Seattle Journal for Social Justice

Volume 19
Issue 1 *Fall 2020*

Article 18

12-31-2020

Facial Recognition in Law Enforcement

Cameron Martin

Recommended Citation
Martin, Cameron (2020) "Facial Recognition in Law Enforcement," *Seattle Journal for Social Justice*: Vol. 19 : Iss. 1 , Article 18.
Available at: https://digitalcommons.law.seattleu.edu/sjsj/vol19/iss1/18

Facial Recognition in Law Enforcement

Cameron Martin*

To be considered:[1] Michael Thomas, a resident of Carrollton, Michigan, has been arrested repeatedly for crimes he did not commit. On October 2018, Thomas saw a neighbor preparing to cut a tree from Thomas's land. The two of them got into a heated argument when the neighbor claimed that the tree posed a danger in the case of a storm. Someone called the police, and a patrolman of the Carrolton Township Police Department (CTPD), Jack Vincennes, responded to the call. Patrolman Vincennes broke up the fight, but the facial-recognition feature of his CopperFR body camera attached to the front of his uniform flagged Thomas. This camera automatically took a picture of Thomas and sent it back to the precinct. The system identified Thomas as another person, Rollo Smith, who was the subject of an outstanding arrest warrant for robbery and murder in Los Angeles, California. Sergeant Edward Exley of the Los Angeles Police Department (LAPD) entered the warrant into CopperFR, which also contained three surveillance-video stills of Smith.

Vincennes arrested Thomas, who was held for three days while the Carrolton and Los Angeles Police Departments (LAPD) conducted further investigations. On the fourth day, a comparison of his fingerprints and physical description with the LAPD's records definitively showed that Thomas was not Smith, who, aside from having different fingerprints, also had several distinctive scars and tattoos. Thomas was released.

*J.D. 2021, Seattle University School of Law. The author would like to thank the editors at The Seattle Journal for Social Justice, and Professor Steve Tapia, Distinguished Practitioner in Residence at Seattle University School of Law. All of their keen eyes, patience, and support have truly made this article into something worthwhile.

[1] This excerpt was adapted from JAMES GRIMMELMANN, INTERNET LAW: CASES & PROBLEMS 664–65 (Semaphore Press ed., 9th ed. 2019).

In March 2019, Thomas was driving when he was stopped for failure to use a turn signal by Bay County sheriff's deputy Bud White outside of Saginaw, Michigan. Deputy White used a CopperFR body camera which also flagged Thomas as Smith. Smith's same warrants remained outstanding. As a result, Deputy White ordered Thomas out of the car at gunpoint, then searched, handcuffed, and arrested him. Two hours after Deputy White made phone calls to the Saginaw Police and the LAPD, Thomas was released.

Since the last arrest in March, Thomas has been arrested three more times—twice at gunpoint—by police in Michigan and Texas. Each time, Thomas was released after his true identity was confirmed. He contacted CopperFR, which refused to discuss the specifics of its system or Smith's record with him, stating that "only the originating law enforcement agency could delete, amend, or correct the computer warrant entry." He also spoke to Captain Dudley Smith of the LAPD, who refused to delete the entry for Smith citing the "need to preserve an ongoing investigation."[2]

Although the above is just a hypothetical scenario, a similar interaction has actually occurred. Robert Julian-Borchak Williams, a Black man in Michigan, was arrested in front of his home and taken to a detention center based on a faulty facial recognition algorithmic match.[3] A low quality image from a jewelry store theft had matched with Mr. Williams' driver's license photo which led to his subsequent arrest.[4] Fortunately, he was later released and the county prosecutor claimed his face and fingerprint data would be expunged.[5] However, what will make up for the time Mr. Williams spent in jail due to a faulty unregulated system? There are currently no laws, regulations, or standards keeping this interaction between

[2] *Id.*

[3] Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020, updated Aug. 3, 2020) https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/ZRA7-94NF].

[4] *Id.*

[5] *Id.*

law enforcement, facial recognition technology, and the public from occurring. Although some smaller municipalities have banned certain uses of facial recognition, instances like this could become the norm.

I. Introduction

The ungoverned use of facial recognition software can result in significant disparities in improper applications against already subjugated groups; ultimately, it poses significant threats to both civil rights and civil liberties if used by law enforcement today due to its untested and biased capabilities.[6]

Facial recognition software or technology (FRT) is software that can make use of a camera and image to analyze a human face for the purpose of identification.[7] To identify a face, FRT takes the biometric data provided by a captured image from a photograph or video and matches it to other images in a data set.[8] There is a wide variety of uses for FRT, such as unlocking a cell phone, identifying a person in a photo posted on a social networking site, or identifying recently landed passengers at an airport security checkpoint.[9] Requiring a face to unlock a personal cell phone provides users with a sense of security.[10] A user makes the choice to allow the phone to take their picture and use the facial recognition feature as a self-selected password; therefore, a user decides on their own to use their face to unlock

[6] *See generally* H.B. 1654, 66th Leg. Reg. Sess. (Wash. 2019).

[7] *Face Recognition Technology*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology [https://perma.cc/4ZM6-CKCS].

[8] Steve Symanovich, *How Does Facial Recognition Work?*, NORTONLIFELOCK INC., https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html [https://perma.cc/UA7L-9BYG].

[9] *Id.*

[10] Lynn La, *10 Best Phones with Facial Recognition: iPhone X, Note 9, LG G7 and More*, CNET (Aug. 22, 2018, 9:00PM), https://www.cnet.com/news/10-best-phones-with-facial-recognition-iphone-x-note-9-galaxy-s9-lg-g7/ [https://perma.cc/P7MF-4UUW].

their device.[11] In order to get an accurate face scan on a phone, the user must do multiple scans.[12] For the user, there may be an increased sense of ease in not having to enter, or remember, the multiple digits or letters of a password to unlock the phone.[13] Furthermore, security is increased by using a face rather than a password.[14] According to Xfinity, "The chances of a random person being able to unlock your phone are one in a million."[15] Theoretically, unless the user's phone is hacked or the user has an identical twin, there should not be a way into the phone.[16] The user's picture is taken and only stored in the phone.[17] However, not all uses of FRT are that straightforward, nor are all FRT face scans done by the choice of the subject of the technology.[18] The use of facial recognition software relies on the gathering of information, which is often done without any consent given by the parties being analyzed by the software.[19]

Due to the growth of the technology market, the reach of facial recognition software and its reported capabilities beyond just face matching are consistently expanding.[20] Currently, "[t]he facial recognition market is expected to grow to $7.7 billion in 2022 from $4 billion in 2017. That growth is because of new commercial applications. This technology can be used for everything from surveillance to marketing."[21] Top FRT companies

[11] *See Use Face ID on Your iPhone or iPad Pro*, APPLE, INC., https://support.apple.com/en-us/HT208109 [https://perma.cc/B3XC-GBZ2].

[12] *Id.*

[13] *See What Is Facial Recognition on a Phone*, XFINITY (Jan. 31, 2019), https://www.xfinity.com/hub/mobile/facial-recognition-on-phone [https://perma.cc/S3LX-ENPU].

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *See* Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, GEO. L. CTR. ON PRIVACY & TECH. (May 16, 2019), https://www.americaunderwatch.com/ [https://perma.cc/972A-FGA2].

[19] *See Face Recognition Technology*, *supra* note 7.

[20] Symanovich, *supra* note 8.

[21] *Id.*

market their technology in fairly straightforward ways, often with a direct call to law enforcement users.[22] Amazon's FRT "Rekognition" advertises that it "provides highly accurate facial analysis, face comparison, and face search capabilities. You can detect, analyze, and compare faces for a wide variety of use cases, including user verification, cataloging, people counting, and public safety."[23] Microsoft's Azure Face APIs provide services such as face detection; face matching, a feature to find similar looking faces; and person identification.[24] In contrast, IBM markets their Watson Visual Recognition API specifically for use in real-time.[25] Law enforcement agencies have hired some companies to do specific research and technological expansion for their departments.[26] In late 2016 and early 2017, IBM attempted to market its facial recognition product's newly developed ability to search for people by ethnicity specifically to law enforcement.[27] An IBM researcher at that time stated that it developed the software with ethnicity tags at the request of the NYPD, but the NYPD decided not to use the new software after testing it.[28] The IBM researcher affirmed, "We would have not explored it had the NYPD told us, 'We don't

[22] *What Is Amazon Rekognition?*, AMAZON WEB SERVS., INC., https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html [https://perma.cc/26R7-FV72].

[23] *Id.*

[24] *What is the Azure Face Service?*, MICROSOFT (Sept. 17, 2020), https://docs.microsoft.com/en-us/azure/cognitive-services/face/overview [https://perma.cc/V7HU-YUPL].

[25] *Integrating IBM Intelligent Video Analytics with IBM i2 Facial Recognition*, IBM, https://www.ibm.com/support/knowledgecenter/en/SS88XH_1.6.1/iva/int_i2frs_intro.html [https://perma.cc/X8LA-NFYB].

[26] George Joseph & Kenneth Lipp, *IBM Used NYPD Surveillance Footage to Develop Technology that Lets Police Search by Skin Color*, INTERCEPT (Sept. 6, 2018), https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/ [https://perma.cc/54JB-L2UK].

[27] *Id.*

[28] *Id.*

want to do that,'" . . . "No company is going to spend money where there's not customer interest."[29]

If the IBM researcher's assertion is to be believed, that companies are only expanding their FRT offerings based on market demand, then Amazon's "Rekognition" software's purported capability to detect human emotions must be desirable.[30] In 2019, Amazon expanded Rekognition's range of detectable emotions to be competitive with other FRT companies who also purport to be able to recognize emotions. [31] In a blog post, Amazon announced it had "improved accuracy for emotion detection (for all 7 emotions [previously detected]: 'Happy,' 'Sad,' 'Angry,' 'Surprised,' 'Disgusted,' 'Calm,' and 'Confused') and added a new emotion: 'Fear.'"[32] The technology registers facial expressions, such as raised eyebrows or a downturned mouth, and attempts to turn those into a determination of emotion.[33] Aside from the negative implications of what might happen if this particular part of FRT were used in law enforcement and the potential to heighten alarm in conflict situations if the technology registeres the emotion as fearful or angry, a study of over 1,000 academic papers has determined that "there just isn't a strong enough correlation between facial expressions and actual human emotions, and common methods for training algorithms to spot emotions present a host of other problems." [34] Yet, this

[29] *Id.*

[30] *See* Janus Rose, *Amazon Says the Face Recognition Tech it Sells to Cops Can Now Detect 'Fear,'* VICE (Aug. 13, 2019, 2:47 PM), https://www.vice.com/en_us/article/7x59z9/the-facial-recognition-system-amazon-sells-to-cops-can-now-detect-fear [https://perma.cc/EU4H-U3GF].

[31] *Id.*

[32] Press Release, Amazon Web Servs., Inc., Amazon Rekognition Improves Face Analysis (Aug. 12, 2019), https://aws.amazon.com/about-aws/whats-new/2019/08/amazon-rekognition-improves-face-analysis/ [https://perma.cc/FZ5U-G33Z].

[33] Rose, *supra* note 30.

[34] *Id.*

emotional detection technology has already been used in hiring processes and attempts to determine if someone is trying to commit insurance fraud.[35]

Other companies have either developed or are working on software that can determine a person's sexuality, propensity to commit crimes, Intelligence Quotient, and propensity to commit terrorism, solely from faces.[36] Most known——or reported——uses of FRT by law enforcement are (1) basic face detection, where the facial recognition software is able to scan an image and determine where faces are present in that image, and (2) face matching, the most contentious use, where probe images (a picture or screenshot from a camera) are run against a database of photos to determine if there is a match. However, the lack of regulation on the use of FRT in law enforcement and the continued expansion of the FRT capabilities as the market grows highlight the need to reconsider the wild west mentality toward FRT in law enforcement. If FRT is used to imply intent to commit a crime, then we end up in a world brushing against due process violations or extremely heightened surveillance at the very least. As determined by the United States Supreme Court, "A person does not surrender all Fourth Amendment [privacy] protection by venturing into the public sphere."[37]

The first section of this article will discuss generally on how facial recognition functions. The second section includes a discussion of the current inherent inaccuracies of facial recognition technology by way of identifying not only the incapabilities of the technology itself, but also the inherent biases in the coding of the technology. The third section provides an in-depth look at how the technology is acquired and used by law enforcement agencies without oversight or regulation. Fourth, this article

[35] Angela Chen, *Computers Can't Tell if You're Happy when You Smile*, MIT TECH. REV. (July 26, 2019), https://www.technologyreview.com/s/614015/emotion-recognition-technology-artifical-intelligence-inaccurate-psychology/ [https://perma.cc/M7BT-649J].

[36] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in*
Commercial Gender Classification, 81 PROC. MACH. LEARNING RES. 1, 2–3 (2018).

[37] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

proposes a legislative solution for municipalities, beginning with a moratorium on the unfettered use of facial recognition technology by law enforcement and concluding with suggestions for possible reimplementation where it is deemed reasonable and useful.

II. HOW FACIAL RECOGNITION WORKS

When facial recognition is not done on a phone, the process works a bit differently. To take a reading on a face, FRT analyzes key facial landmarks in the geometry of the face.[38] Facial landmarks include the distance between the eyes, the size of the nose, and the distance between the nose and the chin.[39] Collectively, the size and distance of the facial landmarks create a facial signature.[40] Different FRT systems gather different amounts of facial information, and some systems are purported to identify sixty-eight different facial landmarks.[41] The collection of measurements is then used to create the unique formula that is a facial signature or face template.[42] Theoretically, a face template can function as well as or better than a person's own signature—it is extremely unique.[43] It is important to note that a face template, a conglomeration of the algorithmic choices programmed into the FRT, is not the same as a photograph.[44] If the FRT is not set to detect certain features (an issue discussed below), then those features will not be taken into account when distinguishing between matches.[45]

For the recognition part of FRT to occur, the mathematically created face template must be matched to other face templates generated from a

[38] Symanovich, *supra* note 8.
[39] *See id.*
[40] *Id.*
[41] *See id.*
[42] *Id.*
[43] *See What Is Facial Recognition on a Phone*, *supra* note 13.
[44] *Street-Level Surveillance: Face Recognition*, ELEC. FRONTIER FOUND. (Oct. 24, 2017), https://www.eff.org/pages/face-recognition [https://perma.cc/VSV3-VGFQ].
[45] *See id.*

collection of images.[46] These images come from a database of "known faces."[47] The databases used for FRT are dependent on the user. For example, a company using Amazon's "Rekognition" simply uploads the images they would like the technology to match up.[48] Additionally, companies may use FRT for facial verification in their building security to match employee ID pictures with those going in or out of a building or secure room. In 2016, as many as forty-three out of fifty states used some form of FRT through their Departments of Motor Vehicles' creation of their databases from driver's license photos.[49] The Federal Bureau of Investigations has a database of photos collected through its own repository of mugshot and correctional photos and expanded by driver's license photos and visa applicant photos from partnerships with local state and municipal agencies.[50] As of 2019, this database had over 641 million faces.[51]

III. INACCURACIES AND BIASES IN FACIAL RECOGNITION TECHNOLOGY

When FRT is making a match, the software allows for a choice on how accurate the match may be.[52] The necessary accuracy will likely be dependent on the situation; for instance, a 100% accurate match is not

[46] *See id.*

[47] Symanovich, *supra* note 8.

[48] *Amazon Rekognition FAQs*, AMAZON WEB SERVS., INC., https://aws.amazon.com/rekognition/faqs/ [https://perma.cc/MN5B-GSCT].

[49] Russell Brandom, *How States Use Facial Recognition to Sniff Out Driver's License Fraud*, VERGE (Aug. 15, 2016, 8:00 AM), https://www.theverge.com/2016/8/15/12478212/facial-recognition-drivers-license-photo-realid-dmv [https://perma.cc/A4FY-4GDP].

[50] GRETTA L. GOODWIN, U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-579T, FACE RECOGNITION TECHNOLOGY: DOJ AND FBI HAVE TAKEN SOME ACTIONS IN RESPONSE TO GAO RECOMMENDATIONS TO ENSURE PRIVACY AND ACCURACY, BUT ADDITIONAL WORK REMAINS 5–6 (2019).

[51] *Id.*

[52] Ben Virdee-Chapman, *The Secret to Better Face Recognition Accuracy: Thresholds*, KAIROS (Sept. 27, 2018), https://www.kairos.com/blog/the-secret-to-better-face-recognition-accuracy-thresholds [https://perma.cc/LZ6X-XPFH].

needed for a phone application or game that is meant to tell the user what famous person they look most like. The range of accuracy is determined by the user-chosen threshold which is a "user setting for Facial Recognition Systems for authentication, verification or identification. The acceptance or rejection of a Facial Template match is dependent on the match score falling above or below the threshold. The threshold is adjustable within the Facial Recognition System."[53] Theoretically, if facial recognition is used in law enforcement, a threshold could be set at 100%; if it were, only perfect matches would be made. The greatest issue of FRT use in law enforcement arises where imperfect matches are made. Currently, due to insufficient algorithms from which the technology draws or problems in the algorithmic programming of the facial recognition software, there is an increased chance of a mismatch for groups of people that are not male and white.[54] The National Institute of Standards and Technology (NIST),[55] a non-regulatory physical sciences laboratory that functions out of the United States Department of Commerce, has been posting its demographic testing results on FRT since 2017.[56] NIST's findings have determined that even the best FRT algorithms have a mismatch rate that is five to ten times greater for persons of color. [57] Idemia, a technology used by Customs and Border Protection in the United States, "falsely matched different white women's faces at a rate of one in 10,000," yet, "it falsely matched black women's faces about once in 1,000—10 times more frequently" at the same threshold.[58] Although NIST's overall findings reported that between 2014 and 2018, FRT became twenty times better at generating matches, the

[53] *Id.*
[54] *See* Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (July 22, 2019), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/ [https://perma.cc/2BNR-WDX8].
[55] *About NIST*, NAT'L INST. OF STANDARDS & TECH. (updated June 14, 2017), https://www.nist.gov/about-nist [https://perma.cc/WJ3L-KZF3].
[56] Simonite, *supra* note 54.
[57] *Id.*
[58] *Id.*

overall disparity in matching for different demographics should not be discounted.[59] When facial recognition is used in law enforcement, that disparity can lead to drastically different outcomes for different communities. Importantly, NIST's tests found great variance in accuracy, with some new algorithms underperforming the older algorithms when minimizing false positives, which should be of the utmost importance in law enforcement use. [60]

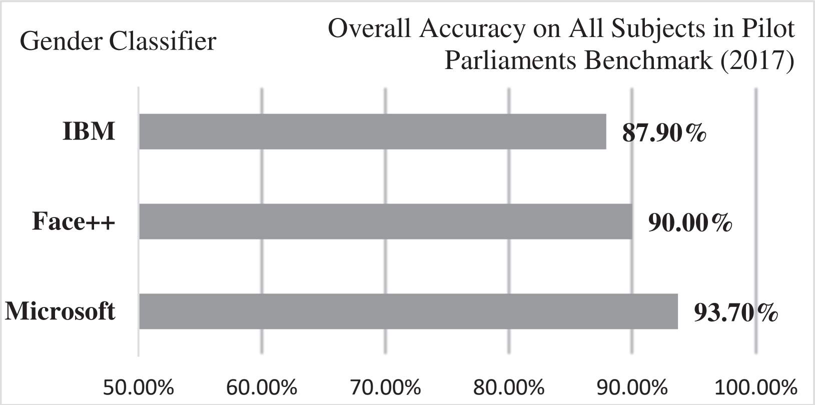
Gender Shades, another independent study that focused mainly on the disparity in determining matches with FRT between different skin shades and gender, found similarly enormous disparities.[61] This study examined reasons why FRT is coming up with biased search results based on skin tones and concluded that the actual programming of the software itself is to blame because of the phenotypic (the way people look, e.g. skin pigmentation) disparities in the initial datasets, or "benchmark datasets."[62]

[59] *See 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 [https://perma.cc/U8QX-LC94].

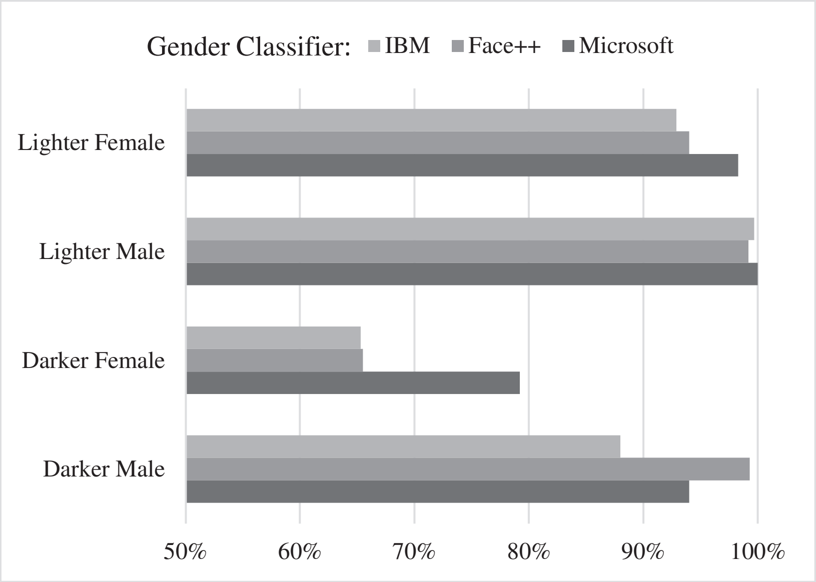
[60] *See id.*

[61] Buolamwini & Gebru, *supra* note 36.

[62] *Id.*



[63]



[64]

[63] *Results*, GENDER SHADES (2018), http://gendershades.org/overview.html [https://perma.cc/YZV6-7T26].

[64] *Id.*

The Gender Shades study shows the difference, when evaluating the capabilities of an FRT, between the technologies' reported match capability and the actual matching ability when broken down by gender and skin shade. The test evaluated those in its matching database according to a "dermatologist approved Fitzpatrick skin type classification system [which] was used to label faces as Fitzpatrick Types I, II, III, IV, V, or VI."[65] Types I, II, and III are classified as "lighter" in this study, and Types IV, V, and VI are grouped as "darker." [66]

The Gender Shades study shows that given the same threshold in which to determine a match, each top company was able to better determine matches on males than females and were signifcantly better at determining accurate matches on women of lighter skin tones than those of darker skin tones.[67] Ultimately, the results of this study are comparable to those of NIST: both portray the stark difference between an FRT's capability to accurately find matches for males of lighter skin tones and males of darker skin tones. This study calls for "rigorous reporting on the performance metrics" focused on "increasing phenotypic and demographic representation in face datasets and algorithmic evaluation."[68] Therefore, FRT systems may be biased from their implementation and, if ever used, need to be continually tested. Law enforcement agencies should take these kinds of differences into account when determining what FRT systems they might use, and it should be intrinsic to the decision to use a system at all. If the system is used in policing and its results are statistically biased, that will ultimately lead to biased policing.

Another study was conducted in 2018 by the American Civil Liberties Union (ACLU) using "Rekognition," Amazon's facial recognition software

[65] *See Results*, *supra* note 63.

[66] *See id.*

[67] *Id.*

[68] Buolamwini & Gebru, *supra* note 36.

that was sold to law enforcement agencies in the past.[69] In this test, the software incorrectly matched twenty-eight members of Congress to those in a database of mugshots, identifying these members of Congress as people who have been arrested for a crime.[70] According to the ACLU, "nearly 40 percent of Rekognition's false matches in our test were of people of color, even though they make up only 20 percent of Congress."[71] The ACLU used publicly available arrest photos and used the Amazon recommended threshold settings to run the test.[72] A match test for all of the members of the House of Representatives and the Senate cost less than $13.00.[73] A few issues arose from this testing: in addition to the disparity in accuracy for those of darker skin tones, the rather inexpensive pricing likely made FRT seem like a relatively cheap tool for law enforcement to use. Although it might be cost effective, the inaccuracy related to skin color could lead to frightening results in a real-time policing situation. For example, a routine traffic stop could turn into a dangerous situation if police use facial recognition in a body camera and the driver is mismatched.

Another troubling issue that has emerged from studies of FRT is that the technology can only determine gender in binary terms of male or female.[74] A study surveying the most popular FRT companies found that only one company, Clarifai, used a classification that was not strictly binary; Clarifai classified "gender appearance," returning values of "feminine" and "masculine," rather than the binaries of "female" and "male" used by other

[69] *See* Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018, 8:00 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/S8NP-BA7Y].

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] *See id.*

[74] *See* Buolamwini & Gebru, *supra* note 36. ("In this work we use the sex labels of 'male' and 'female' to define gender classes since the evaluated benchmarks and classification systems use these binary labels.").

companies.[75] The table below shows that most FRTs define a gender category; some FRTs also assign a probability score between zero and one for each classification.[76]

Facial Analysis and Image Labeling Services[77]

Name	***Service Name***	***Headquarters***	***Gender Classification Terms***	***Prob. Score***
Amazon	Rekognition	United States	Male/Female	Incl.
Baseapp	DeepSight	Germany	Male/Female	Not Incl.
Betaface	BetaFace API	India	Male/Female	Incl.
Clarifai		United States	Masculine/Feminine	Incl.
Face++		China	Male/Female	Not Incl.
Google	Cloud Vision	United States	N/A	N/A
IBM	Watson Visual Recognition	United States	Male/Female	Incl.
Imagga		Bulgaria	N/A	N/A
Kairos		United States	M/F	Incl.

3Morgan Klaus Scheuerman, Jacob M. Paul & Jed R. Brubaker, 144:8

[75] *See* Morgan Klaus Scheuerman, Jacob M. Paul & Jed R. Brubaker, *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services*, 3 Proc. ACM Hum.-Comput. Interaction 144:1, 144:8 (2019).

[76] *See id.* at 144:7.

[77] *Id.*

This restrictive binary system in FRTs speaks directly to the inherent inaccuracies still interlaced with the technologies. This same study found that there were inconsistencies between technologies in making binary determinations (e.g. one determines male and another female).[78] Google's Cloud Vision, which does not purport to classify by gender, nevertheless assigned labels to an image.[79] The study noted that a single image could be assigned multiple labels, such as "person," "boy," "daughter," and "son."[80] A University of Colorado study of Amazon, Clarifai, IBM, and Microsoft's FRTs took 2,450 face images posts from Instagram.[81] Each post used one of seven hashtag identifiers: "#women," "#man," "#transwoman," "#transman," "#agender," "#agenderqueer," and "#nonbinary."[82] The study found that cisgender men and women were correctly identified more than 97% of the time, while "trans men . . . were incorrectly identified as women in up to 38 percent of instances . . . [and] those who identified as agender, genderqueer or non-binary, were misclassified 100 percent of the time because these gender identities have not been built into the algorithms."[83] The accuracy of the technology requires that the software be of the highest caliber; that the image or probe photo, captured from a photograph or video, must be of a high enough quality for the software to analyze what it should match from an input; and that the software be programmed with the ability to match the image data it is given.[84]

[78] *See id.* at 144:10.
[79] *Id.*
[80] *Id.*
[81] Jesse Damiani, *New Research Reveals Facial Recognition Software Misclassifies Transgender, Non-Binary People*, FORBES (Oct. 29, 2019, 3:21 PM), https://www.forbes.com/sites/jessedamiani/2019/10/29/new-research-reveals-facial-recognition-software-misclassifies-transgender-non-binary-people/#124c73eb606b [perma.cc/NC4H-6W5G].
[82] *Id.*
[83] *Id.*
[84] *See* Clare Garvie, *Garbage in, Garbage out: Face Recognition on Flawed Face Data*, GEO. L. CTR. PRIV. & TECH. (May 16, 2019), https://www.flawedfacedata.com/ [https://perma.cc/97PD-HLXB].

Inaccuracies that are embedded in FRT coding are also exacerbated by the common practice of using and reusing data libraries (old code, and/or data informing code) in the initial software development process.[85] It is common for FRT developers to take data for facial recognition software development from older, biased code libraries; this practice contravenes the idea that technologies become better and less biased over time.[86] Notably, the survey in the table above was of FRT from companies most commonly used by law enforcement agencies (where bias and inaccuracy have even more dire consequences) such as Vigilant Solutions, Cognitec, NEC, Rank One Computing, and Clearview AI.[87]

Facial recognition requires accuracy. FRT systems that do not classify people properly are inaccurate and biased; neither of these issues are likely to be addressed and corrected unless consumers (especially law enforcement agencies) demand that FRT companies make adjustments to their codes.

IV. CURRENT UNVETTED AND UNREGULATED USES BY LAW ENFORCEMENT

In the United States, the use or proposed use of facial recognition software is prevalent in a myriad of places: from schools, to stadiums, to police forces.[88] Regardless of whether FRT is used by law enforcement or private security organizations, when that use is publicly disclosed, it has often been fraught with controversy worldwide. Controversy, which has been almost exclusively public backlash, has led to little, if any, regulation. One of the earliest examples was the Super Bowl in 2001 where FRT was

[85] *The Open Mind: Algorithmic Justice* (PBS television broadcast Jan. 11, 2019), https://www.pbs.org/video/algorithmic-justice-aba1wv/ [https://perma.cc/X2H6-D5X5].

[86] *Id.*

[87] 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 [https://perma.cc/ZRA7-94NF].

[88] *See* Symanovich, *supra* note 8.

used in the security systems at the Tampa Bay stadium, leading to the identification of nineteen subjects thought to have outstanding warrants.[89] This incident did not lead to any arrests because law enforcement was unprepared to handle the sheer volume of identifications or the challenge of finding and arresting the individuals.[90] "We thought we were ready to use it, but getting through the crowd and the architecture of the stadium proved overwhelming," said one law enforcement agent present at the stadium.[91] The public backlash was immediate, particularly from the ACLU.[92] A similar situation occurred a decade ago, when Google released a new face-tracking webcam that was unable to see and track Black people, but could identify white people.[93] "In 2015, Google apologized after its then-new Photos application labeled some Black people as 'gorillas.'"[94] More recently, in late 2018, FRT was reportedly used at a Taylor Swift concert to match concert-goers to a database of potential stalkers of the pop star.[95] More pernicious uses of FRT directly impact vulnerable communities, such as the use of Facebook to track Black Lives Matter participants and license plate readers to track Muslim community members.[96] The Chinese government currently uses facial recognition technology for general

[89] Niraj Chokshi, *Facial Recognition's Many Controversies, from Stadium Surveillance to Racist Software*, N.Y. TIMES (May 15, 2019), https://www.nytimes.com/2019/05/15/business/facial-recognition-software-controversy.html [https://perma.cc/4KCF-HGU6].

[90] *Id.*

[91] Dana Canedy, *Tampa Scans the Faces in its Crowds for Criminals*, N.Y. TIMES (July 4, 2001), https://www.nytimes.com/2001/07/04/us/tampa-scans-the-faces-in-its-crowds-for-criminals.html [https://perma.cc/GA7R-2XHF].

[92] Chokshi, *supra* note 89.

[93] *Id.*

[94] *Id.*

[95] Sopan Deb & Natasha Singer, *Taylor Swift Said to Use Facial Recognition to Identify Stalkers*, N.Y. TIMES (Dec. 13, 2018), https://www.nytimes.com/2018/12/13/arts/music/taylor-swift-facial-recognition.html [https://perma.cc/ULN8-DRHM].

[96] H.B. 1654, 66th Leg., Reg. Sess. (Wash. 2019).

monitoring and possibly social control.[97] A controversial ruling in South Wales allows FRT use by the police despite claims of breach of privacy and data protection.[98] In Washington State, previously undisclosed emails were released through an email listserv called "FITlist, which showed cross-departmental and cross-municipal use of FRT."[99] One particular email reads, "Do not mention FITlist in your reports or search warrant affidavits."[100] Not only does this mean that agencies are using FRT, but it also means that they are actively doing it in a manner not meant to be disclosed to the public. It was announced that facial recognition would be used by security at future planned large events, including the 2020 FIFA World Cup in Japan, the 2020 Olympics also in Japan, and the 2024 Olympics in Paris.[101] Furthermore, many municipalities use ClearviewAI

[97] *'Skynet' System Supported by Facial Recognition Technology Boosts Chinese Public Safety*, PEOPLE'S DAILY ONLINE (Mar. 26, 2019), http://en.people.cn/n3/2018/0326/c90000-9441798.html [https://perma.cc/J5T7-7R8R]; Alfred Ng, *How China Uses Facial Recognition to Control Human Behavior*, CNET (Aug. 11, 2020), https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/ [https://perma.cc/EP3J-A2JJ].

[98] Jenny Rees, *South Wales Police Use of Facial Recognition Ruled Lawful*, BBC NEWS (Sept. 4, 2019), https://www.bbc.com/news/uk-wales-49565287 [https://perma.cc/NV3S-FQRL] (noting High Court was the first court in the world to rule on use of the technology); *see also* Adam Satariano, *Police Use of Facial Recognition Is Accepted by British Court,* N.Y. TIMES (Sept. 4, 2019), https://www.nytimes.com/2019/09/04/business/facial-recognition-uk-court.html [https://perma.cc/T9GL-RJD7].

[99] Michael Hays, *Washington Cops Are Taking a Cue From 'Fight Club' for a Secret Facial Recognition Group*, ONEZERO BY MEDIUM (Nov. 11, 2019), https://onezero.medium.com/secret-emails-reveal-how-washington-state-cops-shared-facial-recognition-tech-db8a799c6de6 [https://perma.cc/6LSG-WDWX].

[100] *Id.*

[101] Chris Burt, *Paris 2024 Olympics to Use id3 Facial Recognition for Biometric Event Security*, BIOMETRIC UPDATE (Nov. 12, 2019), https://www.biometricupdate.com/201911/paris-2024-olympics-to-use-id3-facial-recognition-for-biometric-event-security [https://perma.cc/GES2-6AUL]. Due to the effects of the global COVID-19 pandemic, the 2020 World Cup and 2020 Olympics in Japan did not occur. Plans are still in place to use facial recognition at the 2022 World Cup in Qatar.

without a proper understanding of how the technology works.[102] This technology was built by scrubbing billions of pictures from social media sites, yet its accuracy rates in matching non-white non-men remains untested.[103]

The use of facial recognition software often relies on gathering information from subjects who have not given consent to the parties using the software.[104] Most importantly, the unregulated and unvetted use of facial recognition technology by law enforcement has a detrimental impact on already vulnerable and overpoliced populations. The section below presents legislative action that must be taken by states to address the aforementioned issues inherent in facial recognition technology by regulating the use of FRT technology in law enforcement.

V. MORATORIUM AND STRICT ASSESSMENT OF FRT BY LEGISLATURES

The first step state legislatures must take is to enforce a moratorium on all law enforcement usage of facial recognition software. A moratorium would allow legislatures to first assess the legitimacy of looking into FRT usage; they could then evaluate the appropriate usage of FRTs by law enforcement, the limits on what functions a facial match may serve, and acceptable locations to implement the technology.

After the moratorium, legislatures may decide that they would like to assess re-implementation of FRT. The assessment of FRT should be done through an appointed bipartisan vetting committee. The vetting committee would assess FRTs' baseline capabilities in face matching confidence and would ultimately pick which technology will be used. The vetting

[102] Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/2SRS-55P6].
[103] *See id.*
[104] *See Face Recognition Technology*, *supra* note 7; *see also id.*

committee would also determine what sort of oversight, reporting, and training standards to impose upon municipalities that choose to implement FRTs. Additionally, the vetting committee would be responsible for proposing how data collected through FRT systems would be used and how transparency with the public would be managed. Lastly, if a state legislature decides to overcome an FRT moratorium, rules must be established to restrict any use of FRT in ways known to limit or threaten civil liberties.

A. Moratorium

A moratorium on the use of facial recognition software is the best option to protect against civil rights and liberties abuses until there is more transparency in how the technology is used, who is using the technology, and what the expected outcomes of the use of the technology are. The moratorium is therefore the best first step that both individual states and Washington D.C. can take before identifying facial recognition technologies for future use. An overall moratorium on law enforcement using facial recognition in policing is imperative because without clear policies in place to direct law enforcement in its usage, there is a heightened chance that law enforcement may use the technology in a manner it should not be used, such as to identify individuals in a crowd at a protest.[105]

Proponents of unrestricted FRT use often emphasize threat detection and prevention as benefits that law enforcement will reap from using the technology.[106] However, regulation is necessary to the extent that companies that make FRT are stepping forward and asking for regulation in this area.[107] Concern has spread from the public sphere and into companies

[105] *See* Garvie, *supra* note 84.

[106] *See, e.g.*, *Facial Recognition: Top 7 Trends,* THALES (Sept. 12, 2020), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition [https://perma.cc/34G6-MS53].

[107] Sidney Fussel, *The Strange Politics of Facial Recognition*, ATLANTIC (June 28, 2019), https://www.theatlantic.com/technology/archive/2019/06/democrats-and-republicans-passing-soft-regulations/592558/ [https://perma.cc/5CHD-3GMV] ("Axon, the number-

that sell FRT due to a lack of transparency in how law enforcement uses FRT as well as the general lack of regulation on the technology's use.[108] The CEO of facial recognition technology firm Kairos, Brian Brackeen, has stopped taking government contracts, stating, "In the hands of government surveillance programs and law enforcement agencies, there's simply no way that face recognition software will be not used to harm citizens."[109] Similarly, Microsoft President and Chief Legal Officer Brad Smith has called for FRT regulation while expressing concerns about the potential for discrimination in decision making, invasions on personal privacy, and mass surveillances' encroachment on democratic freedoms.[110] While some in law enforcement see the potential benefits to enforcement,[111] a moratorium allows for assessment before the risk of putting citizens in harm's way arises.

If FRT is used by law enforcement to make a match to a picture of someone who looks like a suspect, then law enforcement must be clear about whether that match alone meets the burden of proof used to make that

one body-camera manufacturer in the United States, agreed with its ethics board's proposal not to outfit Axon cameras with facial recognition." Following suit, "[t]he Microsoft president Brad Smith called for governments 'to start adopting laws to regulate this technology' . . . Amazon Web Services CEO Andy Jassy echoed those comments . . . likening the technology to a knife." While these steps are beneficial in calling for enforcement, these promises are only for the foreseeable future, and these companies are able to change course without regulation.).

[108] Brian Brackeen, *Facial Recognition Software is Not Ready for Use by Law Enforcement,* TECH CRUNCH (June 25, 2018, 4:30 AM), https://techcrunch.com/2018/06/25/facial-recognition-software-is-not-ready-for-use-by-law-enforcement/ [https://perma.cc/VY4P-SRGJ].

[109] *Id.*

[110] Brad Smith, *Facial Recognition: It's Time for Action*, MICROSOFT (Dec. 6, 2018), https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/ [https://perma.cc/JX34-W6HW].

[111] *See* Matthew Feeney, *Should Police Be Able to Use Facial Recognition Technology*, FOUND. FOR ECON. EDUC. (May 18, 2019), https://fee.org/articles/should-police-be-able-to-use-facial-recognition-technology/ [https://perma.cc/6VEQ-88RB] (noting that, according to the Captain of the Las Vegas Police Department, the ability to use real time facial recognition to walk past someone and have an instant report back that the person is wanted for burglary "would be huge.").

person a suspect. Even when a clear picture of a suspect is analyzed by the FRT, the resulting match may have a lower rate of accuracy than one hundred percent if the person in the probe photo is not a white cisgender male.[112] Therefore, before any facial recognition software is implemented, law enforcement should be required to use unbiased FRT software and follow clear regulations outlining how the software may be used. If FRT systems are used by police departments attempting to match probe images from a crime, improvements to the software may not directly address problems with bias: "improvements won't matter much if there are no standards governing what police departments can feed into these systems."[113] If departments are incorporating probe photos that have been enhanced or altered, the corrections in software bias will not matter because the probe photos are based on conjecture ultimately altering the accuracy.[114] A moratorium allows for pause, assessment, and transparency because the use of FRT has the potential to get out of hand.[115]

Once a moratorium is in place, state legislatures can then step in and assess the technology's uses to decide whether there is any actual benefit without causing disparate harm to their communities, especially more vulnerable communities. The legislature can also determine whether implementing the software will allow for discriminatory practices. If FRT is used in the process of law enforcement, how a match can be used in that process must be decided by the state. If a match is used "only for investigative purposes," as has been purported by enforcement agencies in the past, minute decisions must be made about how far a facial recognition match can allow an investigation to go.[116] "Investigative purposes" is an unclear limitation set by the few agencies who have been transparent about

[112] *Results*, *supra* note 63.

[113] Garvie, *supra* note 84.

[114] *See id.*

[115] Garvie & Moy, *supra* note 18.

[116] Garvie, *supra* note 84.

their own use and standards when doing FRT matches.[117] The term does not provide enough detail into the process of investigation to provide a transparent marker for law enforcement to follow.[118] States must set clear standards determining how far a match can carry an investigation. State legislatures can use the moratorium as a time to decide if a match alone is sufficient evidence to bring someone in for a lineup.[119] More aggressively, legislatures might decide a matched photo, which is then confirmed by a witness who looks at that same matched photo, is all that is necessary for an arrest warrant.[120] States must make these determinations prior to implementation, with a sense of the actual statistical capability of the FRT. As a result, legislatures can set clear and ongoing standards for implementation and regulation of FRT.

B. State Driven Assessment of FRT and Policy Making is the Only Path for States to Move Beyond a Moratorium

A moratorium on facial recognition software usage allows for regulation that encompasses increasing public safety while also protecting civil liberties, deterring discrimination, and remaining transparent. Once a moratorium is in place, regulations set by state legislatures can then determine exactly what policies will guide implementation of FRT at the local municipality level. The legislatures can then set minimum standards for FRT implementation and usage. Policies across a state allow for a cohesive, transparent, and enforceable structure. Statewide policies also allow for cost-effective implementation for smaller, less-resourced municipalities. Larger municipalities, which have the resources to cooperate with the defined standards to implement the technology, may provide use of FRT to smaller, less-resourced municipalities, which might not be able to

[117] *See id.*
[118] *See id.*
[119] *See id.*
[120] *See id.*

implement their own FRT while remaining in compliance with state-driven regulations.

C. Implementation of a Vetting Committee

The first step a state must take in re-introducing FRT technology after a moratorium is to decide how FRT technology will be used in the process of law enforcement. Vetting committees would inform this decision. Vetting committees would assess the capabilities of the FRT systems to be implemented, determine a minimum match score or match rate that is appropriate during the process, and suggest what steps law enforcement can take with a match once that match is found. A match made by law enforcement may be different for raw probe photos and enhanced probe photos; in anticipation of that distinction, the vetting committee would be responsible for determining if the FRT can be depended on to present reliable matches based on each.

The limitations of the software must be considered when deliberating how the technology might be used, as it could help in an investigation or it could lead to warrants based on little more than suspicion.[121] Because matches can fail even when using a real and clear photo, state legislatures have to grapple with what could happen if something other than a clear photo is used.[122] Further, most composite sketch searches fail,[123] so states need to clearly define whether the use of composite sketch images with FRT should be allowed to lead to an arrest. If the use is strictly to build a lead, but more evidence is needed to make an arrest, the use of composite sketches might be acceptable. However, legislatures should be wary of adding in any use of composite sketches beyond that which is well tested by third-party organizations. If matches based on composite sketches are no better than an actual lineup of suspects, they only serve to hinder the law

[121] *See id.*
[122] *See* Snow, *supra* note 69.
[123] Garvie, *supra* note 84.

enforcement system by placing added burdens on investigation. Furthermore, composite sketch matches do no more than what we require a human to do in a lineup, but an FRT cannot testify in court, posing yet another threat to due process. Thus, the FRT may raise rather than lower costs.

States must also determine whether manipulated photos (e.g. the addition of a mouth, eyebrows, or ears) can be used to determine a match and, if so, how much manipulation is acceptable. Legislatures must require that original and updated probe images become a part of any investigative record, using audits to ensure that law enforcement follows policies and to provide a record that may be used in court. States should set strict guidelines for the lowest threshold a facial match can have to merit follow-up on an investigative action, and additional guidelines for match thresholds if there is enhancement to a photo or a composite sketch is used.[124] States should bar any further action on a match aside from consideration as a potential suspect to look into, rather than providing probable cause for arrest, or even a lineup.[125] Most technology allows for the thresholds to be heightened or lowered to gather more potential matches; therefore, if a match is truly only going to be used to further looking into a suspect or if there is more cause for someone already considered a suspect, a lower threshold may be allowed because the outcome of the match is only furthering an investigation.[126] For law enforcement to be allowed to follow up a match with confrontation, the minimum threshold should be ninety-five percent or higher, similar to suggested standards set for uses in banking.[127] This standard is used in banking because it is a step in the process to allow users to access the highest levels of security at the financial

[124] *Id.*
[125] *Id.*
[126] *See* Virdee-Chapman, *supra* note 52.
[127] *Id.*

institutions.[128] Similarly, a high threshold should be required prior to confrontation as civil liberties necessitate more certainty than access to financial institutions.

D. Technology Vetting Process

The second step for states is to implement a vetting system for any facial recognition technology that might be used.[129] Because FRT technology continues to be commercially developed for non-law enforcement and law enforcement purposes,[130] state legislatures should appoint an on-going committee of ten to fifteen people to vet FRT technology. The vetting committee must be assembled by a bipartisan group of legislators and composed of experts in technology, law enforcement, and privacy law. This vetting committe would be tasked with assessing technology, making yearly suggestions to the legislative body on advancements in technology, and proposing reconsiderations for FRT usage.[131] The committee must assure that any technology used has gone through rigorous third-party testing to meet accuracy standards that they suggest to the legislature. To meet the standards of rigor required for vetting committees, legislatures may elect to partner with other states' committees. The vetting committee will determine what technologies to assess by identifying the technologies offered by companies with the greatest market share in facial recognition and machine learning; also, the technology must go through third-party testing for matching accuracy, mismatching accuracy, and gender and skin-tone bias.

[128] *Id.*

[129] *See* H.R. 1654, 66th Leg., Reg. Sess. (Wash. 2019).

[130] Symanovich, *supra* note 8; *see also Facial Recognition Market*, MKTS. & MKTS. (2019), https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html [https://perma.cc/UNQ3-2MA8].

[131] *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 [https://perma.cc/XTQ2-DJN] ("Between 2014 and 2018, facial recognition software got 20 times better at searching a database to find a matching photograph.").

Because some municipalities may have used FRTs and acquired information about the technology, a vetting committee could capitalize on that knowledge by asking for proposals from the municipalities. If municipalities suggest FRT, they should explain why they would like to use the technologies to enhance their law enforcement capabilities. Suggestions from municipalities could include how FRT may help in investigations and the specific types of investigations for which they would use FRT. Alternatively, a vetting committee may resolve to procure third-party assessments of technology from companies with the greatest current FRT market share.[132] Although the vetting committee would be tasked with determining which technologies will go through the process of vetting, state legislatures must ultimately agree to the standards for accuracy. The vetting committee's standards should require legislatures to account for the technology's bias in false match rates and the potential for photo enhancements or alterations to be used on probe images.

The standard vetted FRT must demonstrate it overcomes bias between rates of mismatches due to gender or skin tone.[133] If a probe of images has a statistically lower chance of matching based on gender, race, skin tone, and age, then it should not be considered for implementation.[134] A confidence threshold should be established requiring the software to match at a rate of ninety-five percent or greater regardless of any of these defining characteristics.[135] To be approved for use, an FRT must cross the threshold into statistically non-biased mismatching, which means, at the very least, equal match confidence ratings regardless of gender or skin tone.[136] If an FRT system is found to have statistically significant differences in finding matches based on those characteristics, the system should not be used

[132] *See id.*

[133] H.R. 1654, 66th Leg., Reg. Sess. (Wash. 2019).

[134] *Id.*

[135] Feeney, *supra* note 111.

[136] *See* Buolamwini & Gebru, *supra* note 36.

because to do so would perpetuate issues of disparate policing on already vulnerable groups.[137]

FRT mismatches inspire the use of modifications practices such as adding eyes or a mouth to a photo in an attempt to achieve a match.[138] If modification practices are allowed at all, they must be done according to the recommendations of the FRT providers or through agreed upon methods which should be determined *ad hoc* by the vetting committee and ultimately approved by the legislature for use by law enforcement.[139] The pressure to enhance or alter photos increases greatly if the technology adopted is already less likely to find a match because of its gender or skin tone biases, or because it has low thresholds for returning matches.[140] Some practices are unregulated and not suggested by FRT companies, such as pasting lips or noses onto low grade or poorly lit photos or using software to make three-dimensional models of a face from a partial-face photo; these problematic practices bring up questions that should be answered prior to the use of FRT.[141] If law enforcement agencies were to use matches from enhanced photos as sufficient probable cause, significant problems would arise due to the inherent potential for a mismatch in the FRT system combined with the fact the match is based on a computer-generated photo rather than an actual photo. Ultimately, an enhanced photo may be no better, and is more likely worse, than a composite sketch.[142] If methods of enhancement are used, they should not be disproportionately implemented. In order to avoid disproportionate implementation, a vetting committee should rely on reports from government agencies like NIST and those of

[137] Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, *Racial Bias*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/findings/racial-bias [https://perma.cc/43M5-N5YD].

[138] Garvie, *supra* note 84.

[139] *Id.*

[140] *Id.*

[141] *Id.*

[142] *Id.*

independent agencies like Gender Shades. A vetting committee must be certain that any FRT system approved for law enforcement use does not have statistically higher mismatches based on gender, race, skin tone, or age.

E. Training and Auditing

FRT vetting must also include a training and auditing process. The implementation of FRT training should require that those running probe photos know how to work the technology. The training process should be based on the best practices for assuring that training for municipalities is implemented according to the suggestions of the vetting committee and the FRT vendors.[143] Training should include a definite threshold adjustment for likely matches and identify how the threshold can be adjusted when making a match using FRT. Vetting committees must ensure that any FRT system chosen has codified training processes and those processes can be manageably followed. Only users who have been certified through the approved vetting training process should be allowed access to the facial recognition software to attempt matches. Certifying users would reduce the possiblity that they will act upon matches received under lower than legislatively mandated thresholds. Thus, this process would cut down on the potential for acting on matches when received under lower thresholds than mandated by the legislature.

Legislatures considering FRT must also decide if using matches based on enhanced or altered probative images or using police sketches is acceptable, and what happens with any match actually found using these methods.[144] Inappropriate searches could include those with a lower threshold for matching or inappropriate use of enhancing or manipulating photos.[145] If a legislature determines that certain types of image enhancements are

[143] Garvie, *supra* note 84.
[144] *Id.*
[145] *Id.*

acceptable, the processes of enhancement should be uniform across the state's municipalities that implement FRT. Each municipality must keep clear documentation of the processes implemented for each photo enhancement. An auditing process must also be maintained. The auditing process must provide a standardized system to review documentation on how matches are being conducted and to document when facial recognition searches are run inappropriately. The auditing process is also necessary to ensure that FRT systems are updated and systems that support photo enhancement are implemented appropriately.

F. Procedures for Collected Data

Legislatures must also make a decision about where and how FRT face data is to be stored and processed to ensure the data is protected.[146] Biometric data, including facial data, have legal privacy obligations, and this data must be protected from being hacked.[147] Although there is federal protection against the accessing of information on any computer without consent through the Computer Fraud and Abuse Act, laws do not always stop hacking.[148] Furthermore, biometric data is at a great risk of attack because it can be tied to personal use, such as phone password and security.[149]

The importance of biometric data security is made explicit in Illinois' Biometric Information Privacy Act.[150] Unlike social security numbers,

[146] DJ Pangburn, *Due to Weak Oversight, We Don't Really Know How Tech Companies Are Using Facial Recognition Data*, FAST CO. (July 5, 2019), https://www.fastcompany.com/90372734/due-to-weak-oversight-we-dont-really-know-how-tech-companies-are-using-facial-recognition-data [https://perma.cc/5SR8-CJQJ] (U.S. Customs and Border Protection recently hacked).

[147] Daniel Newman, *Facial Recognition Software: Where Are We Now?*, FORBES (Sept. 24, 2019), https://www.forbes.com/sites/danielnewman/2019/09/24/facial-recognition-software-where-are-we-now/#1a1e084b25d9_[https://perma.cc/WJ49-ACQU].

[148] 18 U.S.C. §1030 (2020).

[149] Newman, *supra* note 147.

[150] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/5 (2008).

biometric data is "biologically unique to the individual; therefore, once compromised the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[151] Additionally, the Biometric Information Privacy Act only controls for data losses by commercial, not public, entities.[152] Law enforcement must be aware of the risk associated with collecting this data.[153] The protection of all biometric data should be held to a high standard, from probe images created using security or surveillance cameras (also referred to as closed-circuit television or CCTV) to facial recognition run in real-time from body cameras.[154] Similar to recourse available for data breaches of software companies where there is financial harm, there must be recourse for breaches in biometric data, and those costs must be weighed in a legislature's decision to implement technology that requires protection of so much data.[155]

Any collection of data has the possibility of breach.[156] Currently, there is no overarching federal restriction on the release of personal data.[157] States recognize that their residents' privacy and security is at risk when personal data is collected widely.[158] Although all fifty states and the District of

[151] *Id.*

[152] *Id.*

[153] Pangburn, *supra* note 146.

[154] *Id.*

[155] *See* Stacy Cowley, *Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement*, N.Y. TIMES (July 22, 2019), https://www.nytimes.com/2019/07/22/business/equifax-settlement.html?module=inline [https://perma.cc/HMM5-55WW] (Equifax to pay $650 million in data breach settlement).

[156] Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/LS73-7U3F].

[157] *See Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (updated July 17, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/5KXK-RFWW].

[158] O'Connor, *supra* note 156.

Columbia have some restrictions on the release of personal data, what data falls under privacy requirements and when someone should be notified that their personal data has been breached is far from ubiquitous.[159]

In some states, like North Carolina, biometric data is included in the list of personal information that may not be released.[160] However, the North Carolina statute requires affirmatively objecting to disclosure of personal information; to violate the act a person must "knowingly broadcast or publish . . . with actual knowledge that the person whose personal information is disclosed has previously objected to any such disclosure, which is likely opposite of how many imagine their personal data is protected."[161] A large amount of data can be collected by means of real-time data collection.[162] State legislatures must ensure that the biometric data collected by any FRT must not only remain private but be actionably protected. Currently, civil action may be the only recourse for owners of biometric data who object to their data's disclosure. There is current federal protection for health data, which includes biometric data if collected for health services.[163] However, the privacy of health information only applies to certain entities.[164]

Legislatures and ultimately municipalities must take into account that cybercrime is increasing each year.[165] Cybercrime makes it increasingly

[159] Joseph V. DeMarco & Brian A. Fox, *Data Rights and Data Wrongs: Civil Litigation and the New Privacy Norms*, 128 YALE L.J. 1016 (2019).

[160] N.C. GEN. STAT. § 75-66(c)(10) (2018).

[161] *Id.*

[162] Garvie et al., *supra* note 137; *see also* Jon Schuppe, *Facial Recognition Gives Police a Powerful New Tracking Tool. It's Also Raising Alarms*, NBC NEWS (July 30, 2018), https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936 [https://perma.cc/G568-N2S2].

[163] *Your Rights Under HIPAA*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html [https://perma.cc/L54G-EBGZ].

[164] O'Connor, *supra* note 156.

[165] Kelly Bissel, Ryan M. Lasalle & Paolo Dal Cin, *Ninth Annual Cost of Cybercrime Study*, ACCENTURE (Mar. 6, 2019), https://www.accenture.com/us-

difficult to ascertain overall costs of implementing an FRT that collects data susceptible to cybercrime attacks.[166] When municipalities are assessing whether they want to implement FRT, they must account for the cost of cybersecurity necessary for implementation. Cybercrime analysts expect that regardless of protection, at some point, all databases may be hacked.[167] Actionable protection should include civil action against the disclosure and penalties for enforcement agencies who do not attempt to maintain their cybersecurity and keep this information private.[168]

G. Transparency of Data Collection

Along with assuring the protection of any biometric data gathered by law enforcement, there should be public transparency about what records or systems are being used as databases to match probe photos. Often systems only scan mugshots, but at times, law enforcement will request a probe photo to be run through other jurisdictions' systems.[169] For instance, the FBI is reported to be able to use sixteen different state databases,[170] meaning that data collected by a state municipality may be used in systems outside of that state; if that is the case, transparency is necessary to ensure that, if a breach occurs, action can be taken by those affected to resolve the breach.

As far as it has been reported, law enforcement agencies match probe photos to their own internal booking databases or license photos.[171]

en/insights/security/cost-cybercrime-study [https://perma.cc/3XNA-KAK5] (from 2018 to 2019 cybercrime increased by eleven percent).

[166] *Id.*

[167] O'Connor, *supra* note 156.

[168] *See* DeMarco & Fox, *supra* note 159.

[169] Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America: A Risk Framework for Law Enforcement Face Recognition*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/risk-framework [https://perma.cc/HK2R-FVNY].

[170] *Id.*

[171] *Id.*; Schuppe, *supra* note 162.

However, without legislative action, it is uncertain what happens to the data after it is collected.[172] Legislative action should ensure all collected data is not sold, and the vetting committee should ensure the terms of any FRT technology do not allow the vendors of the technology to take or use any of the collected biometric data.[173] In summary, once the data is collected by the law enforcement agency, it should not be in the control of any other party after collection.

H. Uncompromised Restrictions on FRT Usage During Certain Types of Events

State legislatures should also determine time and place restrictions on how FRT data can be used. Time and place restrictions are especially important if legislatures are going to allow for real-time facial recognition to occur through bodycams, security cameras, or any other form of instantaneous facial capture and match.[174] A high degree of matching accuracy, at least ninety-five percent, must be achieved specifically for any FRT matching in real-time.[175] A mismatch in real-time can lead to "a deadly interaction between law enforcement and that person."[176] The

[172] Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/9M2P-V4HR].

[173] *See* Steven Melendez & Alex Pasternack, *Here Are the Data Brokers Quietly Buying and Selling Your Personal Information*, FAST CO. (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information [https://perma.cc/YQF8-ZASJ] (stating that because of a first-of-its-kind Vermont law implemented in early 2019, 121 data brokers have to register with the Secretary of State, but are not required to disclose who is in their data collections, what they collect, or who they sell the data to).

[174] *Facial Recognition: Top 7 Trends*, GEMALTO (Dec. 7, 2020), https://www.gemalto.com/govt/biometrics/facial-recognition [https://perma.cc/SDP7-C2E7] ("Brussels terror attacks was identified thanks to FBI facial recognition software.").

[175] *See* Virdee-Chapman, *supra* note 52.

[176] Queenie Wong, *Why Facial Recognition's Racial Bias Problem Is So Hard to Crack*, CNET (Mar. 27, 2019), https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack/ [https://perma.cc/8VPW-KQCS].

purported benefit of real-time facial recognition is its use in crowd situations to identify suspected terrorists, which makes accuracy imperative.[177]

To ensure the public's First and Fourth Amendment rights, real-time surveillance should be forbidden during instances of protected speech.[178] Furthermore, FRT use at events like protests can amplify issues that have resulted from over-policing where minorities may be more likely to set off alerts by real-time recognition systems due to prior bookings, regardless of actual convictions.[179] The California legislative assembly spoke directly to this concern in its proposed legislation, stating that the collection of biometric data through facial recognition technology "may chill the exercise of free speech in public places."[180]

The potential for real-time FR-enabled policing to suppress constitutionally protected acts presents legislatures with the need for a heightened level of care and consideration, specifically in the implementation of real-time recognition technologies.[181] Without heavy regulation, the potential for misuse is significant, especially on the collection of real-time data.[182] It is a short move from using the technology to identify missing persons to functioning as a "roving surveillance system."[183] Furthermore, additional implications will arise if real-time

[177] *Facial Recognition: Top 7 Trends*, *supra* note 174.

[178] Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, *Executive Summary*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org [https://perma.cc/MP3D-THHN] ("Of the 52 agencies that we found to use (or have used) face recognition, we found only one, the Ohio Bureau of Criminal Investigation, whose face recognition use policy expressly prohibits its officers from using face recognition to track individuals engaging in political, religious, or other protected free speech.").

[179] *Id.*

[180] Assem. Bill 1215, 2019-2020 Reg. Sess., ch. 579 (Cal. 2019).

[181] Garvie et al., *supra* note 169.

[182] *See* Assem. Bill 1215, 2019-2020 Reg. Sess., ch. 579 (Cal. 2019).

[183] *Id.*

recognition leads to real-time police tracking, which often requires a warrant.[184]

I. Critiques

Where is the money coming from? This is where the voters come in. Not only is legislative action needed, but the voters must be the ones to decide whether FRT is acceptable in our law enforcement system. Funds are already being used to implement unregulated use of FRT in law enfocement, which means citizens, through their taxes, are already funding a system with little to no transparency about how it is being used. If FRT is to be allowed back in use after a moratorium, the money must come from somewhere, and it should be for representatives of the voters to decide whether it is worth the cost to implement a potentially harmful system into law enforcement.

VI. CONCLUSION

A moratorium must be placed on law enforcement's use of FRT. Although FRT capabilities have enhanced greatly in the past decade, the leaps it has made are not enough for it to be implemented in our day-to-day lives. Biases remain in the software itself. The FRT systems are incapable of providing the same level of matches, and mismatches increase when the systems are required to process probe photos of anyone who is not a white cisgender male. These issues must be corrected before FRT can be implemented to enhance public safety. State legislatures must enact the moratoriums on FRT use by law enforcement. If a state determines that the

[184] Garvie et al., *supra* note 137 (citing Tracey v. State, 152 So. 3d 504, 515 (Fla. 2014) ("[T]he federal courts are in some disagreement as to whether probable cause or simply specific and articulable facts are required for authorization to access [historical cell-site location information]."); United States v. Espudo, 954 F. Supp. 2d 1029, 1038–39 (S.D. Cal. 2013) (noting that a significant majority of courts "has found that real-time cell site location data is not obtainable on a showing less than probable cause.").

moratorium is adequate for the FRT, then an assessment must occur through purposeful determinations of how the technology may be implemented in the public safety sphere. Those determinations require the formation and use of a bipartisan vetting committee comprised of experts in multiple fields with the ability to assess the technology’s capabilities and how it should be implemented. These determinations must constantly consider any abuses or infringements upon civil rights and civil liberties and the detrimental impact on communities already subject to overpolicing. Regulation of FRT is the only way this technology should be allowed in the hands of law enforcement.