of documented evidence to the contrary, makes these demographic disparities more concerning, as the inequities inherent in the technology can be easily overlooked.

8) **AB 2261 seeks to balance the applications of FRT against these salient concerns**: Policy approaches to the rapid proliferation of FRT have ranged from complete bans of the technology to the complete absence of regulation. Some local governments in California have implemented bans on the use of the technology by law enforcement, but the state as a whole lacks specific regulations for its use. This bill appears to strike a middle ground between these regulatory approaches by permitting, but severely limiting, the use of FRT. Notably, this bill would be the first in the country to comprehensively regulate the use of FRT across both public and private sectors. The bill does not require the use of FRT, nor does the bill as proposed to be amended, prohibit local governments from banning the technology within their jurisdictions. As such, it does not appear to encourage expansion of this technology, but instead seems to put in place reasonable restrictions, consistent with the recent legislative push to expand the data privacy rights of Californians, that are likely to limit its use and provide additional transparency.

   The bill consists of a host of provisions seeking to address particular shortcomings of FRT, including bias, privacy, and civil liberties concerns, by requiring bias and accuracy evaluations and accountability reports, subjecting enrollment in FRT databases and disclosure of facial information to the affirmative consent of the subject, requiring meaningful human review by trained operators for the use of FRT to inform decisions with legal or similarly significant consequences, and permitting the use of FRT for security and law enforcement purposes only in the most severe of circumstances, i.e. when there is probable cause to suspect that a serious criminal offense has been attempted or committed.

   The bill also institutes limitations on the retention of such information, and provides individual rights similar to CCPA to request confirmation of enrollment, request deletion of enrolled facial information, and contest or correct enrollments made on the basis of security or safety. In addition to general limitations the bill places on both public and private entities employing FRT, the bill adds specific obligations relating the use of FRT by public agencies, including law enforcement, recognizing the unsettling threat of state surveillance. These include regular audits for compliance, documentation and reporting of warrants permitting the use of FRT for ongoing surveillance in the very limited circumstances in which it is permitted, and requiring agencies to produce detailed accountability reports outlining the nature of the FRT being employed and its specific uses.

   The author appears to have struck a difficult balance by providing extensive protections against the unauthorized use of FRT, while still practically considering and permitting its ever-expanding applications.

9) **Author's amendments**: The author has worked extensively with Committee staff and stakeholders to craft amendments that strengthen considerations for privacy and civil liberties and address workability concerns expressed by industry and agency representatives. The amendments agreed upon are reflected below.

   - <u>Incorporating agencies into the definitions of "controller" and "processor"</u>: The bill in print excludes public agencies from the definitions of "controller" and "processor."

However, the provisions affecting public and private entities in the bill in print were extremely similar, and private entities were not subject to any provisions that were not also applied to public entities elsewhere in the bill. To improve clarity, reduce confusion, and harmonize provisions that apply to both public and private entities, the author has elected to amend the definitions of "controller" and "processor" to include agencies in addition to natural and legal persons. Note: some provisions in the bill, both in print and as proposed to be amended, apply only to public but not private entities.

- On page 4, in line 7, strike out "(1)"; on page 4, strike out line 10; on page 4, in line 7, strike out "the" and insert: "***an agency or***"
- On page 5, in line 22, strike out "(1)"; on page 5, strike out line 24; on page 5, in line 22, strike out "a" and insert: **"*an agency or***"
- On page 13, strike out lines 3 to 33, inclusive. On page 14, strike out lines 35 to 37, inclusive.

- Including "data representing facial features" in the definitions of "facial recognition service" and "facial template": The bill in print defines "facial recognition service" to mean technology that analyzes facial features and is used for recognition or persistent tracking of individuals in still or video images. It also defines "facial template" to mean the machine-interpretable pattern of facial features that is extracted from one or more images of an individual by a facial recognition service. Both of these definitions are predicated on patterns of facial features. In practice, however, facial features are often stored or analyzed in numerical forms that do not necessarily map directly to specific features of the face (e.g. distance between eyes, nose length, etc.). Rather, facial features are represented in complex variables that are derived computationally from combinations of facial measurements in order to extract the information most effective at differentiating faces (i.e. principal components). Consequently, though these data represent facial features, they are not necessarily, in and of themselves, facial features due to the computational processing they undergo. To ensure that this practice does not disqualify a facial recognition service from these definitions, "data representing facial features" was added into both.

  - On page 4, in line 18, strike out "features" and insert: ***"features, or data representing facial features,"***
  - On page 4, in line 21, strike out "features" and insert: ***"features, or data representing facial features,"***

- Exclude automated face-redacting software from the definition of "facial recognition service": Security industry stakeholders who provide technology to law enforcement agencies pointed out that law enforcement agencies often use automated or semi-automated processes in order to redact faces from recordings for release or disclosure in order to protect the privacy of the individual depicted. For example, a video of a crime may need to be released outside of law enforcement, and to protect the privacy of bystanders, their faces may need to be redacted. Rather than manually redacting each face, software exists that will automatically identify faces in the frame to redact, and will continue to redact that same face even if it leaves and subsequently reenters the frame. Importantly, this process typically does not generate or collect and retain any biometric

data or surveillance information. To avoid impeding this practice, which is generally privacy protective, the author has expressly exempted such processes.

- On page 4, between lines 19 and 20, insert: **"*(2) "Facial recognition service" does not include the use of an automated or semiautomated process for the purpose of redacting a recording for release or disclosure outside of a 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 data or surveillance information."***

- Strengthen the involvement of the individual in the definition of "meaningful human review": The bill in print defines "meaningful human review" to mean review or oversight by one or more individuals who are trained…and who have the authority to alter the decision under review. This definition's passive role for the human reviewer as more or less a rubber stamp on the decision made by the system could minimize the rigor of this review, particularly in light of the common misperception that automated decision systems make reasonable, objective decisions in the absence of a system malfunction. Considering the importance of legal and similarly significant decisions, this passive oversight role for the human reviewer seems insufficient to properly vet the information extracted from a facial recognition system. To resolve this issue, the author has instead required that the human reviewer be responsible for making, rather than simply verifying, the ultimate decision based on the output of the service.

  - On page 4, in line 29, strike out "have the authority to alter the decision under", strike out line 30 and insert: "***are ultimately responsible for making decisions based, in whole or in part, on the output of a facial recognition service."***

- Include tracking without identifying an individual in the definitions of "ongoing surveillance" and "persistent tracking": Definitions of "ongoing surveillance" and "persistent tracking" relate to the tracking of physical movements of individuals over time in real time or via historical records using a facial recognition service. The bill in print specifies that "ongoing surveillance" does not include a single recognition or attempted recognition of an individual if no attempt is made to subsequently track that individual's movement over time ***after that individual has been recognized***, meaning the individual can be tracked before being recognized without constituting ongoing surveillance and being subject to the associated requirements. The definition of "persistent tracking" used qualifies that it involves tracking the movements of an individual on a persistent basis ***without using the facial recognition service for recognition of that individual***. Removing these qualifiers expands these definitions to subject these invasive practices to additional scrutiny and limitations. Accordingly, the author has proposed amendments to remove these qualifiers.

  - On page 4, in line 37, strike out "time after that", strike out line 8 and insert: ***"time"***

  - On page 5, in line 1, strike out "basis without using", strike out line 2 and insert**: "basis,"**

- Require that a "security or safety purpose," which confers specific exceptions to consent requirements, involve an *immediate* purpose related to safety and security: Nearly any

enrollment in an FRS can be justified as constituting a "security or safety purpose" if there is no requirement for immediacy – e.g. the possibility that a given individual could eventually need to be identified in the future due to potential involvement in or adjacency to a crime, the fact that an individual plans to fly on an airplane, etc.. As has been demonstrated time and time again around the world, "national security" has been used as a justification for far-reaching suspensions of civil liberties, whether or not that security claim is justified, sufficiently narrow, and appropriately related. Without requiring immediacy to confer limited exceptions to consent requirements provided in this bill, the "security or safety purpose" provisions could render many of the protections for privacy and civil liberties provided by this bill inapplicable in most or all circumstances.

- *On page 5, in line 31, strike out "a" and* insert: ***"an immediate"***

- Clarify that a processor may satisfy FRS testing requirements by submitting algorithms to the National Institute of Standards and Technology (NIST): Several stakeholders pointed out that NIST performs highly rigorous, methodologically consistent testing of face recognition algorithms to assess accuracy and bias in a manner consistent with the requirements of this bill. Indeed, the results of these tests are cited repeatedly in this analysis. Since many processors already voluntarily submit their algorithms for assessment by NIST, permitting these evaluations to fulfill this requirement both ensures the quality of the independent assessment, and reduces the burden on processors to perform an additional assessment. Additionally, stakeholders requested clarification that the evaluation requirements for these algorithms does not require a processor to disclose protected intellectual property.

  - On page 6, between lines 12 and 13, insert: ***"(B) A processor may satisfy the requirements of this subdivision by submitting deployed algorithms to each relevant Face Recognition Vendor Test that the National Institute of Standards and Technology (NIST) performs, including, but not limited to, overall accuracy and demographic specific tests.***

    (C) This subdivision does not require a processor to disclose trade secrets or other intellectual property."

- Prohibit controllers from denying access or service to an individual for exercising their right to withhold consent for enrollment using an FRS: The intent of this bill is to require informed, affirmative consent in order to enroll an individual in an FRS. If withholding consent results in the denial of access or service to a physical premise open to the public, social pressures and particular needs may coerce individuals into "consenting" to enrollment against their will. To avoid these circumstances, the author has added amendments that prohibit controllers from denying access or services on the basis of exercising the right to withhold consent, except under specified circumstances.

  - On page 7, between lines 12 and 13, insert: **"*(2) Except as provided in paragraph (3), a controller shall not deny access or service to an individual at a physical premise open to the public because that individual has exercised the right to withhold consent for enrolling an image or facial template of that individual in a facial recognition service pursuant to paragraph (1).***

(3) A controller may deny service to an individual at a physical premise open to the public because that individual has exercised the individual's right to withhold consent for enrolling an image or facial template of that individual in a facial recognition service pursuant to paragraph (1) if enrollment of that image or facial template is directly necessary for the provision of that service."

- Raise the burden of proof for the use of an FRS for a security or safety purpose from a reasonable suspicion of criminal activity to probable cause to suspect that a person has committed, or attempted to commit, a serious criminal offense: In an attempt to strike the appropriate balance between the utility and the sensitivity of facial recognition technology, and to harmonize the burden of proof with similarly sensitive surveillance technologies such as wiretaps and tracking which require probable cause warrants, the proposed amendments limit the non-consensual enrollment in an FRS to circumstances in which there is probable cause to suspect a serious criminal offense, as defined. Raising the threshold for enrollment will likely help to limit potentially discriminatory or injudicious use of FRSs, and may further protect against the possibility of an FRS misidentifying an innocent person as a suspect. Additionally, since a controller cannot justifiably enroll an image or facial template without consent or probable cause, the proposed amendments require a controller to remove the image or facial template as soon as the controller no longer has probable cause of a serious criminal offense.

  - On page 7, in lines 17 and 18, strike out "holds a reasonable suspicion, based on a specific incident," and insert: ***"has probable cause to believe"***

  - On page 7, in line 18, strike out "engaged in criminal", strike out line 19 and insert: ***"committed, or attempted to commit, a serious criminal offense"***

  - On page 7, between lines 24 and 25, insert: ***"(C) The controller removes the image or facial template as soon as the controller no longer has probable cause to believe the individual has committed, or has attempted to commit, a serious criminal offense."***

  - On page 7, in line 28, strike out "holds a reasonable suspicion" and insert*:* ***"has probable cause to believe"***

  - On page 7, in line 29, strike out "engaged in", strike out line 30 and insert: ***"committed, or attempted to commit, a serious criminal offense"***

  - On page 14, in line 21, strike out "holds a reasonable suspicion that that" and insert: ***"has probable cause to believe the"***

  - On page 14, in line 32, strike out "reasonable suspicion" and insert: ***"probable cause"***

- Subject decisions that have a negative impact on the civil rights of individuals to meaningful human review: This amendment clarifies that negative impacts on civil rights constitute "legal effects" and "similarly significant effects" on par with denial of access to basic necessities and consequential services or support. This amendment also makes non-substantive changes to the language.

- On page 8, in line 2, strike out "denial of", strike out lines 3 to 6, inclusive, and insert: ***"all of the following:***

  (A) Denial of consequential services or support, including financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services.

  (B) Denial of access to basic necessities.

  (C) Negative impact on civil rights of individuals."

- Specify that training for the operation of an FRS must be conducted at least annually:

  - On page 8, in lines 13 and 14, strike out "conduct periodic" and insert: ***"conduct, at least, annual"***

- Require consent to disclose personal data obtained from an FRS to any person or agency, rather than only law enforcement: CCPA, the standard bearer for privacy protection in California, provides consumers with the right to opt out of the disclosure of their personal information. The author has indicated that due to the particular sensitivity of FRS data, the additional protections provided by this bill are essential, including the requirement for affirmative consent. The bill in print requires consent for the disclosure of FRS data by a controller to law enforcement. To make this provision appropriately appreciative of the sensitivity of this data, the author has expanded this consent requirement for disclosure to apply regardless of the identity of the recipient. According to the author, this amendment was intended to tighten potential loopholes and to ensure the protection of individual liberties against the abuse of this technology by private, as well as public, actors. Indeed, if the protections against sharing this information only applied when sharing with law enforcement, for instance, information obtained using an FRS could be disclosed to a private intermediary without meeting the criteria, and that intermediary could then pass that information along to law enforcement, since it was not directly extracted from FRS.

  Additionally, though invasive public use of an FRS is a central concern, invasive private uses are equally concerning, especially when considering the fact that private entities often contract with law enforcement or share information (for compensation or otherwise) with other private entities. Fundamentally, the civil liberties and privacy considerations are similar whether a pervasive FRS database is compiled by law enforcement or by a private entity. A corporation obtaining facial information from a data broker to track consumers is as much an invasion of personal privacy as the same practice by law enforcement.

  This amendment also stipulates that consent to disclose for the purposes of this provision does not include consent that is required for the provision of a service. Since some services may require the enrollment of facial information, this amendment would prevent such a service from being denied on the basis that the individual does not *also* consent to the disclosure of that information, provided disclosure is not also necessary for the service. For instance, an application that identifies one's celebrity doppelganger based on their facial information may require facial information to be used, but could not, pursuant to this amendment, require consent for disclosure as well in order to provide the service.

  On page 8, in line 27, strike out "law enforcement" and insert: ***"person or"***

On page 8, in line 28, strike out "are" and insert*: **"is"***

On page 8, in line 30, strike out "relates." and insert*: **"relates, and, except as provided in subparagraph (B), consent to share the data was not a requirement for the provision of a service.***

(B) A controller may disclose personal data obtained from a facial recognition service to a person or agency if the disclosure is directly necessary for the provision of a service."

- Exempt from the consent requirement for disclosure sharing of personal data between a controller and processor in specified circumstances: Stakeholders pointed out that in order to operationalize certain aspects of an FRS, including any type of cloud based processing, a disclosure must necessarily be made between a controller and processor. To mitigate the impediment to function the consent requirement would have imposed in these circumstances, the author has proposed to amend the bill to exempt those disclosures from that requirement, so long as certain protections are in place for that personal information.

  - On page 8, below line 40, insert: ***"(5) The disclosure is made between a controller and a processor to provide a facial recognition service, including the processing of personal data pursuant to that service, so long as the engagement is governed by a contract between the controller and the processor that is binding on the processor and that sets out the mandatory processing instructions to which the processor is bound, including the obligations imposed by this paragraph."***

- Clarify that the individual has the right to withdraw consent to enroll an image or facial template of that individual in an FRS used in a physical premise open to the public *at any time:*

  - On page 9, in line 16, strike out "withdraw" and insert: ***"withdraw, at any time,"***

- Provide that a controller that fails to demonstrate that a refused request is manifestly unfounded or excessive is liable for court costs and reasonable attorney fees: The bill in print permits a controller that receives an unreasonable or excessive request to confirm if an individual's facial information is enrolled, delete enrolled facial information, or correct or contest enrolled facial information, to either charge a reasonable fee to cover the administrative costs of complying with the request, or to refuse to act on the request. In either case, the ability to exercise this right would be limited by the good faith of the controller, and by the financial resources of the consumer, as a consumer who cannot afford the fee, who is being charged a fee inappropriately, or who lacks the resources to litigate the fee or the refusal would have no recourse.

  This bill aims to provide protections for certain critical civil liberties, and as such, should not depend on the financial well-being of, or legal resources available to, an individual. Though the bill in print places the burden on the controller to demonstrate that a request is manifestly unfounded or excessive, in reality, such a burden would be impractical if the individual could not litigate the designation in the first place. Holding the controller liable for court costs and reasonable attorneys' fees in the event the request is not found

to be unfounded or excessive would level the playing field between consumers and controllers, as without this protection, a controller with more extensive legal and financial resources could simply deem every request manifestly unfounded or excessive, and that designation would rarely, if ever, be litigated to determine the legitimacy of that claim. Accordingly, the author has agreed to amend the bill to provide for reasonable attorneys' fees and court costs to be recouped by the individual in the even they prevail in contesting a refusal to comply.

On page 10, between lines 3 and 4, insert: ***"(B) A controller refusing to comply with a request pursuant to subparagraph (A) shall bear the burden of demonstrating that a request is manifestly unfounded or excessive.***

(C) If the controller fails to demonstrate that a refused request is manifestly unfounded or excessive pursuant to subparagraph (B), the individual making the request shall be entitled to recovery of court costs and reasonable attorney fees from the controller."

On page 10, strike out lines 11 to 16, inclusive.

- Permit a controller to refuse to comply with a request to exercise rights if the controller is unable to determine using reasonable, rather than "commercially reasonable", efforts, the authenticity of the requeste:

  - On page 10, in line 5, strike out "commercially".

- Use existing Department of Justice processes to document warrants permitting ongoing surveillance using an FRS, rather than requiring judges to maintain this information: The bill in print requires a judge who has issued a warrant for ongoing surveillance to report specific information relating to that warrant to the Supreme Court of California. This would likely be costly, and would place an unnecessary burden on judges issuing these warrants. The Department of Justice currently compiles documentation and reports on executed surveillance warrants, and associated information, under existing law pursuant to the California Electronic Communications Privacy Act (CalECPA). To facilitate record-keeping relating to ongoing surveillance warrants using FRSs, the author has, in consultation with the Attorney General's Office, crafted proposed amendments to utilize this existing process of documenting warrants and informing the subjects of those warrants that surveillance was carried out. (Amendment included with subsequent bullet.)

- Require biennial audits by the nonpartisan California State Auditor of agencies deploying FRSs to evaluate compliance with the provisions of the bill: Though the bill confers sole enforcement authority on the Attorney General, additional oversight may be necessary to ensure that all agencies employing FRSs are doing so in accordance with the comprehensive requirements of this bill. Furthermore, many agencies are responsive to or under the purview of the Attorney General and the Department of Justice. To assure the public that oversight of any use of FRSs by these agencies is performed by an independent body, the author has proposed amendments to place the responsibility of regular compliance audits on the State Auditor.

- On page 15, strike out lines 3 to 17 inclusive, and insert: ***"(b)(1) Within 10 calendar days after the period of ongoing surveillance authorized by a warrant has ended, the officer who executed the warrant shall submit to the Department of Justice all information required by subdivision (a) of Section 1546.2 of the Penal Code.***

  (2) If an order delaying notice is obtained pursuant to subdivision (b) of Section 1546.2 of the Penal Code, the government entity shall submit to the department upon the expiration of the period of delay of the notification all of the information required in paragraph (3) of subdivision (b) of Section 1546.2 of the Penal Code.

  (3) The department shall publish all those reports on its internet website within 90 days of receipt and may redact names or other personal identifying information from the reports.

  (c)(1) Within 10 calendar days after the period of ongoing surveillance authorized by a warrant has ended, the officer who executed the warrant shall notify the person who was tracked pursuant to subdivision (a) of Section 1546.2 of the Penal Code.

  (2) Notice pursuant to this subdivision may be delayed pursuant to subdivision (b) of Section 1546.2 of the Penal Code.

  1798.370. (a) On or before January 1, 2023, and at least biennially thereafter, the nonpartisan California State Auditor shall conduct an independent audit of agencies deploying facial recognition services to evaluate compliance with the provisions of this title.

  (b) Based on the independent audit performed pursuant to subdivision (a), the nonpartisan California State Auditor shall prepare a report detailing its review and shall include in that report any violations of the provisions of this title, as well as any recommendations for improvements to state and local policies on the use of facial recognition services by agencies.

  (c)(1) The report prepared pursuant to subdivision (b) shall be made available to the public and shall be posted on the internet websites of the State Auditor and of the Attorney General.

  (2) A copy of the report prepared pursuant to subdivision (b) shall be distributed to the Assembly Committee on the Judiciary, the Assembly Committee on Public Safety, the Assembly Committee on Privacy and Consumer Protection, the Senate Committee on the Judiciary, and the Senate Committee on Public Safety."

- Remove provision preempting any local measures regarding the development, use, or deployment of FRSs: The bill in print provides that this bill supersedes and preempts laws, ordinances, regulations, or the equivalent adopted by any local entity regarding the development, use, or deployment of facial recognition services. Several localities in California have already adopted bans on the use of FRSs by law enforcement, including Oakland, Berkeley, and San Francisco.

  It is this Committee's view that local jurisdictions are likely to be most in touch with how facial recognition technology is being used in their communities, and are in the best position to effectively evaluate how their community is being served by its use.

Individuals interact most frequently with local governments and local businesses. It is thus reasonable that rules governing use by those entities should be responsive to the needs of their constituents, so long as that response does not compromise their privacy or civil liberties. It is not difficult to see how even limited use of facial recognition technology could be more problematic in some communities than others (e.g. communities with large socioeconomic disparities, large populations of homeless individuals, etc.). This bill effectively provides baseline protections for individuals from the abuse of facial recognition technology, but further regulation may be necessary depending on local circumstances. While the provisions of this bill would apply across the state, the author has agreed to amend the bill remove the preemption of local measures, should a local government opt to expand on these protections.

On page 15, strike out lines 30 to 32, inclusive.

- Make several technical and non-substantive changes:

10) **Arguments in support**: In support of the bill, Microsoft argues:

AB 2261 is a thoughtful approach which recognizes the need for safeguards to balance the opportunities and the risks associated with facial recognition technology.[…] The California legislature has an opportunity to establish appropriate standards for the use of facial recognition technology. Microsoft firmly believes that government must act and determine what regulations will permit the use of facial recognition technology to provide society with a whole host of benefits, while also addressing the challenges that facial recognition technology poses – challenges that go to the heart of fundament human rights protections like privacy, freedom of expression, and freedom of association. Those challenges call for a thoughtful discussion including all stakeholders across society. We appreciate that you are continuing to have conversations with stakeholders to improve and refine the bill.

11) **Arguments in opposition**: A coalition of over 40 civil rights organizations, including ACLU California, the Electronic Frontier Foundation, the Ella Baker Center for Human Rights, the California Immigrant Policy Center, and the Center for American-Islamic Relations (CAIR) California, argues:

As advocates working closely with people most acutely impacted by this unprecedented pandemic – people of color, individuals who are incarcerated or in ICE custody, people experiencing homelessness, and workers, among others – we are witnessing firsthand how the disproportionate harms marginalized communities face every day are exacerbated during moments of crisis. It is therefore more critical than ever that California adopt appropriate measures to protect communities from discriminatory and invasive measures, including face surveillance. AB 2261 will exacerbate the racial, gender, and socioeconomic inequities the pandemic has exposed and is not an effective response to our current public health crisis. In stark contrast, its endorsement of invasive surveillance threatens to divert money from vital public health resources precisely at a moment where we should be heavily investing in them. We should not be giving companies and governments a green light to use facial recognition to track individuals, deny economic opportunities, and further marginalize communities.

12) **Prior legislation**: AB 1281 (Chau, 2019) would have required any business that uses facial recognition technology in California to disclose that usage in a physical sign that is clear and

conspicuous at the entrance of every location. This bill was placed on the inactive file on the Senate Floor.

AB 1215 (Ting, Ch. 579, Stats. 2019) prohibits a law enforcement officer or agency from installing, activating, or using a biometric surveillance system in connection with a law enforcement agency's body-worn camera or any other camera.

AB 375 (Chau, Ch. 55, Stats. 2018) enacted the CCPA to ensure the privacy of Californians' personal information through various consumer rights.

SB 1121 (Dodd, Ch. 735, Stats. 2018) ensured that a private right of action 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

Microsoft Corporation

Oppose Unless Amended

Los Angeles Police Protective League

Oppose

ACLU of Northern California, Southern California, and San Diego and Imperial Counties
ACT for Women and Girls
Alliance San Diego
American Civil Liberties Union
Anti Police-Terror Project
Asian Americans Advancing Justice
California Immigrant Policy Center
California Innocence Coalition: Northern California Innocence Project, California Innocence Project, Loyola Project for the Innocent
California Public Defenders Association
California State Sheriffs' Association
Center for Public Interest Law, Children's Advocacy Institute, University of San Diego
Coalition of Civil Rights Organizations
Coalition on Homelessness, San Francisco
Color of Change
Consumer Federation of California
Data for Black Lives
Electronic Frontier Foundation
Ella Baker Center for Human Right
Ensuring Opportunity Campaign to End Poverty in Contra Costa
Fight for the Future

Freedom for Immigrants
Fresno Barrios Unidos
Hollywood Now
Ice Out of Marin
Immigrant Legal Resource Center
Indivisible CA Statestrong
Indivisible East Bay
Indivisible Los Gatos
Indivisible Sausalito
Indivisible SF
Indivisible South Bay LA
Inner City Struggle
Lawyers Committee for Civil Rights of The San Francisco Bay Area
Legal Aid At Work
Media Alliance
MediaJustice
National Lawyers Guild Los Angeles
Oakland Privacy
Organizing for Action Contra Costa
San Bernardino County Safety Employees' Benefit Association
NAACP – San Jose & Silicon Valley Chapters
Scholars Group
Secure Justice
Showing Up for Racial Justice, Marin
Siren Bay Area
South Bay People Power
Starting Over INC.
Students Deserve Justice
Tenth Amendment Center

Analysis Prepared by: Landon Klein / P. & C.P. / (916) 319-2200