A Californian Algorithm: Amending Assembly Bill 2261 to Regulate Law Enforcement's Use of Facial Recognition Technology in *Post Hoc* Criminal Investigations

A. Spencer Davies[*]

The use of facial recognition technology (FRT) is exploding across all sectors of society. From smartphones to government agencies, FRT systems are used on a daily basis to verify identity and to identify unknown people. As FRT use expands and the technology becomes more sophisticated, reliance on FRT-generated results becomes second nature. However, this reliance also creates concerns in the policing context, as several studies show FRT systems disproportionately misidentify women and racial and ethnic minorities as compared to white men. There is also concern that police will over-rely on FRT, which, in effect, could create a society subject to perpetual police surveillance.

In the last year, the federal government and some state governments have proposed bills to regulate FRT and address problems of misidentification. None of these proposals have been as robust and comprehensive as California Assembly Bill 2261, which sought to regulate both public and private FRT use. A.B. 2261 fell short, however, by only regulating law enforcement's use of FRT for "ongoing surveillance." Specifically, A.B. 2261 failed to address law enforcement's use of FRT in post hoc criminal investigations, where misidentification can lead to wrongful arrest and incarceration. In this context, "post hoc" is used to distinguish criminal investigations that

DOI: https://doi.org/10.15779/Z38SB3X03N

[*] Associate, Moore & Van Allen PLLC, Charlotte, NC; J.D., 2021, Vanderbilt University Law School. The author thanks the members of the Berkeley Journal of Criminal Law for their suggestions and edits during the publishing process. He also thanks Professor Nancy J. King, Vanderbilt University Law School, for her guidance and thoughtful input during the writing process.

occur after a crime has been committed and a perpetrator remains at large from those that prevent a threatened crime from ever occurring. In post hoc investigations, police sometimes upload a low-quality, unconstrained "probe" photo to an FRT system to identify unknown criminals. Unfortunately, these low-quality probe photos inherently increase the risk of misidentification.

By failing to address FRT use in post hoc criminal investigations, A.B. 2261 (along with every other federal and state proposal preceding it) failed to directly address concerns of discriminatory policing. This Article proposes an amendment to A.B. 2261 to condition law enforcement's use of FRT by requiring an independent agency of forensic facial reviewers to assess probe photo quality. This process would ensure that low-quality probe photos prone to generating incorrect matches would not be used in FRT systems and therefore could not be used for identification purposes. Not only would this amendment limit law enforcement's power to unilaterally generate FRT matches, but it could help prevent disproportionate misidentifications while still permitting law enforcement's use of important investigative techniques.

INTRODUCTION

In October 2018, five watches were stolen from an upscale boutique in Detroit, Michigan.[1] From an evidentiary standpoint, the police considered a photo from the store's surveillance video to be their most vital asset. That photo showed an unknown African American man dressed in black clothing and wearing a red St. Louis Cardinals baseball cap.[2] The hat obscured the man's face and the image's quality was poor. In a final attempt to identify the unknown perpetrator, the police disregarded the photo's limitations and uploaded the image to DataWorks Plus, the Detroit Police Department's facial recognition technology system.[3] DataWorks Plus generated a match, identifying Robert Julian-Borchak Williams as the thief.[4] The boutique's security guard corroborated the match,[5] and Mr. Williams was arrested.[6] Ostensibly, the case was closed. However, the man in the surveillance photo was not Mr. Williams. The facial recognition software generated a false positive that led to Mr. Williams's wrongful arrest for a crime he did not commit.[7]

Mr. Williams is considered the first American wrongfully arrested

[1] Kashmir Hill, *Wrongfully Accused by An Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] Brian Fung & Rachel Metz, *This May Be America's First Known Wrongful Arrest Involving Facial Recognition*, CNN (June 24, 2020, 5:13 PM), https://www.cnn.com/2020/06/24/tech/aclu-mistaken-facial-recognition/index.html. Interestingly, the store's security guard was not a firsthand witness to the robbery; their only "witnessing event" was watching the surveillance video that provided the original probe photo. *Id.*

[6] Hill, *supra* note 1. Williams was also held in custody for 30 hours.

[7] *Id.* Following Mr. Williams's false arrest, the Wayne County, Michigan, prosecutor's office expunged Mr. Williams's fingerprint data, acknowledging that this could not make up for the emotional and reputational damage inflicted on Mr. Williams. Fung & Metz, *supra* note 5.

on the basis of a false facial recognition technology (FRT) match, and his case highlights issues that can arise when law enforcement officers upload low-quality photos to FRT systems during "*post hoc*" criminal investigations.[8] In this Article, *post hoc* is used to describe criminal investigations that occur after a crime has been committed and a suspect remains at large, as distinguished from criminal investigations that prevent a crime from ever occurring. Regardless of the context in which FRT is used, the primary issue is that such systems can disproportionately misidentify women, people with darker complexions, and transgender and non-binary individuals.[9] These demographic-based discrepancies can be significant and are largely caused by two factors: (1) training FRT algorithms with majority white male faces[10] and (2) suboptimal photo quality.[11] A MIT study found that three FRT algorithms never had higher than a 0.8% error rate when analyzing light-skinned men's faces, but up to a 46.8% error rate when analyzing darker-skinned women's faces.[12] A similar study conducted by the University of Colorado-Boulder found that transgender men were incorrectly identified as women 38% of the time and non-binary individuals were misclassified 100% of the time.[13]

[8] REUTERS, *Facial Recognition Leads to First Wrongful U.S. Arrest, Activists Say*, NBC NEWS (last updated June 24, 2020, 2:10 PM), https://www.nbcnews.com/tech/security/facial-recognition-leads-first-wrongful-u-s-arrests-activists-say-n1231971.

[9] Emma Lux, *Facing the Future: Facial Recognition Technology Under the Confrontation Clause*, 57 AM. CRIM. L. REV. ONLINE 20, 23 (2020); Jesse Damiani, *New Research Reveals Facial Recognition Software Misclassifies Transgender, Non-Binary People*, FORBES (Oct. 10, 2019, 3:21 PM), https://www.forbes.com/sites/jessedamiani/2019/10/29/new-research-reveals-facial-recognition-software-misclassifies-transgender-non-binary-people/?sh=449c70bc606b.

[10] Studies suggest that FRT algorithms disproportionately misidentify women and people with darker complexions because such algorithms are "taught" how to identify biometric similarities by databases that are predominately White and male. These studies suggest that the misidentification rates for minorities can be reduced if the initial training sets are more diverse and representative of the general public. *See* Alex Najibi, *Racial Discrimination in Face Recognition Technology*, HARV. UNIV. GRADUATE SCH. OF ARTS & SCI.: SCI. POL'Y & SOC. JUST. BLOG (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

[11] *See id.* ("Default camera settings are often not optimized to capture darker skin tones, resulting in lower-quality database images of Black Americans.").

[12] Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems*, MIT NEWS (Feb. 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

[13] Damiani, *supra* note 9. Non-binary individuals were allegedly misclassified because that gender identity had not been built into the FRT algorithms. *Id.*

Because law enforcement agencies often use FRT systems in their post hoc criminal investigations, in which the consequences for a suspect can include incarceration, it is important that regulations reduce the likelihood that the technology will disproportionately impact historically marginalized groups.[14] This can largely be achieved through compulsory quality assessments of "probe" photos, which are photographs collected during "routine investigative activity, including mugshots, surveillance photos, social media posts, and images confiscated from phones or other data devices."[15]

FRT opponents argue that unregulated, unlimited FRT use threatens individual privacy rights and augurs perpetual police surveillance.[16] In Florida, the Pinellas County Sheriff's Office uses a FRT system[17] populated with over 30 million images scraped from databases of driver's license images, mug shots, and photos from juvenile bookings.[18] The Pinellas County database indicates that FRT systems host vast libraries of photos from disparate sources. Perhaps, then, it is unsurprising that over half of American adults' faces are stored in a FRT database—over 117 million people.[19] FRT databases are also vulnerable

[14] This is especially true considering the current protests around the country against systemic racism in policing. *See* Zack Beauchamp, *What the Police Really Believe*, VOX (July 7, 2020, 8:10 AM), https://www.vox.com/policy-and-politics/2020/7/7/21293259/police-racism-violence-ideology-george-floyd. If law enforcement uses FRT systems that negatively impact historically marginalized groups, the public will further resent police.

[15] U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE ICE USE OF FACIAL RECOGNITION SERVICES 6 (May 13, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf.

[16] *See generally* Katelyn Ringrose, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns*, 105 VA. L. REV. ONLINE 57 (2019) (examining the privacy issues associated with FRT-enabled officer-worn body cameras); Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591 (2017) (arguing that real-time use of facial recognition technology violates the reasonable expectations of privacy protected under the Fourth Amendment).

[17] This system is called the Face Analysis Comparison and Examination System (FACES). Malena Carollo, *National Moves Against Facial Recognition Won't Mean Much in Tampa Bay Area*, TAMPA BAY TIMES (June 26, 2020), https://www.tampabay.com/news/business/2020/06/26/national-moves-against-facial-recognition-wont-mean-much-in-tampa-bay-area/.

[18] Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

[19] Sam Levin, *Half of US Adults Are Recorded in Police Facial Recognition Databases, Study Says*, THE GUARDIAN (Oct. 18, 2016, 4:43 PM),

to hacking by malicious third parties seeking to use stored photos for fraudulent purposes.[20] Further, in the absence of substantive FRT regulations at both the federal and state levels, opponents worry that a lack of oversight and public transparency will permit law enforcement to perpetually track our everyday movements.[21] These opponents argue that regulation is required to prevent law enforcement's misuse of powerful and flawed FRT. To build trust with the public, a comprehensive FRT regulation should therefore not only address photo quality but also place explicit limits on law enforcement's FRT use.[22]

Proponents of FRT, including law enforcement agencies themselves, contend that FRT generates unique investigative leads for various crimes.[23] These leads are increasingly important in modern times, as digital videos and photos comprise a substantial portion of all criminal evidence.[24] Because FRT is designed to quickly evaluate digital evidence, it serves an essential role in *post hoc* criminal investigations. FRT's investigative efficiencies have also gained public attention. In a recent PEW study, 56% of Americans said they trust law enforcement to use FRT responsibly, and 59% of Americans agree that law enforcement should have access to FRT to address public security threats.[25] Proponents also argue that, absent corroborating evidence, FRT-

https://www.theguardian.com/world/2016/oct/18/police-facial-recognition-database-surveillance-profiling.

[20] *See* Mike Snider, *Clearview AI, Which Has Facial Recognition Database of 3 Billion Images, Faces Data Theft*, USA TODAY (Feb. 26, 2020, 4:34 PM), https://www.usatoday.com/story/tech/2020/02/26/clearview-ai-data-theft-stokes-privacy-concerns-facial-recognition/4883352002/.

[21] *See generally* Sam DuPont, *Without Legal Safeguards, Facial Recognition Is Here But We Have No Laws*, NEXTGOV (July 8, 2020), https://www.nextgov.com/ideas/2020/07/facial-recognition-here-we-have-no-laws/166711/.

[22] There are thorough academic and policy discussions about FRT's effects on privacy. These discussions are largely outside the scope of this Article and will not be analyzed in detail.

[23] *See* James Andrew Lewis, *Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape*, CTR. FOR STRATEGIC & INT'L STUD. (Sept. 29, 2021), https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape.

[24] NEC America, *How Criminal Investigations Can Be Expedited Using Facial Recognition*, YOUTUBE (Nov. 1, 2018), https://www.youtube.com/watch?v=FmETjl4fREg.

[25] Aaron Smith, *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, PEW RSCH. CTR. (Sept. 5, 2019), https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/.

generated matches are never dispositive grounds for an arrest.[26] Instead, they claim FRT matches are solely used for investigative leads and for identification.[27]

Regardless of individual viewpoints, FRT's identifiable shortcomings require regulation at some level.[28] This Article builds off the California legislature's groundwork for robust regulation and proposes an amendment to the state's most recent FRT bill—Assembly Bill 2261—which died before enactment in November 2020.[29] The proposed amendment focuses on probe photo quality, which directly correlates with FRT accuracy. Although the amendment is specific to California's bill, it serves as a model for other states and the federal government. This Article is organized as follows: Part I describes how law enforcement currently uses FRT; Part II evaluates other regulatory proposals and explains why California is the best forum for enacting FRT regulations; Part III sets forth the proposed amendment, which conditions California state and local law enforcement's FRT use on compulsory *ex ante* probe photo quality assessments conducted by forensic facial reviewers; Part IV justifies the proposed amendment's strict requirements; Part V offers rebuttals to potential critiques of the proposed amendment; and lastly, a brief conclusion.

I. HOW LAW ENFORCEMENT USES FACIAL RECOGNITION TECHNOLOGY

Law enforcement agencies currently use FRT to achieve two

[26] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. ON PRIV. AND TECH. (May 16, 2019), https://www.flawedfacedata.com/ ("Most agencies do not yet consider face recognition to be a positive identification. Many law enforcement agencies, the NYPD included, state that the results of a face recognition search are possible matches only and must not be used as positive identification.").

[27] Valentino-DeVries, *supra* note 18. Note that there is evidence contradicting this claim that shows FRT matches are often used as the primary basis for arrest. *See generally* Garvie, *supra* note 26 (examining several cases where law enforcement agencies arrested individuals on the basis of FRT-generated matches and in the absence of substantial corroboration via other evidence).

[28] This is highlighted by the fact that the COVID-19 pandemic has accelerated the use of biometric data collection tools across the board. *See generally* Mia Sato, *The Pandemic is Testing the Limits of Face Recognition*, MIT TECH. REV. (Sept. 28, 2021), https://www.technologyreview.com/2021/09/28/1036279/pandemic-unemployment-government-face-recognition/.

[29] CAL. LEGIS. INFO., *AB-2261 Facial Recognition Technology: Status*, https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201920200AB2261 (last visited Dec. 28, 2021).

objectives: (1) verification, and (2) identification.[30] Verification produces one-to-one matches that ensure a person is who they say they are.[31] For example, during a routine traffic stop, a police officer may use a portable facial recognition system to compare the person's driver's license to a live photograph.[32] Verification methods typically have higher accuracy rates than other FRT procedures because the person can be positioned strategically in front of the camera, ensuring adequate lighting and angles.[33] Because verification systems return one-to-one matches, they are rarely used in *post hoc* investigations, during which law enforcement attempts to identify an unknown suspect.

Identification procedures, on the other hand, play a crucial role in *post hoc* criminal investigations. These methods produce one-to-*many* matches to identify unknown faces by comparing biometric facial measurements[34] in a probe photo to millions of photos stored in an FRT database.[35] In most cases, probe photos are "unconstrained," meaning they are derived from sources that cannot control image quality.[36] Surveillance cameras are the most common source of probe photos. Due to their unconstrained nature, probe photos have suboptimal image quality and generate lower accuracy rates than their verification counterparts.[37]

[30] William Crumpler, *How Accurate Are Facial Recognition Systems – and Why Does It Matter?*, CTR. FOR STRATEGIC & INT'L STUDIES STRATEGIC TECHS. BLOG (Apr. 14, 2020), https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter.

[31] *Id.*

[32] *See generally id.* Verification methods are also used to unlock smartphones and run airport security checks.

[33] *Id.*

[34] These measurements typically include the distance between one's eyes, the distance between one's eyes and the point of their chin, the distance between one's ears, and the distance between one's eyes and ears.

[35] Crumpler, *supra* note 30. Identification methods are deployed in various ways, including: (1) automatic recognition of people in an image (*i.e.*, Facebook identifying someone in a photograph for tagging purposes); (2) access to services; (3) tracking a passenger traveling over multiple jurisdictional lines; (4) searching for unidentified people; (5) monitoring an individual person's movements in public spaces; (6) reconstructing a person's journey by analyzing their historical movements; and (7) identification of wanted persons in public spaces. COMM'N NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, RECONNAISSANCE FACIALE – POUR UN DEBAT A LA HAUTEUR DES ENJEUX, *translated in* FACIAL RECOGNITION – FOR A DEBATE LIVING UP TO THE CHALLENGES (Nov. 15, 2019), https://www.cnil.fr/sites/default/files/atoms/files/facial-recognition.pdf (English translation version).

[36] U.S. DEP'T OF HOMELAND SEC., *supra* note 15, at 6.

[37] Crumpler, *supra* note 30; *Street-Level Surveillance: Face Recognition*, ELEC.

It is important that FRT regulations consider the increased probability that such procedures will generate misidentifications due to image quality.

II. A REGULATION BALANCING FRT'S PROS AND CONS CAN PREVENT LAW ENFORCEMENT AGENCIES FROM MISUSING THE TECHNOLOGY

Law enforcement's FRT use is mostly unregulated in the United States.[38] In the absence of federal law, states and municipalities have enacted a hodgepodge of regulations with varying degrees of severity.[39] This has added complexity and confusion to criminal investigations occurring across jurisdictional lines.[40] To illustrate, imagine a murder occurred in Los Gatos, California, where law enforcement is prohibited from using FRT. Would that prohibition bar Los Gatos police from using relevant evidence that police in neighboring Palo Alto derived from

FRONTIER FOUND., https://www.eff.org/pages/face-recognition (last visited Oct. 22, 2020).

[38] Susan Crawford, *Facial Recognition Laws Are (Literally) All Over the Map*, WIRED (Dec. 16, 2019, 8:00 AM), https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/.

[39] For localities embracing facial recognition as an investigative tool see, e.g., DIRECTIVE 307.5, DETROIT, MICH., POLICE DEP'T MANUAL 1–2 (2019), https://detroitmi.gov/sites/detroitmi.localhost/files/2019-09/Revised%20facial%20recognition%20directive%20transmitted%20to%20Board%209-12-2019.pdf) (permitting use of still images in the context of Part 1 Violent Crimes investigations, which are defined as robbery, sexual assault, aggravated assault, or homicide); Brian New, *Fort Worth, Irving and Plano Police Using Controversial Facial Recognition App on 'Trial Basis'*, 21 CBS DFW (Mar. 9, 2020, 6:45 PM), https://dfw.cbslocal.com/2020/03/09/fort-worth-irving-plano-police-controversial-facial-recognition-app-trial-basis/ (explaining North Texas police departments' trial with Clearview AI, a leader in facial recognition software). For localities completely banning facial recognition in the law enforcement context see, e.g., Dave Lee, *San Francisco is First US City to Ban Facial Recognition*, BBC (May 14, 2019), https://www.bbc.com/news/technology-48276660#:~:text=Legislators%20in%20San%20Francisco%20have,transport%20authority%2C%20or%20law%20enforcement (explaining that San Francisco enacted an outright ban to prohibit local agencies, including law enforcement and transport authorities, from using the technology); Jay Peters, *Portland Passes Strongest Facial Recognition Ban in the US*, THE VERGE (Sept. 9, 2020, 10:41 PM), https://www.theverge.com/2020/9/9/21429960/portland-passes-strongest-facial-recognition-ban-us-public-private-technology (explaining that Portland's regulation prohibits use by both public and private companies). Other cities with facial recognition regulations include Oakland, California; and Boston and Sommerville, Massachusetts. Crawford, *supra* note 38.

[40] Crawford, *supra* note 38.

FRT?[41] Considering Los Gatos is only 23 miles away from Palo Alto, it is easy to see how divergent municipal laws can complicate criminal investigations.

This regulatory landscape (or lack thereof) could soon change, however, as protests following the death of George Floyd have reignited bipartisan discussion about FRT.[42] A 2019 study published by the National Institute of Standards and Technology (NIST) bolsters the case for reform, showing that FRT *verification* software generated disproportionate rates of false positives for women, Asians, African Americans, and Indigenous people.[43] The false positive rates for women were 2 to 5 times higher than for men,[44] while the false positive rates for ethnic and racial minorities were up to 100 times higher than for white individuals.[45] Similarly, FRT *identification* software generated high rates of false positives for ethnic and racial minorities, especially African American women.[46] Various algorithms performed differently across different metrics; thus, NIST's conclusions should not be broadly applied without first distinguishing the facial recognition algorithm, the task the algorithm accomplished, and the machine learning techniques used by the developer.[47] Although nuanced, NIST's findings still highlight a significant consideration: the California legislature should regulate law enforcement's use of FRT to mitigate the probability that algorithms will generate demographic disparities.[48]

[41] This is assuming, of course, that the criminal is reasonably believed to be in the second state. The question is not meant to inquire about whether it is correct for law enforcement officers to circumvent local regulations by offhandedly deciding to go to another jurisdiction to investigate evidence from their own jurisdiction.

[42] Cristiano Lima, *Big Tech to Congress: Your Move on Facial Recognition*, POLITICO (June 13, 2020, 7:00 AM), https://www.politico.com/news/2020/06/13/facial-recognition-congress-316235.

[43] Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NAT'L INST. OF STANDARDS AND TECH. 4 (Dec. 2019), https://doi.org/10.6028/NIST.IR.8280.

[44] *Id.* at 5.

[45] *Id.* at 2.

[46] *Id.* at 63.

[47] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software,* NAT'L INST. OF STANDARDS AND TECH. (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. ("Such distinctions are important to remember as the world confronts the broader implications of facial recognition technology's use.").

[48] *See* Grother et al., *Face Recognition Vendor Test (FRVT), supra* note 43. Because identification procedures are associated with higher levels of misidentification and they make up the majority of FRT use, this Article will focus exclusively on regulating law enforcement's deployment of FRT for identification purposes.

A. Proposed Federal Bills Either Fail to Regulate FRT Use in *Post Hoc* Investigations or Ban It Entirely

1. Federal Proposals

In the summer of 2020, Capitol Hill was flooded with proposed FRT regulations. Each of the proposals failed to effectively address FRT opponents' fears of racial bias in policing. In June of 2020, Congressman Donald Beyer, a Democrat from Virginia, introduced the Stop Biometric Surveillance by Law Enforcement Act, which would prohibit a state or unit of local government from attaching FRT-enabled devices to officer-worn body cameras.[49] The bill has a limited scope, applying only to "real time" FRT analyses. It therefore fails to address law enforcement's FRT use in *post hoc* investigations.[50]

In the U.S. Senate, Democratic Senators Jeff Merkley of Oregon and Bernie Sanders of Vermont introduced a bill targeting private companies' FRT use. The National Biometric Information Privacy Act of 2020[51] would require private companies to obtain individuals' consent before collecting "biometric data."[52] The bill exempts "writing samples, written signatures, photographs, tattoo descriptions, or physical

[49] Stop Biometric Surveillance by Law Enforcement Act, H.R. 7235, 116th Cong. § 3(a) (2020).

[50] The bill is currently being deliberated by members of the House Subcommittee on Emergency Preparedness, Response, and Recovery, where it has been since August 1, 2020. *All Information (Except Text) for H.R. 7235 – Stop Biometric Surveillance by Law Enforcement Act*, CONGRESS, https://www.congress.gov/bill/116th-congress/house-bill/7235/all-info?r=1&s=1 (last visited Oct. 26, 2020).

[51] National Biometric Information Privacy Act of 2020, S. 4400, 116th Cong. (2020). The bill largely resembles state statutes addressing biometric privacy, namely those enacted in Illinois and Texas. Illinois was the first state to enact a biometric privacy law, and it expressly prohibits private companies from possessing biometric information for the purpose of selling, leasing, trading, or profiting from such information. Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/15(c) (West 2008). Texas regulates a person's use of "biometric information," but it excepts disclosure to law enforcement agencies when they have warrants. TEX. BUS. & COM. § 503(c)(1)(D) (West 2009). As the bill's name suggests, its primary objective is to protect individual rights to privacy rather than to address and mitigate alleged racial disparities.

[52] Under the proposal, "biometric data" is broadly defined to include eye scans, voiceprints, faceprints (including any derived from photographs), fingerprints, palm prints, and "any other uniquely identifying information." National Biometric Information Privacy Act of 2020, *supra* note 51, § 2(1)(A); Hunton Andrews Kurth's Privacy and Cybersecurity Group, *Senate Bill Limits Corporate Use of Facial Recognition*, NAT'L L. REV. (Aug. 6, 2020), https://www.natlawreview.com/article/senate-bill-limits-corporate-use-facial-recognition.

descriptions" from the scope of "biometric data."[53] These are significant exemptions because the bill would likely allow the continued use of probe photos from surveillance cameras in FRT analyses. Thus, as in the case of Robert Julian-Borchak Williams, the Michigan man falsely implicated by a probe photo, law enforcement would still be able to obtain a warrant to run images from a private business's surveillance camera through a facial recognition database.[54] The bill focuses solely on FRT's privacy prong, thereby failing to directly address law enforcement's FRT use in *post hoc* criminal investigations.

Lastly, in June 2020, Merkley and Massachusetts Senator Ed Marky introduced The Facial Recognition and Biometric Technology Moratorium Act (the "Moratorium Act").[55] The Moratorium Act makes it unlawful for any federal agency or official "to acquire, possess, access, or use" any biometric surveillance system[56] or information derived from such a system.[57] The Moratorium Act regulates FRT analyses run against both "real time" surveillance *and* recorded videos or photographs.[58] If enacted, this blanket moratorium would unreasonably impede federal law enforcement efforts to identify unknown criminals during *post hoc* investigations—especially in cases where traditional evidence (i.e.,

[53] National Biometric Information Privacy Act of 2020, *supra* note 51, § 2(1)(B) (emphasis added).

[54] *See* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 383 (2015) ("[A] video still from the robbery that does not allow for a facial recognition match. The photo, however, clearly shows a neck tattoo, and officers obtain a partial description of the getaway car. Running a search for the tattoo against a database might narrow the list of suspects. . . . The result is that big data can help identify the suspect with a few search queries.").

[55] The bill's sponsors expressly state that the bill is in response to studies highlighting "systemic inaccuracy and bias issues" that pose "disproportionate risks to non-white individuals." Press Release, Sen. Ed Markey of Mass., Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology (June 25, 2020), https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology).

[56] A biometric surveillance system is defined as "any computer software program that performs facial recognition or other remote biometric recognition in real time *or on a recording or photograph*." Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. § 2(1) (2020) (emphasis added). Facial recognition is also broadly defined to include "an automated or semi-automated process that . . . assists in identifying an individual, capturing information about an individual . . . based on physical characteristics of the individual's face . . . ." *Id.* § 2(3)(A).

[57] *Id.* § 3(a).

[58] *See* commentary in *supra* note 55.

fingerprints, footprints, residue, bodily fluids, etc.) is absent.[59]

The Moratorium Act also fails to specify conditions for its sunset. Instead, the bill's sponsors imply that the moratorium will continue indefinitely until FRT systems no longer exhibit false positives that disproportionately impact minority groups.[60] In light of NIST's 2019 study, which found that algorithmic accuracy varied significantly across FRT systems, it makes little sense that the moratorium would only end once *all* FRT systems exhibited no demographic disparities. Such a requirement causes the bill to operate as a complete ban rather than a temporary moratorium. Not only does this unduly preclude law enforcement from achieving the efficiencies offered by FRT, but it also threatens to stymie the growth of the entire FRT industry.

2. *Evaluating the Moratorium Act: Why It Is Too Harsh*

The Moratorium Act is the most comprehensive FRT bill at the federal level, but it goes too far. Indeed, a bipartisan coalition of senators called the Moratorium Act "extreme,"[61] arguing that a middle ground alternative is required to ensure regulations do not completely eliminate an important investigative tool.[62] To understand the importance of permitting law enforcement's continued FRT use, the California legislature should focus on the efficiencies FRT has created to solve and deter crime.

[59] The *ex post* use would be prohibited unless an Act of Congress explicitly and particularly excepted the use. Facial Recognition and Biometric Technology Moratorium Act, *supra* note 56, § 3(b).

[60] Press Release, Sen. Ed Markey of Mass., *supra* note 55 (reporting that Senator Merkley stated that "[t]he federal government must ban facial recognition until we have confidence that it doesn't exacerbate racism and violate the privacy of American citizens.").

[61] Private commentators have also argued that a complete ban goes too far because "an outright ban . . . needlessly locks us out of using helpful tools that could assist law enforcement in serious cases when traditional investigative techniques fail." Nila Bala & Caleb Watney, *What Are the Proper Limits on Police Use of Facial Recognition?*, BROOKINGS INST. (June 20, 2019), https://www.brookings.edu/blog/techtank/2019/06/20/what-are-the-proper-limits-on-police-use-of-facial-recognition/.

[62] *See generally* Caitlin Chin, *Highlights: Setting Guidelines for Facial Recognition and Law Enforcement*, BROOKINGS INST. TECHTANK (Dec. 9, 2019), https://www.brookings.edu/blog/techtank/2019/12/09/highlights-setting-guidelines-for-facial-recognition-and-law-enforcement/ (including video clips from a Q&A discussion with Senator Chris Coons (D-Del.) and Senator Mike Lee (R-Utah) during which they discuss the need for a "middle ground" regulation).

In the law enforcement context, the FBI has long been considered a leader in FRT use. The agency's Facial Analysis, Comparison, and Evaluation (FACE) Services Unit provides FRT investigative support for field officers.[63] In a recent impact analysis, the FBI's Senior Official for Privacy stated that the FACE Services Unit serves a compelling purpose in investigative policing because it generates results that are "not available with any other investigative method."[64] These results have helped the FBI identify violent criminals and locate violent crime victims when other evidence was either inadequate or absent.[65] Other FRT systems have had similar success, including Spotlight, a tool designed by the nonprofit Thorn. The nonprofit claims Spotlight has helped investigators rescue 15,000 children from underage sex trafficking and identify 17,000 traffickers in North America alone since 2015.[66] U.S. Customs and Border Protection has also used FRT to intercept approximately 300 people attempting to enter the United States under fraudulent credentials and who were believed to be involved with sex trafficking and drug smuggling.[67] It is also hard to overlook the importance of quickly analyzing video and photo evidence. Today, digital evidence constitutes approximately one-third to one-fourth of all evidence.[68] Without FRT systems, there would be no way to process such a vast number of investigative leads and criminal investigations could take much longer to solve.[69]

Local police have achieved similar success. Most notably, police used facial recognition to identify an unknown shooter who killed five people at the Capital Gazette newsroom in Maryland.[70] The suspected

[63] Ernest J. Babcock, *Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit*, FBI (May 1, 2015), https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit.

[64] *Id.*

[65] *Id.*

[66] Jake Parker, *Facial Recognition Success Stories Showcase Positive Use Cases of the Technology*, SEC. INDUS. ASS'N (July 16, 2020), https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/.

[67] *Id.*

[68] NEC America, *supra* note 24.

[69] *Id. See also* Parker, *supra* note 66 (explaining how the New York City Police Department used FRT to identify a man via surveillance images who attempted to commit terror only one hour after the attempt).

[70] Alex Mann & Jessica Anderson, *Capital Gazette Shooting: Maryland Man Pleads Guilty to Attack that Killed Five as Chilling Details Emerge*, CAP. GAZETTE (Oct. 28, 2019, 5:19 PM), https://www.capitalgazette.com/news/crime/ac-cn-capital-shooting-

shooter, Jarrod Ramos, was brought into custody, but the police struggled to identify him because he had no identification, would not speak, and fingerprint analyses returned zero matches.[71] After exhausting alternative measures, the police took a photo of the suspect and submitted it to the Maryland Combined Analysis Center. The Center ran an FRT analysis against millions of mugshots and driver's license photos stored in the Maryland Image Repository System (MIRS).[72] MIRS generated a hit—it matched the suspect's photo to a previous mugshot, when Ramos had been arrested for harassing a high school classmate.[73] Ramos pleaded guilty to the murders.[74] In this case, MIRS successfully identified an unknown criminal after traditional investigative and forensic procedures had failed. In a similar case in Pennsylvania,[75] police credited FRT for solving a two-year-old cold case, stating "[i]f it wasn't for facial recognition, it would still be an open case. We really didn't have a whole lot of leads to go on."[76] The investigative efficiencies that the technology offers for solving a vast array of crimes, ranging from murder to robbery, and from child sex abuse to cashing stolen checks,[77] should not be

hearing-1028-20191028-nkxc5ukn4nbzjdwoltewbmqx6u-story.html.

[71] Derek Hawkins, *How Maryland Police Used Facial Recognition to Catch Annapolis Shooter Jarrod Ramos*, INDEP. (July 2, 2018, 8:11 PM), https://www.independent.co.uk/news/world/americas/annapolis-shooting-maryland-police-facial-recognition-catch-jarrod-ramos-a8427181.html.

[72] Marco della Cava & Elizabeth Weise, *Capital Gazette Gunman Was Identified Using Facial Recognition Technology That's Been Controversial*, USA TODAY (June 29, 2018, 6:49 PM), https://www.usatoday.com/story/tech/talkingtech/2018/06/29/capital-gazette-gunman-identified-using-facial-recognition-technology/744344002/. MIRS contains 7 million Maryland driver's license photos, 3 million state offender images, and nearly 25 million FBI mugshots. Justin Jouvenal, *Police Used Facial-Recognition Software to Identify Suspect in Newspaper Shooting*, WASH. POST (June 29, 2018), https://www.washingtonpost.com/local/public-safety/police-used-facial-recognition-software-to-identify-suspect-in-newspaper-shooting/2018/06/29/6dc9d212-7bba-11e8-aeee-4d04c8ac6158_story.html.

[73] Jouvenal, *supra* note 72.

[74] David Alsup, *Man Accused of Killing 5 Employees in Newsroom Shooting Pleads Guilty*, CNN (Oct. 29, 2019, 5:45 PM), https://www.cnn.com/2019/10/28/us/capital-gazette-shooter-admits-guilt-reports/index.html.

[75] In late 2018, a Pennsylvania police department used a photo saved on a sexual assault victim's cellphone to run comparisons against an FRT database populated with mugshots and driver's licenses. The FRT system positively identified the perpetrator, who later admitted to the assault. Julie Bosman & Serge F. Kovaleski, *Facial Recognition: Dawn of Dystopia, or Just the New Fingerprint?*, N.Y. TIMES (May 18, 2019), https://www.nytimes.com/2019/05/18/us/facial-recognition-police.html.

[76] *Id.*

[77] *Id.*; Barry Friedman & Andrew Guthrie Ferguson, *Here's A Way Forward on Facial Recognition*, N.Y. TIMES OPINION (Oct. 31, 2019),

ignored.[78]

Additionally, and in direct response to concerns about misidentification, a NIST study surveying 127 FRT systems from 39 developers found that FRT accuracy improved twenty-fold between 2014 and 2018.[79] The study analyzed different probe photos, including conventional booking mugshots, poor-quality webcam images, photos from surveillance videos, and "wild images" from disparate "wild" sources.[80] NIST found that FRT systems averaged 4% failure rates in 2014 but only 0.2% failure rates in 2018.[81] As in its 2019 study, NIST conditioned these positive results with a disclaimer that not all algorithms performed equally. Some improved significantly, while others only marginally.[82] Although the report fails to break down failure rates by demographics,[83] it illustrates how rapidly the technology is improving

https://www.nytimes.com/2019/10/31/opinion/facial-recognition-regulation.html (arguing that although facial recognition helps solve petty crimes, its use by law enforcement should be limited to violent crimes, like murder, rape, robbery, and aggravated assault).

[78] In California, San Diego County's police department used a regional database known as the Tactical Identification System (TACIDS), which contained approximately 1.8 million booking photos from 30 regional law enforcement agencies. Roxana Kennedy, the Chief of police in Chula Vista, California, highlighted the importance of TACIDS because it "work[ed] at a quicker pace for us to make sure we identified people correctly… (to) get our officers back on the streets quicker to patrol and keep our community safe." Katy Stegall, *3-Year Ban on Police Use of Facial Recognition Technology in California to Start in the New Year*, SAN DIEGO UNION-TRIBUNE (Dec. 20, 2019, 6:00 AM), https://www.sandiegouniontribune.com/news/public-safety/story/2019-12-20/3-year-ban-on-police-use-of-facial-recognition-technology-in-california-to-start-in-the-new-year. This suggests that the benefits of FRT extend beyond merely identifying unknown perpetrators. It also helped put officers back in the field sooner to patrol for other legal violations.

[79] *NIST Evaluation Shows Advance in Face Recognition Software's Capabilities,* NAT'L INST. OF STANDARDS & TECH., (Nov. 30, 2018), https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities.

[80] Patrick Grother, Mei Ngan & Kayee Hanaoka, *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, NAT'L INST. OF STANDARDS & TECH. 3 (Nov. 2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.

[81] *NIST Evaluation Shows Advance in Face Recognition Software's Capabilities*, *supra* note 79. NIST sampled accuracy rates through a 1-to-many identification test, during which a probe photo was run against a database of 26.6 million photographs.

[82] *Id.*

[83] Grother et al., *Ongoing Face Recognition Vendor Test (FRVT), supra* note 80, at 3, 5 (explaining that the report includes results for ageing and twins but not other demographics but noting that future reports will analyze demographic-based discrepancies).

each year.[84] The investigative efficiencies of FRT, combined with its increasing accuracy, make clear that blanket, indefinite bans, including the Moratorium Act, are unreasonably draconian.[85] The California legislature should avoid this path.

B. California's Recent Reforms and Proposals Fail to Comprehensively Regulate Law Enforcement's FRT Use

As the epicenter of the U.S. technology industry, it is perhaps unsurprising that California has been active in the FRT sphere. Some California cities have enacted ordinances that ban law enforcement's use of FRT altogether. In 2019, San Francisco was the first U.S. city to enact such a ban.[86] In addition to prohibiting local agencies from using FRT, San Francisco requires city administrators' approval before a local agency can "buy any kind of new surveillance technology."[87] Across the bay in Oakland, police are prohibited from "acquiring, obtaining, retaining, requesting, and accessing" FRT systems.[88] Oakland's ordinance amended a 2018 law that permitted law enforcement's FRT use if approved by a member of the city's Privacy Advisory Commission.[89]

Although the two municipal ordinances discussed above are similar, the California legislature has tried to pass uniform FRT regulations that would prevent the effects of divergent municipal laws. In January 2020, California enacted a statute that prohibits law enforcement from using "real time" facial recognition software on officer-worn body cameras.[90] The Body Camera Accountability Act establishes a robust

[84] *NIST Evaluation Shows Advance in Face Recognition Software's Capabilities*, *supra* note 79.

[85] *See generally* INFO. COMM'R'S OFFICE, *ICO Investigation into How the Police Use Facial Recognition Technology in Public Places* 3 (2019), https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf (highlighting a U.K. study that showed live facial recognition technology's rapid improvement in recent years).

[86] Gregory Barber, *San Francisco Bans Agency Use of Facial-Recognition Tech*, WIRED (May 14, 2019, 6:17 PM), https://www.wired.com/story/san-francisco-bans-use-facial-recognition-tech/.

[87] Lee, *supra* note 39.

[88] OAKLAND, CAL., MUN. CODE, tit. 9, ch. 9.64 § 9.64.045 (2019).

[89] Carolina Haskins, *Oakland Becomes Third U.S. City to Ban Facial Recognition*, VICE (July 17, 2019, 7:41 AM), https://www.vice.com/en/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz.

[90] Dustin Gardiner, *California Blocks Police from Using Facial Recognition in Body Cameras*, S.F. CHRON. (Oct. 8, 2020, 7:25 PM), https://www.sfchronicle.com/politics/article/California-blocks-police-from-using-facial-

disciplinary framework permitting sanctions, penalties, and even private causes of action against any individual officer or law enforcement agency that "install[s], activate[s], or use[s] any biometric surveillance system in connection with an officer camera."[91] California Assemblyman Phil Ting argued that the law prevents turning body cameras into "a 24-hour surveillance tool, giving law enforcement the ability to track our every movement."[92] It is important to note that the statute was enacted as an express three-year moratorium—the statute automatically sunsets on January 1, 2023. The moratorium was enacted with the hope that facial recognition developers would acknowledge and improve their technology's current limitations before the automatic repeal date.[93] Because California passed a moratorium rather than an indefinite ban—unlike the federal Moratorium Act—the state legislature appears willing to permit law enforcement's FRT use. Yet, there remains a large hole in the state's current regulatory paradigm, as the statute fails to address FRT use in *post hoc* investigations.[94]

14502547.php. The statute defines "officer camera" as "a body-worn camera or similar device that records or transmits images or sound and is attached to the body or clothing of, or carried by, a law enforcement officer." CAL. PENAL CODE § 832.19(a)(7) (Deering 2020).

[91] CAL. PENAL CODE, § 832.19(b)–(c). Ironically, the prohibition was enacted after the U.S. Department of Justice's dedicated of over $20 million to law enforcement agencies across the nation for the purpose of obtaining facial recognition-equipped body cameras. Ringrose, *supra* note 16, at 57.

[92] ACLU OF N. CAL., *California Governor Signs Landmark Bill Halting Facial Recognition on Police Body Cameras* (Oct. 8, 2019), https://www.aclunc.org/news/california-governor-signs-landmark-bill-halting-facial-recognition-police-body-cams. The legislative notes highlight the Assembly's primary concerns: racial and gender biases, and the protection of individual privacy from overbroad surveillance. Indeed, the statute was adopted on the heels of an ACLU study that found facial recognition software to incorrectly match 26 California lawmakers, especially women and people of color. *Id.* The statute explains that "the use of facial recognition and other biometric surveillance is the functional equivalent of requiring a person to show a personal photo identification card as all times in violation of recognized constitutional rights. . . . Facial and other biometric surveillance would corrupt the core purpose of officer-worn body camera by transforming those devices from transparency accountability tools into roving surveillance systems." 2019 Cal. Adv. Legis. Serv. ch. 579 § 1(c), (e) (LEXIS).

[93] The statute will repeal on January 1, 2023. CAL. PENAL CODE, § 832.19(e). The original statute was written as an indefinite ban, but the California state senate amended the statute to be a three-year moratorium. Gregory Barber, *California Bill Would Halt Facial Recognition on Bodycams*, WIRED (Sept. 11, 2019, 7:06 PM), https://www.wired.com/story/california-bill-halt-facial-recognition-body-cams/.

[94] The scope of the statute is expressly limited to "use . . . in connection with an officer camera or data collected by an officer camera." CAL. PENAL CODE, § 832.19(b).

California Assemblyman Ed Chau introduced A.B. 2261 to fill the regulatory hole left open by the Body Camera Accountability Act. Commentators described A.B. 2261 as the first bill in the United States to "comprehensively regulate the use of FRT across both public and private sectors."[95] At the law enforcement level, however, A.B. 2261's text only limited an agency's[96] deployment of FRT for "ongoing surveillance."[97] Specifically, the bill would have prohibited law enforcement from using FRT systems that "analyze facial features . . . in still or video images"[98] for the purpose of "tracking the physical movements of an individual through one or more public places *over time*, whether in real time or through application of a facial recognition service to historical records."[99] The bill exempted this prohibition for "law enforcement activities,"[100] and for evidence in serious criminal offenses if either a search warrant is obtained or law enforcement reasonably believes ongoing surveillance is necessary to prevent an imminent risk of death or serious bodily harm.[101] The bill also established several administrative protocols requiring law enforcement to: (1) maintain FRT use records,[102] (2) publish annual use reports,[103] and (3) produce biannual accountability reports.[104]

Still, A.B. 2261 did not substantively limit state and local law enforcement's FRT use. Although the bill addressed some issues

[95] Rebecca Robbins, *The Fight over Facial Recognition Technology Gets Fiercer During the Covid-19 Pandemic*, STAT (May 5, 2020), https://www.statnews.com/2020/05/05/facial-recognition-technology-covid19-tracking-california-bill/. In terms of private use, the bill would require that companies obtain affirmative consent from individuals before enrolling their image in a facial recognition system. Individuals can revoke their initial consent and demand that their photo be deleted from records at any time, and the company must acquiesce within 30 days of that request. Assemb. B. 2261 § 1798.315, § 1798.320, 2019-2020 Reg. Sess. (Cal. 2020). If companies violate any of the provisions of the bill, they would be subject to civil penalties. *Id.* § 1798.375.

[96] This includes state and local public agencies, like public police departments. *Id.* § 1798.360.

[97] *Id.*

[98] *Id.* § 1798.305(f)(1).

[99] *Id.* § 1798.300(j)(1) (emphasis added).

[100] Interestingly, the bill fails to define was constitutes "law enforcement activities." Considering the bill differentiates "law enforcement activities" from "evidence of a serious criminal offense," which is presumably a law enforcement activity, it is only natural to inquire what the legislature meant with this term. The legislative history and notes fail to provide guidance on this question.

[101] Assemb. B. 2261, *supra* note 95, § 1798.360(a).

[102] *Id.* § 1798.365.

[103] *Id.* § 1798.340.

[104] *Id.* § 1798.335.

associated with FRT—namely, public transparency—civil rights activists believed the bill failed to deter racially biased policing because it lacked true oversight in several respects, including for *post hoc* identification procedures.[105] Further, the ACLU, which was the most outspoken critic of A.B. 2261, was joined by fifty groups to argue that the bill would set a dangerous precedent by undercutting municipal ordinances across the state, including the bans enacted in San Francisco and Oakland.[106] Assemblyman Chau's bill was laudable for its comprehensive approach to FRT regulation but more must be done to ensure law enforcement does not abuse its authority to utilize FRT systems and to address opponents' concerns. A.B. 2261's failure can be attributed to these shortcomings.[107] In its absence, the probability that more restrictive regulations will be enacted, such as outright bans and indefinite moratoriums, continues to rise.

[105] Susan Carpenter, *Controversial California Facial Recognition Tech Bill Put on Hold*, SPECTRUM NEWS (June 4, 2020, 6:45 AM), https://spectrumnews1.com/ca/la-west/news/2020/06/02/controversial-california-facial-recognition-technology-bill-put-on-hold. *See also Hearing on AB 2261 Before the Assemb. Committee on Appropriations*, 2019-2020 Reg. Sess. (Cal. 2020) (arguments in opposition) ("AB 2261 will subject Californians to the harms of face surveillance at a moment where our collective responsibility to promote public health and protect people is more critical than ever. As the nation looks to California's leadership in regulating big tech . . . we hope the Legislature will take the threat of facial recognition and the lasting societal impact it will have seriously.").

[106] *Carpenter*, supra note 105; Laurence Colletti & Kirsten Errick, *AB 2261: California's Facial Recognition Bill*, LEGAL TALK NETWORK (June 24, 2020), https://legaltalknetwork.com/podcasts/legal-talk-today/2020/06/ab-2261-californias-facial-recognition-bill/.

[107] In June of 2020, the bill was stalled in the California Assembly's Appropriations Committee, and it has been held there ever since [last updated December 2021]; *Carpenter*, *supra* note 105.

C. Private Sector Seeks Regulatory Guidance

The aforementioned federal and state bills join measures enacted by Amazon,[108] Microsoft,[109] and IBM,[110] which cited civil rights concerns as grounds for no longer selling their FRT software to police departments.[111] The companies' prohibitions vary in severity, but they further underscore the importance of ensuring the technology is regulated to discourage misidentifications along racial, gender, and age lines. Each of these companies have expressly requested regulatory guidance.

[108] Amazon announced a one-year moratorium on police use of its facial-recognition technology, Rekognition, beginning June 10, 2020. The company cited inaccuracy rates for racial minorities, women, and younger people as its biggest concerns. Bobby Allyn, *Amazon Halts Police Use of Its Facial Recognition Technology*, NPR (June 10, 2020, 6:59 PM), https://www.npr.org/2020/06/10/874418013/amazon-halts-police-use-of-its-facial-recognition-technology. This moratorium follows Amazon's past defenses of Rekognition in which Amazon claimed studies of accuracy "misperceived" how the technology operates. Bobby Allyn, *IBM Abandons Facial Recognition Products, Condemns Racially Biased Surveillance*, NPR (June 9, 2020, 8:04 PM), https://www.npr.org/2020/06/09/873298837/ibm-abandons-facial-recognition-products-condemns-racially-biased-surveillance.

[109] Microsoft's President, Brad Smith, said that the company will not sell facial recognition technology to police departments until there is a federal law regulating it. Jay Greene, *Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM*, WASH. POST (June 11, 2020, 2:30 PM), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/. Since California introduced A.B. 2261, Microsoft announced that "AB 2261 is a thoughtful approach which recognizes the need for safeguards to balance the opportunities and risks associated with facial recognition technology. The California legislature has an opportunity to establish appropriate standards for the use of facial recognition technology." *Hearing on AB 2261 Before the Assemb. Committee on Appropriations*, *supra* note 105 (arguments in support). Although this is not an outright endorsement of A.B. 2261, it shows that these tech giants are open to significant regulation.

[110] IBM's statement is perhaps the bluntest: it will no longer provide facial recognition technology to police departments "for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose which is not consistent with our values." Tim Bajarin, *Why It Matters That IBM Has Abandoned Its Facial Recognition Technology*, FORBES (June 18, 2020, 2:27 PM), https://www.forbes.com/sites/timbajarin/2020/06/18/why-it-matters-that-ibm-has-abandoned-its-facial-recognition-technology/#63a4b35aafaf (quoting IBM CEO, Arvind Krishna's letter to Congress).

[111] *See generally* Rebecca Heilweil, *Big Tech Companies Back Away from Selling Facial Recognition to Police. That's Progress.*, VOX (June 11, 2020, 5:02 PM), https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police (summarizing each company's approach to the issue).

III. PROPOSED AMENDMENT TO CALIFORNIA ASSEMBLY BILL 2261

In 2019, the Commission Nationale de l'Informatique et des Libertés[112] posited that FRT regulations should take an "experimental approach" that establishes specific "criteria for . . . [FRT] deployment," thereby limiting use to time and space.[113] California's A.B. 2261 failed to achieve this limited use.[114] Before reintroducing A.B. 2261, California should amend the current version to condition *all* of law enforcement's FRT use on probe photo quality assessments conducted by independent forensic facial reviewers. These quality assessments should occur before uploading a probe photo for FRT analysis, and the facial reviewers should work in an independent organization that is separate from state and local police departments. The independent organization should also assess all reported FRT matches before sending them to a law enforcement agency. This amendment should be added to A.B. 2261 as a new section, § 1798.360 (Conditions for Agency Use of Facial Recognition Services). The proposed amendment is as follows:

> (1) **Conditions for Use**. A submitting agency, including any state and local law enforcement agency, shall not use a facial recognition service for any reason, including for investigative purposes, unless all of the following conditions are met:
>
> (a) The submitting agency shall send all probe photos collected for facial recognition analysis to an independent organization of examiners who have forensic facial reviewer certification as required by the California Bureau of Forensic Services, and that independent organization shall be separate from any law enforcement agency;
>
> (b) The independent organization of forensic facial reviewers shall evaluate the quality of each probe photo to ensure it satisfies threshold objective requirements promulgated by the National Institute of Standards and Technology (NIST). These evaluations shall be completed before the probe photo is used in a facial recognition system, and at least two reviewers shall conduct independent evaluations for each probe photo. In cases where two initial reviewers render opposite evaluations, a third reviewer shall conduct an independent evaluation for the probe photo and that

[112] The Commission is an independent French administrative body that focuses on data privacy.

[113] COMM'N NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *supra* note 35, at 10.

[114] *See* Assemb. B. 2261, *supra* note 95, § 1798.360.

reviewer's evaluation shall be final and binding;

(c) The submitting agency and the independent organization of forensic facial reviewers shall not replace the physical or digital features of a probe photo for enhancement purposes, even if meant to improve the quality of a probe photo to satisfy NIST's requirements under subsection (b) or to increase the probability of a positive facial recognition match, but the independent organization of forensic facial reviewers may enhance the digital features of a probe photo according to enhancement recommendations promulgated by NIST;

(d) The submitting agency shall retain ownership of each probe photo as evidence, but the independent organization of forensic facial reviewers shall delete all probe photos from their records, either physical or digital, within thirty (30) days of either:

i. Rendering a quality assessment to the agency that requested the facial recognition service, informing that agency of a probe photo's inadequate quality; or

ii. If the probe photo meets NIST's requirements, sending facial recognition matches, if any, to the agency that requested the facial recognition service pursuant to subsection (e);[115] and

(e) If the independent organization of forensic facial reviewers concludes that the probe photo meets NIST's requirements and uses the probe photo for FRT analysis, then at least two forensic facial reviewers shall analyze the FRT matches, if any, against the initial probe photo to determine, in their discretion, whether such matches, if any, should be returned to the submitting agency as evidence.

(2) **Software Contracts**. The California Department of Technology shall have the sole discretion to establish a list of approved facial recognition technology vendors

[115] This provision was included because the law enforcement groups submitting probe photos to the independent agency will maintain ownership rights in that photo evidence. In other words, the police are merely loaning the image, in either digital or hard copy, to the independent agency for quality assessment and FRT purposes *only*. Thus, to protect the privacy rights of individual captured in any probe photo, and consistent with the California Consumer Privacy Act, the independent agency will be required to permanently delete the probe photo from its internal, independent records. This will ensure confidentiality and eliminate a channel for hacking of personally identifiable information.

that can contract their technology to forensic facial reviewers.[116] All California agencies are prohibited from contracting with facial recognition technology vendors that are not approved by the California Department of Technology.

(3) **Limitations**. If any of the conditions set forth in paragraph 1 are not met, then all California entities, including state and local law enforcement and the independent organization of forensic facial reviewers, are prohibited from uploading a probe photo to a facial recognition service.

(4) **Remedies**. If any California entity, or any individual employed by any such entity, violates any of the provisions of this Section 1798.360, then the Attorney General has exclusive authority to enforce this title by bringing an action in the name of the people of the State of California and such remedies may include injunctions and civil liabilities of not more than two thousand five hundred dollars ($2,500) per each unintentional violation and not more than seven thousand five hundred dollars ($7,500) per each intentional violation. If more than one agency contributes to the same violation of this Section 1798.360, then the liability for the violation shall be allocated among the parties according to principles of comparative fault.[117]

IV. JUSTIFICATIONS FOR THE ELEMENTS IN THE PROPOSED AMENDMENT

A. Compulsory Probe Photo Quality Assessments Mitigate Misidentifications

The proposed amendment requires that all probe photos satisfy threshold quality requirements established by NIST. This requirement follows NIST's 2019 study, which concluded that high-quality probe photos generate very low misidentification rates[118] with almost

[116] According to CAL. PUB. CONT. CODE § 12100(b)(1) (West 2018), all government contracts for the "acquisition of information technology goods" "shall be made by or under the supervision of the Department of Technology." Although the statutory framework fails to define "information technology goods," FRT most likely falls within the ambit of this statutory requirement. *See id.* § 12101.3(g)(2) (defining "information technology services" broadly).

[117] These remedies are adopted from the current version of A.B. 2261. *See* Assemb. B. 2261, *supra* note 95, § 1798.375.

[118] As a notable distinction, the study found that higher image quality had a limited impact on false *positive* rates with ethnic and racial minorities being incorrectly identified at

unquantifiable demographic differentials across FRT algorithms.[119] In FRT analyses, poor image focusing, dim lighting, and off-centered angles can increase the likelihood of misidentification.[120] With respect to individuals with darker complexions, the study reasoned that under-exposure could cause increased misidentification.[121] In cases with probe photos of suboptimal quality, "true matches become indistinguishable from false positives."[122]

At the federal level, some law enforcement agencies have acknowledged the importance of probe photo quality, but they continue to use low-quality images in their analyses. In a 2020 report assessing the U.S. Immigration and Customs Enforcement's use of FRT to counteract domestic and international crimes, the Department of Homeland Security (DHS) acknowledged the positive correlation between low quality probe

higher rates. Grother et al., *Face Recognition Vendor Test (FRVT)*, *supra* note 43, at 2. *But see infra* Section IV(C) for the amendment's steps to further reduce these false positive rates.

[119] Grother et al., *Face Recognition Vendor Test (FRVT)*, *supra* note 43, at 7. The study complements research conducted in other forensic fields, namely latent fingerprints, which are incomplete prints with variable and diminished quality. When used in fingerprint analyses, the accuracy of latent fingerprint results is highly dependent on the relative quality and clarity of the original print, including the surface that was touched and the "mechanics" of the touch. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., REPORT TO THE PRESIDENT ON FORENSIC SCIENCE IN CRIMINAL COURTS: ENSURING SCIENTIFIC VALIDITY OF FEATURE-COMPARISON METHODS 88 (Sept. 2016). Note the similarity between the quality of latent fingerprints and the quality of traditional probe photos, which each contain suboptimal characteristics.

[120] *See* Grother et al., *Face Recognition Vendor Test (FRVT)*, *supra* note 43, at 15–16 ("A poor image can undermine detection or recognition, and it is possible that certain demographics yield photographs ill-suited to face recognition e.g. young children, or very tall individuals."). Using low quality data to train FRT algorithms in identifying patterns across facial features is also attributable to increased false positivity rates. The NIST study stated that "[a] number of algorithms developed in China give low false positive rates on East Asian faces, and sometimes there are lower than those with Caucasian faces. . . . [T]he location of the developer [is] a proxy for the race demographics of the data they used in training – [this] matters . . . and is potentially important to the reduction of demographic differentials due to race and national origin." *Id.* at 7. Amazon maintains an FAQ page about its FRT, Rekognition, in which it states that the quality of results can be impacted by video resolution, heavy blur, fast moving persons, lighting conditions, and poses. *Amazon Rekognition FAQs*, https://aws.amazon.com/rekognition/faqs/ (last visited Oct. 15, 2020).

[121] *See* Grother et al., *Face Recognition Vendor Test (FRVT)*, *supra* note 43, at 15–16.

[122] Qumodo Ltd., *Automatic Facial Recognition: Why Do We Need a Human in the Loop?*, MEDIUM (March 26, 2019), https://medium.com/@1530019197930/automatic-facial-recognition-why-do-we-need-a-human-in-the-loop-de8366d10680 (citing a 2018 NIST study).

photos and higher rates of misidentification.[123] DHS said there is a risk that investigators could submit low quality images exhibiting poor lighting, sharpness, image resolution, camera angle, facial expression, facial impediments (i.e., hats, sunglasses, and facial hair), or zooming and cropping features that would increase the likelihood of false matches.[124] DHS argued, however, that this risk is mitigated because "most [facial recognition providers] exercise quality control of images accepted into their systems. . . . [T]he [facial recognition providers] can reject a probe photo that is of too low quality to produce a candidate list."[125] In other words, the report suggests DHS lacks formal internal rules that prevent investigators from routinely using low-quality images and, instead, relies on the facial recognition providers to prevent misidentifications. Absent coherent, strict probe photo quality requirements, DHS's current policy theoretically enables it to routinely upload probe photos that NIST has identified as inadequate and facilitative of misidentification. DHS then claims that any such misidentifications should have been filtered by the FRT providers' permissive photo quality assessments. This report shows that agencies need statutory guidance for using sophisticated technology because, without it, they do not enact adequate policies.

By conditioning law enforcement's FRT use on compulsory probe photo quality assessments, the proposed amendment affirmatively prevents state and local law enforcement officials from unilaterally and subjectively deciding which probe photos can be used in FRT analyses. Quality assessments will ensure that only probe photos with characteristics facilitative of *accurate* FRT results are permitted for FRT analyses. Under the proposed amendment, quality assessments will be guided by independent and objective standards that NIST has identified as the characteristics most likely to generate accurate results.[126] Partnering with NIST is consistent with A.B. 2261's other provisions. One existing section (§ 1798.310) allows FRT vendors to satisfy accuracy testing requirements by "submitting deployed algorithms to each relevant Face Recognition Vendors Test that [NIST] performs, including, but not

[123] ICE routinely uses various private and public facial recognition services, which employ independently selected FRT software to run comparisons. DEP'T OF HOMELAND SEC., *supra* note 15, at 3.

[124] *Id.* at 26.

[125] *Id.* at 27 (emphasis added).

[126] It is important that the assessments be guided by objective standards that can be applied consistently as opposed to subjective standards that are burdensome and costly to verify. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., *supra* note 119, at 89.

limited to, overall accuracy and demographic-specific tests."[127] Further, the proposed amendment seeks to employ NIST's unmatched empirical expertise in FRT algorithmic accuracy. The proposed amendment does not codify specific image-quality considerations—like lighting, angle, or pixilation—but rather allows for flexibility in response to FRT's rapid development and improvement.[128] By allowing NIST to update its quality recommendations from time to time, the amendment would not be rendered outdated if NIST's initial recommendations turn out to be incorrect.

B. *Ex Ante* Assessments Thwart Confirmation Bias

The proposed amendment requires that forensic facial reviewers analyze probe photo quality before using the photo in a FRT analysis. This would reduce confirmation bias, a psychological phenomenon defined as "the tendency to process information by looking for, or interpreting, information that is consistent with one's existing beliefs. . . . [It] is largely unintentional and often results in ignoring inconsistent information."[129] In the FRT context, confidence scores—meant to indicate the system's certainty of a match—can encourage confirmation biases and therefore increase the likelihood of misidentification. This is especially problematic when probe photo quality is low because it is harder to manually compare the probe photo to any generated matches, causing human reviewers to potentially defer solely to an FRT system's top match.

Developers code FRT systems to report matches only above a predetermined confidence score.[130] The score falls on a scale between 0% and 100%, indicating the probability that a given FRT result is accurate.[131] For example, if an FRT system was coded with 95% confidence, then the system would only generate matches that it believed were at least 95% accurate. These predetermined scores are often manipulated based on the context in which the FRT system is deployed.[132] When human specialists review the accuracy of FRT-generated matches, the confidence threshold

[127] Assemb. B. 2261, *supra* note 95, § 1798.310(a)(3)(B).

[128] *See* Crumpler, *supra* note 30.

[129] *Confirmation Bias*, BRITANNICA, https://www.britannica.com/science/confirmation-bias (last visited Nov. 11, 2020).

[130] Crumpler, *supra* note 30.

[131] *Id.*; *Amazon Rekognition FAQs*, *supra* note 120.

[132] *Amazon Rekognition FAQs*, *supra* note 120 ("Applications that are very sensitive to detection errors (false positives) should discard results associated with confidence scores below a certain threshold. The optimum threshold depends on the application.").

is reduced on the supposition that those specialists will manually compare the probe photo and corresponding matches to filter out false matches.[133] Supposedly, the rationale for reducing the confidence score is that providing the human specialists with a larger pool of FRT hits enables them to more accurately identify an unknown criminal.

However, because specialists know the FRT system only reports results with at least 95% confidence, they may confirm the results' accuracy without running complete and thorough comparisons.[134] This phenomenon was illustrated in a Department of Justice study conducted in 2011, which found that scores accompanying technologically generated fingerprint matches directly influenced human reviewers' decisions.[135] In that study, human reviewers were presented with a list of either ten or twenty fingerprint matches.[136] The results were ranked in order from highest probable match to lowest probable match.[137] The researchers found that the mere order of the list—and the confidence score itself—affected human reviewer decision-making. Because the reviewers knew the results were listed from highest to lowest confidence, they often concluded that the matches listed at the top were accurate without reviewing the entire list or after only a brief review of matches towards the bottom of the list.[138] This study illustrates how high confidence scores can impact human reviewers when such scores are paired directly to specific technologically generated matches.

Confirmation bias is often exacerbated when specialists work on complex tasks, carry heavy workloads, and are required to produce results quickly and under pressure.[139] These factors are common in law enforcement, especially in *post hoc* investigations in which police

[133] Crumpler, *supra* note 30. On the other hand, when humans are not employed to assess the FRT matches, the confidence threshold is generally set around 99% to filter out false positives. *Id.*

[134] Kate Goddard, Abdul Roudsari & Jeremy C. Wyatt, *Automation Bias: A Systemic Review of Frequency, Effect Mediators, and Mitigators*, 19 J. AM. MED. INFO. ASS'N 121, 124 (2012) ("[P]hysicians were more likely to be biased by automation and accept . . . advice when they were less confident of their own diagnosis. . . . [A]utomation reliance is essentially a trade-off between self-confidence and trust in the [automated support system].").

[135] *See* ITIEL DROR & KASEY WERTHEIM, QUANTIFIED ASSESSMENT OF AFIS CONTEXTUAL INFORMATION ON ACCURACY AND RELIABILITY OF SUBSEQUENT EXAMINER CONCLUSIONS (2011), https://www.ojp.gov/pdffiles1/nij/grants/235288.pdf).

[136] *Id.* at 11.

[137] *Id.* at 47.

[138] *Id.* at 50 ("[E]xaminers take less time to compare items when they are presented at a lower position on the list.").

[139] *Id.* at 125.

scramble to identify unknown criminals who pose potential threats to the public. By requiring *ex ante* probe photo quality assessments, the proposed amendment relieves some of the pressures associated with manually reviewing FRT-generated results. Higher quality probe photos will likely produce fewer matches and the initial probability of incorrect matches will be lower.[140] This provision in the amendment reduces the probability that confirmation bias will influence law enforcement's use of incorrect FRT-generated matches.

C. Fusing Multiple Human Forensic Facial Reviewers' Quality Assessments with FRT Analyses Increases Matching Accuracy

Research shows that humans are superior to algorithms in identifying people in lower quality images. In a 2012 study, researchers compared facial identification performance between various FRT algorithms and individuals without professional face recognition training.[141] The study compared identification accuracy rates across three photo types: (1) still frontal images with studio-like controlled lighting or ambient outdoor lighting; (2) digital video sequences with natural motion effects; and (3) edited images of faces, where either the background and the person's body were deleted or the person's face was masked, leaving only the person's body and the background visible.[142] The study found that FRT algorithms outperformed humans when asked to identify people in the high-quality still frontal images.[143] On the other hand, humans outperformed the algorithms when asked to identify people in video sequences and the edited face images.[144] The researchers reasoned that the results were likely due to humans' ability to interpret non-facial identity cues, such as pose and body shape, which were missing in the edited face images.[145]

[140] *See generally supra* Section IV(A).

[141] P. Jonathon Phillips & Alice J. O'Toole, *Comparison of Human and Computer Performance Across Face Recognition Experiments*, 34 ELSEVIER: IMAGE AND VISION COMPUTING 74, 76 (2013), https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=913011.

[142] *Id.* at 76, 78.

[143] *Id.* at 75 ("For these images, machines represent a person's identity primarily by encoding information extracted from the face; information from the body, hair, and head is generally ignored. For video and extremely difficult-to-recognize face pairs, experiments show that humans take advantage of all available identity cues when recognizing people.").

[144] *Id.* at 81.

[145] *Id.* The study noted that FRT developers were beginning to integrate changing poses in their machine learning techniques, so the results could be significantly different. *Id.*

These results suggest that human reviewers could prove to be assets in identification procedures because law enforcement will rarely have access to professional-grade photo evidence similar to the images in Figure 1.[146] In the majority of *post hoc* criminal investigations, law enforcement must analyze low-quality probe photos like those in Figures 2 and 3. In those images, the suspect sits at an offset angle in dim light, or their face is obscured by physical objects, like a baseball cap. Based on the aforementioned study, humans are better equipped to assess these lower quality probe photos because humans consider non-facial characteristics in determining facial recognition.

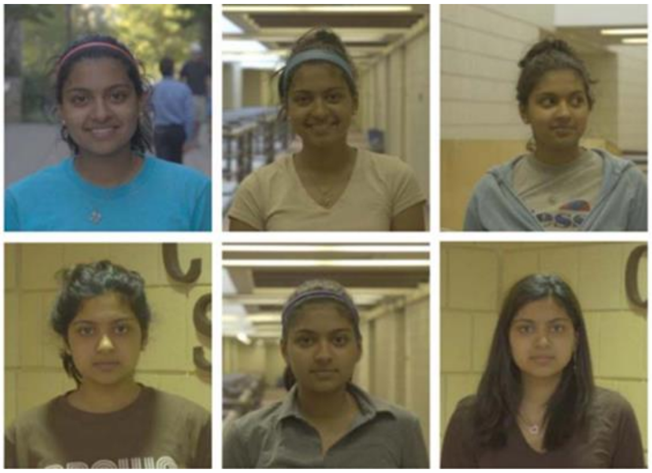

Figure 1: These images represent the study's studio-like frontal images, where FRT outperformed humans.[147]

[146] These kinds of photos could be captured through ATM robberies, pictures from phones, or social media, but they are rarely found from video surveillance, which is the majority of probe photos.

[147] Phillips & O'Toole, *supra* note 141, at 78.

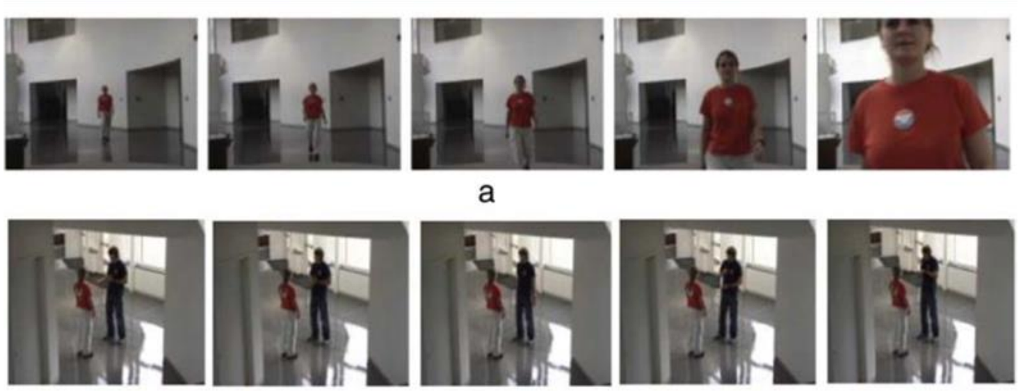

Figure 2: These images were used in video experiments, where humans outperformed FRT systems by considering pose and body shape.[148]

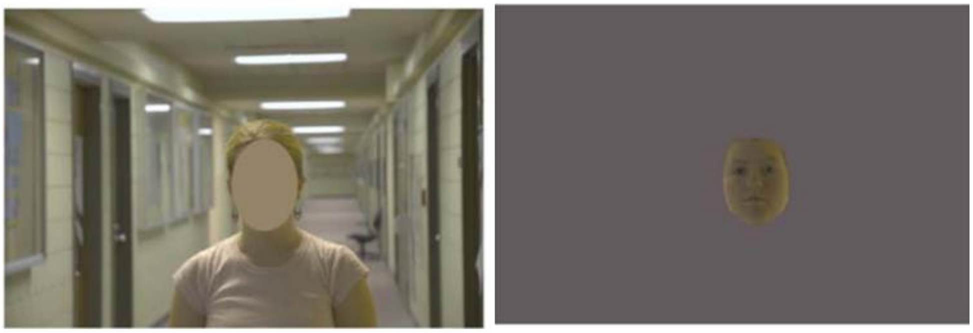

Figure 3: These images were used in the extremely-difficult frontal face experiments, where either the face was blocked or the person's body and background were blocked. Humans outperformed FRT systems in these experiments.[149]

Further, FRT accuracy can be improved by "combining human and machine face identification judgments."[150] In a recent study, researchers compared the identification accuracy of various groups of human examiners to that of FRT systems. The experiment used images with uncontrolled illumination, expression, and appearance, much like conventional probe photos.[151] The various human groups included: (1a)

[148] *Id.* at 81.

[149] *Id.* at 80.

[150] P. Jonathon Phillips et al., *Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms*, 115 PROC. OF THE NAT'L ACAD. OF SCI. OF THE U.S. 6171, 6171–72 (2018), https://222.pnas.org/content/115/24/6171.

[151] *Id.* at 6172. The results from this study are supported by other research that shows humans accounting for non-face information makes them superior to computer analyses when facial recognition analyses assess suboptimal photo conditions. Chaochao Lu &

forensic facial experts and (1b) forensic facial reviewers, all of whom are extensively trained in facial identification;[152] (2) untrained people "with strong skills in face recognition," also known as "super-recognizers";[153] and (3) two control groups consisting of fingerprint examiners and undergraduate students. The study found that forensic facial experts identified faces with the highest degree of accuracy (93%), followed by forensic facial reviewers (87%) and super-recognizers (83%).[154] On the FRT side, the most advanced FRT system completed the same experiment with 96% accuracy.[155] After analyzing these baseline scores, the researchers combined scores across experimental groups. When a single forensic facial reviewer's score was combined with an advanced FRT system's score, the accuracy rate improved to 100%—in other words, there were no misidentifications.[156] Combining the strengths of professionally trained forensic face reviewers with the strengths of advanced FRT algorithms maximizes FRT accuracy.[157]

The proposed amendment requires that humans with forensic training both conduct the compulsory probe photo quality assessments and review any FRT matches before sending those matches to law enforcement as evidence. Similar provisions in A.B. 2261 would have required "meaningful human review" of any agency decision producing "legal effects."[158] A.B. 2261 defined meaningful human review as "oversight by one or more individuals who are trained . . . and who are ultimately responsible for making decisions based, in whole or in part, on the output of a facial recognition service."[159] The intent of the proposed amendment is the same: using human judgment to prevent overreliance on FRT matches and to ensure clearly incorrect matches are not sent to law enforcement for investigative purposes. The proposed amendment goes further, however, by expressly requiring forensic facial review training to capitalize on the advantages laid out in the 2012 study. This

Xiaoou Tang, *Surpassing Human-Level Face Verification Performance on LFW with Gaussian Face*, *in* PROCEEDINGS OF THE TWENTY-NINTH AAAI CONFERENCE ON ARTIFICIAL INTELLIGENCE (2015).

[152] Phillips et al., *supra* note 150, at 6172.

[153] *Id.* at 6171.

[154] *Id.* at 6172. The score falloff from superrecognizers to fingerprint examiners and undergraduate students was statistically significant, with those groups logging 76% and 68% accuracy rates, respectively. *Id.*

[155] *Id.*

[156] *Id.* at 6173.

[157] *Id.*

[158] Assemb. B. 2261, *supra* note 95, § 1798.310(f).

[159] *Id.* § 1798.305(i).

requirement is rooted in the study's finding that forensic face reviewers positively identified faces with 87% accuracy.[160] Forensic facial "reviewers" are trained to perform faster and less-rigorous identifications to generate leads in criminal investigations, unlike forensic facial "experts," who are trained to complete more thorough and time-consuming comparisons.[161] Although NIST's 2019 study found that increased photo quality did not significantly reduce the rate of FRT-generated false positives for ethnic and racial minorities absent human review,[162] fusing together FRT results with meaningful human review of those results can reduce or eliminate those disparities.[163]

The amendment also requires quality assessments by at least two forensic facial reviewers. This comports with traditional forensic protocols, where double-blind verification is used to ensure consistency and consensus.[164] Moreover, it will prevent a sole examiner from having conclusive decision-making power over whether a probe photo is of sufficient quality for FRT analysis. If these two compulsory assessments lead to different conclusions, then the probe photo will go to a third forensic facial reviewer for their own independent quality assessment. That assessment will then be final and binding. By capping the assessment to three reviewers, the amendment not only ensures the analysis does not turn on a single human's judgment,[165] which is "more susceptible to human error, bias, and performance variability across examiners,"[166] but also prevents a perpetual review process that could delay the entire criminal investigation. Notably, neither A.B. 2261 nor federal proposals have considered these kinds of forensic protocols.

Finally, the forensic facial reviewers must work in an independent organization that is free from law enforcement agencies' control.[167] This

[160] Phillips et al., *supra* note 150, at 6172. Although forensic facial experts scored 6% higher, the researchers ruled this difference statistically insignificant. *Id.*

[161] *Id.* at 6172.

[162] *See* commentary in *supra* note 118.

[163] *See* the discussion on this in Section IV(C) above.

[164] Phillips et al., *supra* note 150, at 6173.

[165] Note that in cases where the assessment decision must include a third forensic facial reviewer whose decision is then final and binding, that decision will necessarily match one of the initial two reviewers. As a result, in all cases where a third forensic facial reviewer is involved, there will be a two-to-one agreement in favor of the final and binding decision.

[166] PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., *supra* note 119, at 47.

[167] The American Polygraph Association (the "APA") is an example for how this independent organization should be structured. The APA educates polygraph examiners, provides sophisticated testing equipment, and establishes codes of conduct that each APA member must follow. *See generally About the APA*, AMERICAN POLYGRAPH

independence ensures that law enforcement officials cannot pressure the reviewers to circumvent the amendment's requirements. It also ensures that outside pressures do not influence internal decision-making. If the reviewers were personally beholden to law enforcement personnel, the amendment's efficacy would be fundamentally jeopardized.

D. Prohibiting Subjective Probe Photo Replacements But Allowing Certain Enhancements Mitigates the Probability of Misidentification

1. Probe Photo Replacements

To further reduce the probability of misidentification, the amendment would prohibit both law enforcement agencies and forensic facial reviewers from replacing low-quality probe photos during the quality assessment process. This thwarts a widespread practice where, in extreme cases, officers have replaced authentic, low-quality probe photos with high-quality photos of a suspect's purported celebrity doppelgänger.[168] These probe photo replacements can both increase the probability of misidentification[169] and subject the FRT process to subjective biases.[170] For example, one officer could perceive a probe photo suspect to look like Celebrity A, but another officer could perceive the suspect to look like Celebrity B. Even if Celebrity A and Celebrity B resemble each other to the naked eye, their individual biometric measurements could generate substantially different FRT match lists.

In a similar vein, at least half a dozen U.S. police departments use hand drawn or computer-generated eyewitness sketches in FRT analyses.[171] This is concerning because forensic scholars argue that FRT analyses utilizing eyewitness sketches are complete "fabrication[s] of facial identify points: at best an attempt to create information that isn't

ASSOCIATION, https://www.polygraph.org/about-the-apa (last visited December 28, 2021).

[168] The New York Police Department was (rightfully) criticized for substituting authentic probe photos with Internet-scraped images of Woody Harrelson and New York Knicks players. Jon Schuppe, *NYPD Used Celebrity Doppelgängers to Fudge Facial Recognition Results, Researchers Say*, NBC NEWS (May 16, 2019, 3:07 PM), https://www.nbcnews.com/news/us-news/nypd-used-celebrity-doppelg-ngers-fudge-facial-recognition-results-researchers-n1006411.

[169] *Id.* ("It doesn't matter how accurate facial recognition algorithms are if police are putting very subjective, highly edited or just wrong information into their systems . . . .").

[170] For example, one officer could look at a surveillance image and conclude that the unknown suspect looks like X celebrity. Another officer could look at the same surveillance image and conclude that the unknown suspect looks like Y celebrity.

[171] Garvie, *supra* note 26.

there in the first place and at worst the introduction of evidence that matches someone other than the person being searched for."[172] A similar fabrication was used to arrest Robert Julian-Borchak Williams in Michigan. In that case, the police added Williams' photo to a printed lineup that was given to the store's security guard.[173] That guard only saw the low-quality surveillance video that generated the initial probe photo. However, they picked Williams from the lineup.[174] The security guard's eyewitness testimony was flawed, but it still served as corroborating evidence sufficient for Williams's arrest.[175]

Researchers have recently taken interest in FRT analyses of artist sketches. In 2014, a NIST study found that using eyewitness sketches negatively impacted FRT accuracy. The study found that FRT algorithms infrequently matched the sketch to the correct photo "mate."[176] Indeed, the best algorithms successfully reported the match within their top 50 matches only 70–80% of the time.[177] NIST conditioned their findings, stating that the accuracy of matching sketches was heavily dependent on eyewitness recall, artist interpretation, and software interfaces.[178] But all of these dependencies are subjective, and they introduce significant room for error in a process that is already prone for misidentification.[179]

[172] *Id. See also* Hossein Nejati, Terence Sim & Elisa Martinez-Marroquin, *Do You See What I See? A More Realistic Eyewitness Sketch Recognition*, in 2011 INTERNATIONAL JOINT CONFERENCE ON BIOMETRICS (2011), https://www.comp.nus.edu.sg/~tsim/documents/IJCB2011_camera_ready.pdf (discussing the unreliability of traditional eyewitness sketches and recommending a more reliable model).

[173] Hill, *supra* note 1.

[174] *Id.*

[175] *Id.*

[176] Patrick Grother & Mei Ngan, *Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms, NIST Interagency Report 8009*, NAT'L INST. OF STANDARDS AND TECH. 4 (May 26, 2014), https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf.

[177] *Id.*

[178] *Id.*

[179] Garvie, *supra* note 26.

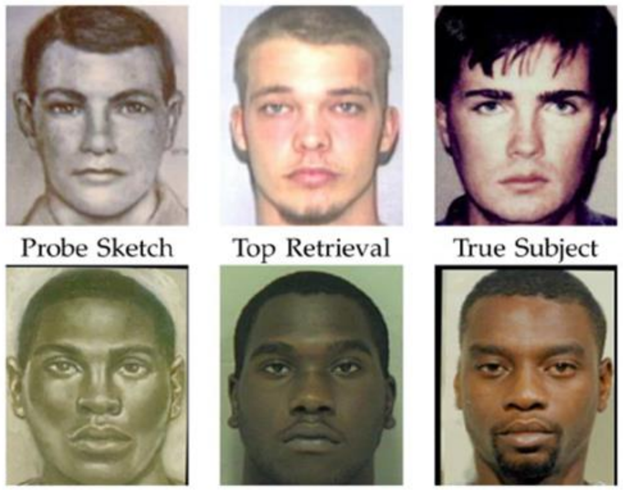

Figure 4: This figure shows: (1) how artist sketches based on eyewitness testimony can lead to drawings substantially dissimilar to true suspects; and (2) the concern that artist sketches can increase the likelihood that FRT algorithms will generate incorrect matches, which is evidenced by comparing the FRT system's top retrieval to the true suspect.[180]

In a critique of current forensic procedures, the President's Council of Advisors on Science and Technology argued that forensic examiners should establish objective procedures to generate "reproducible and consistent forensic results."[181] To achieve this objectivity, the Council posited that the steps required for feature identification, feature comparison, and matching must be well established and precisely defined.[182] The Council's recommendation contrasts current forensic examination practices, including latent fingerprints, where examiners can "adjust features manually to retrieve stored prints with the same features in analogous places."[183] Although these customizations may be useful in specific forensic fields, they are dangerous in the FRT context because the technology cannot distinguish

[180] Brendan F. Klare, Zhifeng Li & Anil K. Jain, *Matching Forensic Sketches to Mug Shot Photos*, 33 IEEE TRANSACTIONS ON PATTERN ANALYSIS & MACH. INTEL. 639, 645 (2011), http://biometrics.cse.msu.edu/Publications/Face/KlareLiJain_MatchingForensicSketchesMugshotPhotos_PAMI10.pdf.

[181] PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., *supra* note 119, at 48.

[182] *Id.*

[183] *See* NAT'L RSCH. COUNCIL, STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 270 (2009) ("[S]ubmitting a latent print for examination is a more customized process, requiring fingerprint examiners to mark or adjust the features manually to retrieve stored prints with the same features in analogous places. Because latent prints normally are not as clear or as complete as images from a 10-print card, the image processing algorithm use for 10-prints are not as good as the human eye in spotting features in poor images.").

original facial characteristics from those fabricated via enhancement.[184]

The proposed amendment's prohibition on probe photo replacements would achieve objectivity by barring officers from using their individual discretion to replace low-quality probes. This amendment complies with the Council's advice for ensuring that forensics continue to become more reliable over time.[185] Indeed, by combining compulsory probe photo quality assessments with an express prohibition on replacement, the proposed amendment would ensure that all FRT searches are solely dependent on authentic evidence. This thwarts biases at both the law enforcement and examining levels, which can bolster public trust in the FRT process. It also eliminates the reliance on controversial and unreliable eyewitness sketches that could generate inconsistent results. As FRT is especially critiqued for its purported racial and ethnic disparities, it is unwise to continue providing law enforcement free rein to replace probe photos.

2. *Probe Photo Enhancements*

Various photo enhancement procedures have shown promise for increasing FRT accuracy. Thus, the amendment would allow an independent organization of forensic facial reviewers to conduct certain enhancements along various photo quality characteristics, as promulgated by NIST.

In a 2021 study using face images from 33 actual FRT analyses, researchers concluded that "image denoising" can improve FRT results.[186] Image denoising is the process of removing "image information that is useless or interfering with the target information" while preserving important image features.[187] High image noise is caused by several factors, including the length of exposure, the physical temperature of objects in a picture, and the sensitivity of the camera.[188] Noise is often greater in low-light images, like nighttime surveillance

[184] Garvie, *supra* note 26.

[185] *See generally* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., *supra* note 119 (qualifying the efficacy of established forensic procedures and making recommendations to address significant concerns).

[186] *See* Jinhua Zeng, Xiulian Qiu & Shaopei Shi, *Image Processing Effects on the Deep Face Recognition System*, 18 MATHEMATICAL BIOSCIENCES & ENG'G 1187, 1187–88 (2021), https://www.aimspress.com/article/doi/10.3934/mbe.2021064).

[187] *Id.*

[188] Julia Kuzmenko McKim, *Understanding Image Noise*, RETOUCHING ACAD., https://retouchingacademy.com/qualities-of-digital-images-understanding-image-noise/ (last visited Oct. 17, 2021).

videos.[189] Extreme noise often manifests as a grainy image and sometimes discoloration, which distort the visual details of a photo.[190]

Scientists and mathematicians have introduced several procedures for denoising images, each employing a unique mathematical algorithm to achieve optimal photo quality by reducing noise's negative effects without distorting the photo subject itself.[191] Although the 2021 study demonstrated that denoising can increase image blurriness, the highest-scoring denoising procedure improved FRT accuracy by 2.445%.[192] This is a significant improvement that cannot be ignored, and the proposed amendment would permit enhancements like denoising so long as NIST considers them to be reliably tested and proven.

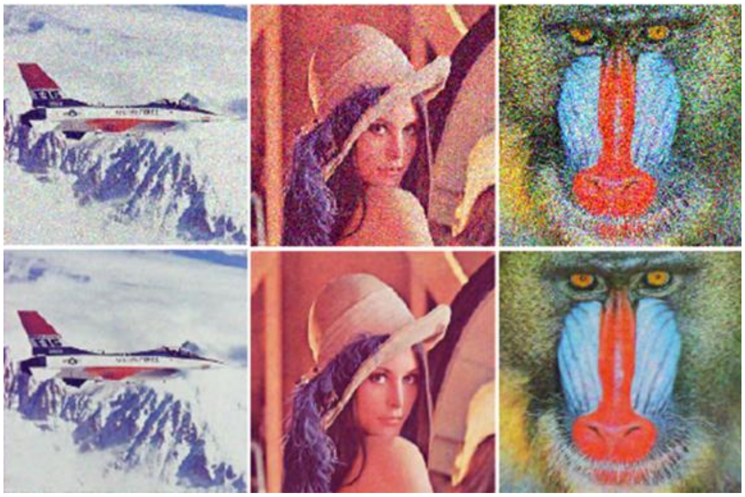

Figure 5: This figure shows the difference between a noisy image (on the top row) versus an image with reduced noise.[193] As you can see, the denoised image appears somewhat blurry to the human eye. However, these images increase FRT accuracy compared to their noisy counterparts.

[189] *Understanding the Basics of Low Light Photography*, PHOTO REV., https://www.photoreview.com.au/tips/shooting/understanding-the-basics-of-low-light-photography/ (last visited Oct. 17, 2021).

[190] *Id.*

[191] Vandana Roy & Shailja Shukla, *Spatial and Transform Domain Filtering Method for Image De-Noising: A Review*, 7 L.J. MODERN EDUC. & COMPUT. S. 41 (2013), http://mecs-press.org.ua/ijmecs/ijmecs-v5-n7/IJMECS-V5-N7-5.pdf).

[192] Zeng, *supra* note 186, at 1194.

[193] Image adopted from AARON WETZLER & RON KIMMEL, EFFICIENT BELTRAMI FLOW IN PATCH-SPACE 2 (2011), http://cs.technion.ac.il/~twerd/WetzlerKimmel-SSVM-2011.pdf).

The 2021 study cautioned, however, that "pure" image enhancements were not as successful as denoising.[194] The researchers concluded that pure image enhancement increased the visual display of the image and improved human perception of items within the photo, but it "also partially augmented the image noises," [195] causing slight image distortion. As compared to the 2.445% increase in accuracy of the denoising procedure, this pure image enhancement increased FRT accuracy by only 0.864%.[196] This improvement may not be sufficient to justify pure photo enhancements that merely improve the quality of a photo for human pleasure but have little effect on FRT accuracy.[197] The amendment would delegate these decisions to NIST because of its unparalleled expertise in FRT scientific research.

The proposed amendment's limitation on enhancements is further justified by the fact that certain developers have added internal enhancement features to FRT systems.[198] NEC America's NeoFace Widenet software enables law enforcement personnel to substantially alter a probe photo, including turning a head towards the camera, changing pose, and increasing an image's sharpness.[199] Although the company claims these features will increase accuracy, the company has offered no proof. These procedures are closer to photo replacement than to denoising, because denoising only changes the digital features of the image and does not alter the subject's physical position. There is no doubt that more research is required to understand how image enhancements affect FRT accuracy, but a complete ban on photo enhancements (as opposed to photo replacements) could be seen as draconian, as the above studies have shown that certain enhancement procedures—namely denoising—can have positive results on FRT analyses.

V. REBUTTALS AGAINST CRITICISMS

Although the proposed amendment places more stringent restrictions on law enforcement's FRT use than A.B. 2261 would have, opponents may still argue that: (1) it is self-contradictory because it seeks to harness FRT's time efficiencies while simultaneously enacting time-consuming regulatory protocols; (2) it could bloat California's debt; and

[194] Zeng, *supra* note 186, at 1197.
[195] *Id.*
[196] *Id.* at 1194.
[197] It is interesting to note that images that appear blurry to the naked eye increase FRT accuracy more than photos that are more pleasurable to the human eye.
[198] NEC America, *supra* note 24.
[199] *Id.*

(3) by adding a third-party independent organization of forensic facial reviewers, the amendment creates another potential source for data breaches. As discussed below, however, each of these critiques are somewhat illusory.

A. Self-Contradictory

First, opponents may argue that the proposed amendment is self-contradictory because the investigative efficiencies generated by FRT will be negated by a burdensome, dilatory probe photo review process. This is misguided. Yes, requiring at least two *ex ante* probe photo quality assessments can be cumbersome. But delays are not unique to the *ex ante* approach. Indeed, the unregulated procedures currently used by law enforcement agencies could have administrative delays on the back end of FRT analyses. For example, the FBI's FACE Systems Unit is required to manually assess the quality of each FRT-generated match before reporting those matches to field officers.[200] As stated, FRT identification systems are used to report one-to-many matches in *post hoc* investigations.[201] Considering these systems can generate hundreds of matches with lower confidence scores,[202] the back-end manual assessments could be extremely time consuming and expensive, especially when matching accuracy is prioritized. Although a specific time has not been assigned to this back-end review process, some real-world FRT identifications have involved several hundred potential matches and multiple stages of human review.[203]

On the other hand, the *ex ante* quality assessments inherently increase the probability that FRT systems will report more accurate matches. When adding the effect of increased confidence scores, the amendment makes it more likely that the FRT system will not report matches closer to the minimum confidence threshold which, in the grand scheme of things, will save time by reducing the number of matches that need to be reviewed by the forensic facial reviewers. Thus, although it is impossible to estimate specifically how much time would be spent on the *ex ante* assessments, relying on back-end assessments is not immune to time delays.

[200] Babcock, *supra* note 63.
[201] *Supra* Section I.
[202] *See generally* Parker, *supra* note 66.
[203] *See generally id.*

B. Too Expensive

Opponents may argue that the amendment is too expensive because it creates a new organization of forensic facial reviewers that would be funded by the California state government. When added to the cost of FRT systems themselves, some opponents will argue that an outright ban on FRT would be more cost-effective. This criticism fails to appreciate the economic benefits of the FRT industry. Globally, the facial recognition industry is expected to grow from a $4.4 billion valuation in 2019 to more than $10.9 billion in 2025—and $12.92 billion in 2027.[204] In the United States alone, the facial recognition industry is expected to grow from $3.2 billion in 2019 to more than $7 billion by 2024.[205] California is home to two of the 13 largest global FRT companies.[206] By continuing to embrace the projected growth of the industry, albeit with statewide regulation, the proposed amendment would ensure job security for Californians already employed by these companies. It could also increase long-term tax revenue for the state, again assuming the companies' growth matches that of the entire industry. A blanket ban, on the other hand, could lead companies to relocate to states where regulation embraces experimental FRT use and where they can "innovate, grow, and take risks more easily than" they could in California.[207]

Aside from corporations, there are also smaller, localized facial recognition developers in California. Headquartered in Southern California, there's PopID, "the nation's first payment system based on facial recognition."[208] PopID is currently used in a number of restaurants

[204] REPORTLINKER, *Facial Recognition Market – Growth, Trends, and Forecast (2020–2025)* (May 7, 2020), https://www.reportlinker.com/p05891613/Facial-Recognition-Market-Growth-Trends-and-Forecast.html?utm_source=PRN; FORTUNE BUS. INSIGHTS, Facial Recognition Market to Reach USD 12.92 Billion by 2027 (July 9, 2020, 2:23 PM), https://www.globenewswire.com/news-release/2020/07/09/2059692/0/en/Facial-Recognition-Market-to-Reach-USD-12-92-Billion-by-2027-Increasing-Demand-for-Advanced-Video-Surveillance-Systems-to-Augur-Growth-Fortune-Business-InsightsTM.html. The ReportLinker report notes that the Asia-Pacific region will experience the highest market growth, as countries like China invest heavily in the facial recognition industry for surveillance purposes.

[205] Nicole Martin, *The Major Concerns Around Facial Recognition Technology*, FORBES (Sept. 25, 2019, 3:15 PM), https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/#20c3539a4fe3.

[206] These two companies include FaceFirst, Inc., which is based in Encino, California, and Intellivision, which is based in San Jose. FORTUNE BUS. INSIGHTS, *supra* note 204.

[207] Michael Roennevig, *Why Do Companies Need to Go Overseas?*, CHRON, https://smallbusiness.chron.com/companies-need-overseas-58292.html (last visited Oct. 17, 2021).

[208] Sam Dean, *Forget Credit Cards – Now You Can Pay With Your Face. Creepy or*

surrounding the company's Pasadena headquarters.[209] During the COVID-19 pandemic, contactless payment has been a viable lifeline for small businesses struggling amid widespread economic turmoil. California Assemblyman Chau was cognizant of this reality when drafting A.B. 2261. He recently stated, "now that we are fighting COVID-19 and deploying touchless sensor technology to measure body temperatures and track individuals, facial recognition technology is brought to the forefront."[210] When analyzing these economic factors, a statewide ban or moratorium on all FRT use would make little economic sense.

Some commentators may argue that the proposed amendment would restrict law enforcement's FRT use so severely that it would operate as a constructive ban. This argument ignores the fact that even significant restrictions will not stymie the industry's growth, because regulations embracing limited experimental approaches will permit continued FRT testing and development.[211] Moratoriums and blanket bans could stymie the growth of the entire facial recognition industry, which would disincentivize FRT developers from improving their systems. This would eliminate an industry that is projected to help California's economy. It could also lead to job transfers out of California to states or countries where FRT is permitted. This potential FRT exodus would deteriorate California's strong position in the FRT industry, effectively placing the state behind the technological arms-race and resulting in the loss of tax revenue.

C. Increases Hacking Potential

Finally, opponents may argue that transferring authentic probe photo evidence to a third-party agency will increase the probability of data hacking. According to opponents, this is concerning because probe photos typically contain personally identifiable facial images collected from crime scenes. As a result, a malicious third-party hacker could infiltrate the FRT database or computer servers and disseminate these images to the public, which could threaten someone's right to privacy and

Cool?, L.A. TIMES (Aug. 14, 2020, 5:00 AM), https://www.latimes.com/business/technology/story/2020-08-14/facial-recognition-payment-technology.

[209] *Id.*

[210] Evan Symon, *Controversial Facial Recognition Regulation Bill Stalled in Appropriations Committee*, CAL. GLOBE (June 3, 2020, 6:23 PM), https://californiaglobe.com/section-2/controversial-facial-recognition-regulation-bill-stalled-in-appropriations-committee/.

[211] COMM'N NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *supra* note 35, at 10.

endanger their constitutional right to a presumption of innocence until proven guilty.

This critique fails to consider the realities of our digital world. In our technologically advanced society, no electronic database is completely foolproof. Thus, arguing that this amendment uniquely endangers an individual's right to privacy ignores that the same steps taken to prevent hacking of one server can be used to prevent the hacking of data stored across several loci, including cyber training, firewalls, and sophisticated authentication requirements. Additionally, the proposed amendment affirmatively addresses this concern by requiring that third-party agencies permanently delete all electronic and physical probe photocopies within thirty days of either determining a probe photo is insufficient for FRT analysis or submitting FRT-generated matches to law enforcement agencies. This provision ensures that multiple databases store the images simultaneously for a short period of time. Therefore, the amendment enacts reasonable measures to prevent mass data leaks that threaten the privacy of individuals in probe photos.

CONCLUSION

FRT is a powerful technological tool that will continue to permeate various aspects of society. There are many valid arguments in opposition to FRT, but there are various ways to mitigate the problems associated with the technology without banning it entirely, including enacting regulations that control the data that imputes bias into the technology. As FRT serves an important tool in *post hoc* criminal investigations, the California legislature should not enact strict bans or indefinite moratoriums that preclude law enforcement agencies from harnessing the technology's investigation efficiencies. Such draconian regulations would stifle innovation and could prove detrimental to a burgeoning industry that provides California with current and future economic benefits.

A.B. 2261 did not go far enough to adequately address legitimate concerns regarding law enforcement's use of FRT, especially the disparate effects on marginalized and minority groups. The goal of this Article is to provide the California legislature with a concrete roadmap for an effective, middle-ground regulatory framework. If the proposed regulation is enacted, it could strike a balance between FRT's core benefits and limitations to exploit its efficiencies while protecting people in California from the dangers of improper use. If successful, the California amendment could be adopted in other states and by Congress. Regardless, two things are certain: (1) A.B. 2261 did not pass as currently written due to its shortcomings in addressing civil rights concerns; and (2) FRT is not going anywhere soon. An amended regulation is necessary and California can lead the way.