Texas A&M Law Review

Volume 8 | Issue 1

11-1-2020

Countenancing Employment Discrimination: Facial Recognition in Background Checks

Kerri A. Thompson
thompson.kerri.ann@gmail.com

Follow this and additional works at: https://scholarship.law.tamu.edu/lawreview

Part of the Civil Rights and Discrimination Commons, Labor and Employment Law Commons, and the Science and Technology Studies Commons

Recommended Citation
Kerri A. Thompson, *Countenancing Employment Discrimination: Facial Recognition in Background Checks*, 8 Tex. A&M L. Rev. 63 (2020).
Available at: https://doi.org/10.37419/LR.V8.I1.2

This Article is brought to you for free and open access by Texas A&M Law Scholarship. It has been accepted for inclusion in Texas A&M Law Review by an authorized editor of Texas A&M Law Scholarship. For more information, please contact aretteen@law.tamu.edu.

COUNTENANCING EMPLOYMENT DISCRIMINATION: FACIAL RECOGNITION IN BACKGROUND CHECKS

by: Kerri A. Thompson

Abstract

Employing facial recognition technology implicates anti-discrimination law under Title VII of the Civil Rights Act when used as a factor in employment decisions. The very technological breakthroughs that made facial recognition technology commercially viable—data compression and artificial intelligence—also contribute to making facial recognition technology discriminatory in its effect on members of classes protected by Title VII. This Article first explains how facial recognition technology works and its application in employee background checks. Then, it analyzes whether the use of facial recognition technology in background checks violates Title VII under the disparate impact theory of liability due to the known issue of skewed data sets and disproportionate inaccuracy on some populations. The Article concludes by calling on the Equal Employment Opportunity Commission to issue specific guidance warning employers of impending liability under Title VII, including class action liability, due to the use of facial recognition technology, and to use its enforcement authority to file lawsuits against employers who continue to use the technology.

Table of Contents

DOI: https://doi.org/10.37419/LR.V8.I1.2

I. Facial Recognition and Employer Background Checks

A. *How Employers Use Facial Recognition in Background Checks*

When employers conduct background checks on job candidates, they generally use third-party consumer reporting agencies to search for an applicant's name through databases of public records, including arrest records, felony convictions, and liens, with the goal of verifying an applicant's identity and determining whether an applicant has a criminal record.[1] Some third-party agencies offer facial recognition technology as an additional step in the background check process, claiming that the technology makes the process more accurate. This Article argues that employers should not take advantage of this additional service. Currently, facial recognition technology actually makes background check results less accurate, and using it may expose the employer to liability for employment discrimination.

Under Title VII of the Civil Rights Act of 1964, employers may not make employment decisions, limit employment opportunities, or make decisions that would tend to deprive individuals of employment opportunities, because of sex or race, among other protected classes.[2] Using facial recognition technology in an employment background check is less accurate when used on certain groups, even when it is applied uniformly to everyone who applies for an open position. A recent study by the National Institute of Standards and Technology ("NIST")[3] tested several facial recognition algorithms on different demographics to test whether the algorithm was as accurate when compared across different racial-, ethnic-, and sex-based groups. The report found the algorithms to have, in some cases, wildly different accuracy levels for some groups, with a higher rate of error for Ameri-

[1] *See, e.g.*, Brian T. Horowitz, *Facial Recognition Aids Background Checks*, PCMag (June 21, 2019), https://www.pcmag.com/article/368500/selfie-request-facial-recognition-aids-background-checks [https://perma.cc/3ND2-XVDS]; Laura Denton, *Don't Panic! Background Screening Explained*, Hire Right Blog (Sept. 20, 2018), https://www.hireright.com/blog/background-checks/dont-panic-background-screening-explained [https://perma.cc/J9R2-RKX9]; *Not All Background Checks Are Created Equal*, Evident (Jan. 17, 2019), https://www.evidentid.com/resources/not-all-background-checks-are-created-equal-2/ [https://perma.cc/G977-X6EU].

[2] 42 U.S.C. § 2000e-2(a) (2012).

[3] Patrick Grother, Mei Ngan & Kayee Hanaoka, Nat'l Inst. of Standards & Tech., Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects 1 (Dec. 2019), https://doi.org/10.6028/NIST.IR.8280 [https://perma.cc/9JG7-RDLC].

can Indian women and women of Asian and African descent.[4] For example, because the accuracy level is much lower for African African women, using the technology would tend to deprive these women of employment opportunities: it would have a disparate impact on them, even if the employer was not singling them out for different treatment.

Background check services vary in the databases they search. Because background checks are used to check for a job candidate's criminal background, the employer's background check will search public records of systems used by law enforcement. Some search the *National Criminal Screen* and county data where the candidate lives, or county data where the *National Criminal Screen* has flagged a potential record, while other services search every county in which the individual has resided for the past seven years.[5] The results of the background check sweep are usually a variation on either "pass," with no matches found in these government databases, or "fail," which means that some kind of flag has been detected.[6] Of course, employers who get thousands of job applications likely will not consider someone with a flag, and these candidates will be rejected.[7]

Facial recognition technology, when used as part of a background check, not only searches for the candidate's name in court records and criminal records, but also searches for the candidate's face.[8] In order for a third-party background check service to perform the check and query whether the target photo matches any photos in the database, the photos in the database must have already been analyzed by facial recognition technology, which is commonly done. According to the Georgetown Law Perpetual Lineup report from 2016, one in four of all American state and local law enforcement agencies had the capability to "run face recognition searches of their own databases, run those searches on another agency's face recognition system, or [had] the option to access such a system."[9] Of the twenty-five jurisdictions surveyed by the Perpetual Lineup study, *none* of the surveyed jurisdic-

[4] *Id.* at 47.

[5] *See Not All Background Checks Are Created Equal*, *supra* note 1, at 5.

[6] *See* Horowitz, *supra* note 1, at 2.

[7] While the Federal Credit Reporting Act ("FCRA") provides some protection to employees who are rejected based on a background check, it does not provide a fulsome remedy for those who are passed over at this stage in the hiring process. The FCRA provides that employers who make an adverse employment decision based on information in a background check must notify the candidate with an adverse action notice, but an employer is not required to hold a job open if someone needs to correct incorrect information in his or her background report. *See* Ryan Neumeyer, *5 Steps for Making an Employment Decision Based on a Background Check*, McDonald Hopkins (Nov. 20, 2017), https://mcdonaldhopkins.com/Insights/Blog/Employer-Advocate/2017/11/20/5-steps-for-making-an-employment-decision-based-on-a-background-check [https://perma.cc/54WH-E6CX].

[8] *See* Horowitz, *supra* note 1, at 2–3.

[9] *See* Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Ctr. on Privacy & Tech. at Geo.

tions limited enrollment in the database based on the underlying offense, meaning that a background check facial recognition algorithm trained to recognize matches in such a database will flag people with any kind of arrest record, including those who have been arrested for a misdemeanor, those who have been arrested and then dismissed without charges, and those who have been found not guilty.[10]

B. *Ban the Box Laws Protect the Convicted; Facial Recognition Shuts Out the Innocent*

Lawmakers have already recognized one aspect of the problem that underlies background check screening: employers who rely on criminal background information as a way to screen unsuitable employees may be using criminal background as a proxy for race because of the overrepresentation of African Americans and Latinos in the criminal justice system. Ban the box laws, for example, are targeted toward preventing employers from asking a question about criminal background that disproportionately removes African Americans and Latinos from the applicant pool. These laws prohibit an employer from asking an applicant about his or her criminal record on an initial job application, but do not prohibit running criminal background checks and eventually making employment decisions based on criminal records, as long as those decisions are nuanced to fit the job description.[11]

But laws like ban-the-box, already limited in their scope, do not reach the discriminatory effect of facial recognition. Facial recognition technology is an added layer to the background check that has a redoubling effect on African Americans and Latinos. If an applicant is falsely matched with someone with a criminal record, he or she is barred from consideration, just as the individual who actually has the criminal record would be. Discriminating against potential employees based on a blanket policy of barring anyone who has ever been arrested has already been proscribed by the EEOC.[12] But discriminating against potential employees based on a false match will affect even

L. (Oct. 18, 2016), https://www.perpetuallineup.org/findings/deployment [https://perma.cc/S9TA-83PE].

[10] With regard to the use of such a database, several jurisdictions have no legal standard for how the database may be used, other than it may be used for any law enforcement or criminal justice purpose. Jurisdictions with such unlimited deployment include the FBI, Florida, Iowa, Maryland, Michigan, Nebraska, Ohio, Pennsylvania, Texas, Vermont, Lincoln, Nebraska, Los Angeles, Maricopa County, Northern Virginia Regional Information System, San Diego Association of Governments, San Francisco, Seattle Region and the West Virginia Intelligence Fusion Center. *See id.*

[11] *See* Joseph Fishkin, *The Anti-Bottleneck Principle in Employment Discrimination Law*, 91 WASH. U. L. REV. 1429, 1441–43, 1455–70 (2014).

[12] *See Pre-Employment Inquiries and Arrests & Conviction*, U.S. EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/laws/practices/inquiries_arrest_conviction.cfm [https://perma.cc/5GYU-8EMW]; *EEOC Enforcement Guidance*, U.S. EQUAL

more people: African Americans, Latinos, and others with no criminal records might be falsely matched with an African American, Latino, or anyone else in the databases who does have a criminal record. Ironically, ban the box laws would provide protection to someone who has a criminal record, but would not offer recourse for an applicant whose face was falsely matched to someone with a criminal record.

C. *Biased Outcomes from Objective Algorithms*

The Seattle Police Department claims the facial recognition technology it uses to scan a suspect's photo "does not see race" and therefore cannot exhibit racial bias, meaning that because the technology does not explicitly include race as an attribute in its code, the algorithm cannot produce outcomes that prefer one race over another.[13] This claim of racial blindness is false because facial recognition has been independently assessed and proven to be less accurate on certain populations—even if the algorithm does not explicitly include race as an attribute, the outcomes still favor one race over another.[14]

The problem is compounded when a target photo is searched for in a law enforcement database. Because African Americans are arrested by law enforcement at disproportional rates, they are overrepresented in mug shot databases (especially considering that such databases do not scrub data for no-charges or not-guilty verdicts, and will thus pick up any police encounter that ends in arrest).[15] In addition, facial recognition algorithms disproportionately provide false positives for African Americans.[16] If the algorithm tends to provide false positives, and if there are more photos of African Americans in the databases, the target's likelihood of being falsely matched to someone with a "criminal" background will skyrocket. As the Georgetown Perpetual Lineup study notes, facial recognition "may be overused on the segment of the population on which it underperforms."[17]

Someone applying to jobs online where employers use facial recognition technology in their background checks may thus run into a problem: the algorithm may match a female African American applicant (the population for which facial recognition is the least likely to

EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/laws/guidance/arrest_conviction.cfm [https://perma.cc/TB2A-JGZN].

[13] Garvie et al., *supra* note 9.

[14] *See generally* GROTHER ET AL., *supra* note 3, at 2; *see also* Ignacio N. Confone, *Algorithmic Discrimination Is an Information Problem*, 70 HASTINGS L.J. 1389, 1396 (2019).

[15] Garvie et al., *supra* note 9.

[16] *See* GROTHER ET AL., *supra* note 3, at 2. The NIST report from 2019 analyzed more algorithms and found that African Americans had more false positives than false negatives. *Id.* However, the Perpetual Lineup notes that, based on a 2012 FBI report, African Americans were *less* likely to be identified in facial recognition databases (i.e., they had more false negatives than false positives). *See* Garvie et al., *supra* note 9. The NIST report is more current and analyzed more data.

[17] Garvie et al., *supra* note 9.

be accurate) to the identity of a totally different person, and that person may have a criminal background. The applicant is then shut out from the job solely because an algorithm taught itself to produce outcomes that consistently favor non-African American applicants. The technology intended to be a more objective gateway thus becomes an insurmountable, automated barrier.

II. How Facial Recognition Technology Works

A. *How to Recognize a Face*

The two goals of facial recognition technology—mimicking the activities of the human brain to recognize faces[18] and providing more objective results than humans[19]—are at odds with each other. Visual facial recognition in humans is very highly developed and plays a critical role in social interaction, but it is never "objective."[20] The ways of perceiving a face and the meanings attached to those perceptions are inconsistent and context-dependent; there is no one "objective" way to recognize a face.[21] A system that strives to recognize faces as humans cannot claim to be objective or immune to bias.[22]

Human perception of faces varies within populations and among individuals.[23] Certain individuals can recognize familiar faces well, but not unfamiliar ones, while other individuals demonstrate the opposite strengths.[24] Humans also often exhibit "own-race bias," or being less able to recognize faces from races other than the one they consider their own.[25] The algorithms designed by humans are no different: they can exhibit race bias, gender bias, and a bias toward recognizing the race of the programmers who designed them.[26]

[18] *See* Asit Kumar Datta, Madhura Datta & Pradipta Kumar Banerjee, Face Detection and Recognition: Theory and Practice 4 (2016).

[19] *See* Kelly A. Gates, Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance 10 (2011).

[20] *See, e.g.*, Alexander Todorov, Face Value: The Irresistible Influence of First Impressions 9–48 (2017) (describing how physiognomists interpreted the meaning of various facial features based on national stereotypes).

[21] Gates, *supra* note 19, at 10–11 ("Just as there is no standard or universal way of seeing, there is no universal way of seeing the face.").

[22] Not least because, ultimately, algorithms are programmed to make decisions on behalf of humans. *See, e.g.*, Sarfiya Umoja Noble, Algorithms of Oppression: How Search Engines Reinforce Racism 1, 26 (2018) (stating decisions made by algorithms are ultimately made by human beings).

[23] *See* Gates, *supra* note 19, at 10–11.

[24] *See* Vicki Bruce, Peter J. B. Hancock & A. Mike Burton, *Human Face Perception and Identification*, *in* Face Recognition: From Theory to Applications 51–72 (Harry Wechsler et al. eds., 1998).

[25] Gates, *supra* note 19, at 10–11.

[26] *See, e.g.*, P. Jonathon Phillips et al., *An Other-Race Effect for Face Recognition Algorithms*, 8 ACM Transactions on Applied Perception 10 (2011); Grother et al., *supra* note 3, at 39; *see also* Kathleen L. Hourihan et al., *A Cross-Race Effect in Metamemory: Predictions of Face Recognition Are More Accurate for Members of Our Own Race*, 1 J. Applied Rsch. Memory & Cognnition 158, 164 (2012).

If the algorithms that recognize faces cannot achieve what they advertise, why do employers use them? Other biometric identification methods, such as fingerprints, are more accurate. Fingerprints are more consistent over time: faces age and can be changed with cosmetics and various obstructions whereas fingerprints generally need more radical work to be changed.[27] However, the United States military heavily invested in and developed facial recognition technology in the 1990s, not in widespread fingerprinting. Facial recognition technology was touted as non-invasive, more easily accepted by the public than fingerprints, and as the only biometric that can be captured without a person's consent.[28] Researchers thought that because the technology "simply recognized people the way humans do," it would be more acceptable than fingerprinting, which is associated with criminal identification, and retinal scanning, which involves scanning the blood vessels in one's eyes.[29]

The idea that faces can be read and interpreted for meaning is ancient. Physiognomists claimed to be able to read the forehead for intelligence and the nose for morality, and such facial assessments were even used for employment—servants, for example, would be analyzed before their hiring to assure good moral character and fitness for the position.[30] Such assessments were based on "blatantly racist beliefs" and illustrations of "national types," but were lauded at the time as objective assessments based on common sense.[31]

For a modern example of facial recognition technology presenting biased results, consider that Google, one of the preeminent tech companies and which must, as such, use state-of-the-art engineering in its algorithms, automatically tagged photos of African Americans as "apes" and "animals" in 2015.[32] Google claimed that such a horrifying error was aberrant, but the incident shows that automatically produced results are not synonymous with objective, accurate, or fair results—and may in fact be the opposite in each case. Closer analysis of the technical aspects of facial recognition technology belies an underlying subjectivity that is as susceptible to bias as is the human who designs it.

[27] Garvie et al., *supra* note 9; *see also* PATRICK J. GROTHER, GEORGE W. QUINN & P. JONATHON PHILLIPS, NAT'L INST. OF STANDARDS & TECH., REPORT ON THE EVALUATION OF 2D STILL-IMAGE FACE RECOGNITION ALGORITHM 1, 2 (2011).

[28] GATES, *supra* note 19, at 44–45.

[29] *Id.*

[30] TODOROV, *supra* note 20; *see also* Sahil Chinoy, Opinion, *The Racist History Behind Facial Recognition*, N.Y. TIMES (July 10, 2019) https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html?auth=login-email&login=email [https://perma.cc/A7EC-NNEE].

[31] *See* TODOROV, *supra* note 20, at 17.

[32] *See* NOBLE, *supra* note 22, at 6.

B. *The Development of Facial Recognition Technology: From Likeness to Likely*

At the 1970 World's Fair in Osaka, a scientist took photographs of passers-by for an exhibition entitled "Computer Physiognomy." Based on a computer analysis of the photograph, he told them which of seven celebrities they most resembled.[33] Rudimentary iterations of facial recognition technology have existed since the late 1960s, but the technology was limited by computer processing power much weaker than current capabilities. Facial recognition changed in the 1990s when the U.S. Department of Defense developed the Face Recognition Technology ("FERET") program, allowing researchers to share information about their algorithms and compare different approaches, which advanced the state-of-the-art technologies.[34]

Several different technologies are often collapsed into the label of facial recognition technology, including facial authentication and target facial recognition.[35] Facial authentication matches a new, unknown image to several images of the same individual, verifying whether the unknown individual is the same person or a different one.[36] Facial authentication is what the iPhone uses to recognize a user with Face ID, and it is generally easier to make more accurate as the software only needs to match the unknown face to the images of one individual, not compare it to several different individuals.[37]

[33] GATES, *supra* note 19, at 25.

[34] *See* P. JONATHON PHILLIPS, HYEONJOON MOON, SYED A. RIZVI & PATRICK J. RAUSS, NAT'L INST. OF STANDARDS & TECH., THE FERET EVALUATION METHODOLOGY FOR FACE-RECOGNITION ALGORITHMS 1, 2–4 (1999).

[35] Other applications of facial recognition technology include facial movement analysis, another technology used by companies to assess applicants' body language in job interviews, or emotion detection, which uses face scanning to detect certain emotions. *See, e.g.*, Ivan Manokha, *How Using Facial Analysis in Job Interviews Could Reinforce Inequality*, PBS NEWS HOUR (Oct. 7, 2019, 3:26 PM), https://www.pbs.org/newshour/economy/making-sense/how-using-facial-recognition-in-job-interviews-could-reinforce-inequality [https://perma.cc/BUB8-YQC2] (stating face scanning company HireVue analyzes language and body language to predict how well the candidate will perform on the job); Oscar Schwartz, *Don't Look Now: Why You Should Be Worried About Machines Reading Your Emotions*, THE GUARDIAN (Mar. 6, 2019), https://www.theguardian.com/technology/2019/mar/06/facial-recognition-software-emotional-science [https://perma.cc/6BB6-CTYT] (describing the "objective" analysis of faces to deduce emotions).

[36] *See, e.g.*, Andrew Gebhart, *Facial Recognition: Apple, Amazon, Google and the Race For Your Face*, CNET (Mar. 18, 2019, 3:00 PM), https://www.cnet.com/how-to/facial-recognition-apple-amazon-google-and-the-race-for-your-face-facebook/ [https://perma.cc/2UUT-78QM].

[37] Apple's facial authentication system, Face ID, is generally considered to be more accurate than target facial recognition, partially because the software is using images from an infrared camera that can measure depth, and each time the camera is used on a face, the software has a deeper database from which to authenticate an image. *See, e.g.*, *id.*

Target facial recognition involves more complex programming.[38] The software first must have a database of known faces from which to match.[39] Then, the software must be able to analyze an image to see if there is a face in it, picking a face out of a background of image "noise" (facial detection).[40] Then, it must measure the target face using the same measurements it used to measure the database of known faces.[41] This last crucial step—how the face is measured to compare it to others—slowed down the development of target facial recognition from its initial development in the 1960s because, to analyze a face most accurately, one would have to take into account thousands of variables.[42] Early facial recognition algorithms were not automated and required manual input.[43] Local feature analysis was one such method, which represented the face as a graph of data points but required manual input for grid structures and was not automated.[44] This Article will focus on target facial recognition applications of facial recognition technology—using a target face and looking for the same face in a database of previously identified faces (such as running a photo of a suspect through a database of mug shots).

The first breakthrough in target facial recognition came in the late 1980s through data compression.[45] Developers were able to narrow down how much data was needed to successfully match a target face to faces in a database using principal component analysis.[46] Essentially, the images are reduced in dimensions to their "principal components."[47] For example, if a face has one thousand different characteristics that vary when compared to another face, not all of the thousand different characteristics are necessary to distinguish one face from the other.[48] The programmer instead chooses principal components to compare. Instead of comparing all data, the software "flat-

[38] *See* Datta et al., *supra* note 18, at 5.

[39] *Id.*

[40] *Id.*

[41] *See id.*

[42] *See id.* at 5–7.

[43] Nat'l Sci. & Tech. Council, Comm. on Tech., Comm. on Homeland & Nat'l Sec., Subcomm. on Biometrics, *Face Recognition*, FBI, https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-face-recognition.pdf [https://perma.cc/3XJB-G7Y7].

[44] Stefano Arca, Paola Campadelli & Raffaella Lanzarotti, *A Face Recognition System Based on Local Feature Analysis*, 2003 Audio & Video-Based Person Authentication Proc. 1, 1 (2003) https://doi.org/10.1007/3-540-44887-x_22 [https://perma.cc/NN4B-Y6Q5].

[45] Nat'l Sci. & Tech. Council et al., *supra* note 43 (describing Kirby and Sirovitch's application of principal component analysis to face recognition); *see generally* L. Sirovich & M. Kirby, *A Low-Dimensional Procedure for the Characterization of Human Faces*, 4 J. Optical Soc. Am. A. 519, 519–24 (1987).

[46] Nat'l Sci. & Tech. Council et al., *supra* note 43.

[47] *Id.*

[48] *See id.*

tens" the data so it can be more easily manipulated and compared with less computer processing power.[49]

Researchers in facial recognition technology applied principal component analysis to facial recognition by compressing the data stored in a face—compressing perhaps one thousand attributes to just one hundred—and by using statistical variance methods to weigh which faces looked least like each other.[50] By process of elimination, the code eventually finds the faces that most resemble each other based on the compressed attributes.[51] The facial recognition application of principal component analysis is termed Eigenfaces.[52]

Eigenfaces algorithms find the "mean image" in a dataset by first comparing the two most dissimilar faces in a dataset, then the next two, and so on.[53] After ordering the faces according to their similarity, the algorithm computes the mean image, or a "ghost image," so-called because it is an average of all of the faces in the databases and is not itself one of the database's "real" faces.[54] When the algorithm sees a new face, the target face, it measures how closely the target face resembles the faces in the dataset.[55] The programmer sets a minimum threshold for how closely the faces need to be in order to "match."[56] If the face meets the threshold, it is "recognized," and if not, the image is not found among the dataset and no match is produced.[57]

By compressing the data in a face in order to measure the face, Eigenfaces essentially changes the inquiry from which faceprint matches this faceprint to which face in the database meets a minimum threshold of similarity to this face. In other words, which known face is most likely to match this unknown face? Depending on what the risks are in creating false positives (for example, higher risk in a criminal database or lower risk in a Facebook photo image recognizing system), the threshold for how similar the photos need to be to produce a

[49] *See* StatQuest with Josh Starmer, *Principal Component Analysis Clearly Explained*, YouTube (Aug. 13, 2015), https://www.youtube.com/watch?v=_UVHneBUBW0 [https://perma.cc/R2JD-7XV4].

[50] Matthew A. Turk & Alex P. Pentland, *Face Recognition Using Eigenfaces*, 1991 Inst. Elec. & Elecs. Eng'rs Proc. 586, 587 (1981), https://sites.cs.ucsb.edu/~mturk/Papers/mturk-CVPR91.pdf [https://perma.cc/LSG4-YU69].

[51] *Id.*

[52] *Id.* (explaining "Eigenfaces" took its name from "Eigenvectors"). The prefix "eigen-" in German denotes ownership or property and is occasionally translated as "proper vector." Elizabeth S. Meckes & Mark W. Meckes, Linear Algebra 1, 69 (2018).

[53] Nev Acar, *Eigenfaces: Recovering Humans from Ghosts*, Towards Data Sci. (Aug. 21, 2019), https://towardsdatascience.com/eigenfaces-recovering-humans-from-ghosts-17606c328184 [https://perma.cc/X8JR-6NCX] (describing how facial recognition algorithms work).

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *See, e.g.*, Shang-Hung Lin, *An Introduction to Face Recognition Technology*, 3 Informing Sci. 1, 5 (2000).

match can be raised or lowered.[58] Because software code is protected under trade secrets law,[59] software code is generally unavailable to the public, and it is therefore impossible to divine exactly how similar the target face has to be to the faces in the database: the programmer decides based on a balance struck between accuracy and expediency, making a subjective choice as to how likely is like enough.

Despite such advances within the last five years[60] and the sudden omnipresent presence of facial recognition technology,[61] these technologies that are already in use do not perform equally well on different populations. Indeed, the error rate varies so wildly across different demographics that the one government agency (NIST) that performs audits on facial recognition algorithms for volunteer vendors issued an entire report detailing so-called "demographic differentials," or higher inaccuracy for certain demographics.[62] Such disparate effects have been known since at least 2003, as reported by NIST in the 2002 Face Recognition Vendor Test.[63] Most of the 126 algorithms studied by NIST in 2019 were found to have higher false positive results for women than men. The highest error rate occurs with images of American Indians: one algorithm tested had an error rate for American Indian women that was sixty-eight times higher than the rate of error for

[58] *Id.*

[59] *See* Taylor R. Moore, *Trade Secrets and Algorithms as Barriers to Social Justice*, CTR. FOR DEMOCRACY & TECH. (Aug. 2017), https://cdt.org/files/2017/08/2017-07-31-Trade-Secret-Algorithms-as-Barriers-to-Social-Justice.pdf [https://perma.cc/D5AM-3KU5]. Developers rely on trade secret common law to protect algorithms from public disclosure because, as an abstract mathematical formula, the Supreme Court held that they are ineligible for patent protection. *See* Diamond v. Diehr, 450 U.S. 175, 188 (1981). FRANK PASQUALE, THE BLACK BOX SOCIETY 83 (Harvard Univ. Press 2015) (explaining trade secret protection never expires and never needs to be publicly disclosed); *see generally* CATHERINE L. FISK, WORKING KNOWLEDGE: EMPLOYEE INNOVATION AND THE RISE OF CORPORATE INTELLECTUAL PROPERTY, 1800-1930 37 (Univ. of North Carolina Press 2009).

[60] *NIST Evaluation Shows Advance in Face Recognition Software's Capabilities*, NAT'L INST. STANDARDS & TECH. (Dec. 6, 2018), https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities [https://perma.cc/2RJY-KV6X] (finding facial recognition became twenty times better between 2014 and 2018); *see also* GROTHER ET AL., *supra* note 3, at 14 n.1, 16.

[61] *See, e.g.*, Lily Hay Newman, *Facial Recognition Has Already Reached Its Breaking Point*, WIRED (May 22, 2019, 4:48 PM), https://www.wired.com/story/facial-recognition-regulation/ [https://perma.cc/3EJG-MCA].

[62] *See* GROTHER ET AL., *supra* note 3, at 6; Joss Fong, *What Facial Recognition Steals From Us*, VOX (Dec. 10, 2019, 8:00 AM), https://www.vox.com/recode/2019/12/10/21003466/facial-recognition-anonymity-explained-video [https://perma.cc/RA4K-4S47] (describing how facial recognition algorithms work); James Vincent, *Gender and Racial Bias Found in Amazon's Facial Recognition Technology (Again)*, THE VERGE (Jan. 25, 2019, 9:45 AM), https://www.theverge.com/2019/1/25/18197137/amazon-rekognition-facial-recognition-bias-race-gender [https://perma.cc/F4CF-9GU3].

[63] *See* GROTHER ET AL., *supra* note 3, at 18; PATRICK GROTHER, ROSS MICHEALS & P. JONATHON PHILLIPS, NAT'L INST. STANDARDS & TECH, FACE RECOGNITION VENDOR TEST 2002 PERFORMANCE METRICS 7 (2003).

white men. There is also a higher error rate for women of Asian and African descent.[64]

The reasons why facial recognition technology generally performs better on white populations and performs worse on minority populations are not definitively known, but two reasons are often proposed: skewed data and programmer bias (implicit or actual).[65] First, the dataset that an algorithm uses to train itself is skewed, as it contains more white images than non-white images. Thus, the algorithm more accurately recognizes white images simply because it has more practice recognizing white images. Some companies have blamed the datasets on which algorithms are initially trained and have taken steps to create more "balanced" datasets[66]—some via unscrupulous means. For example, in order to rectify the paucity of face images of people of African descent in its training dataset for the Pixel 4 smartphone, a Google contractor claimed that Google had instructed its contractors to target black homeless people and students, take their pictures, and then give them a $5 gift card in exchange for adding their picture to Google's facial recognition training database.[67] Other companies claim to have improved the accuracy of their facial recognition technology by creating balanced and diverse datasets.[68] Second, some researchers claim that programmers' own biases affect their coding, saying that because the majority of programmers are white men, their bias and weaker ability to identify non-white faces compared to white ones may permeate the actual coding.[69]

[64] *See* GROTHER ET AL., *supra* note 3, at 47.

[65] *See, e.g.*, Joy Buolamwin & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PROC. MACHINE LEARNING RSCH. 3 (2018) (showing that an MIT study of datasets used to train facial recognition algorithms overrepresented lighter males and underrepresented both darker females and darker individuals in general); Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, THE ATLANTIC (Apr. 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/ [https://perma.cc/7X88-7EQS].

[66] *See* Larry Hardesty, *Study Finds Gender and Skin Type Bias in Commercial Artificial Intelligence Systems*, MIT NEWS (Feb. 11, 2018), http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212 [https://perma.cc/8F8A-83AC] (quoting IBM engineer who claims to have improved accuracy through use of "balanced types").

[67] Isobel Agher Hamilton, *Google Suspended Research for the Pixel 4 Smartphone After Reportedly Targeting Homeless Black People*, BUS. INSIDER (Oct. 7, 2019, 8:05 AM), https://www.businessinsider.com/google-suspends-facial-recognition-research-after-daily-news-report-2019-10 [https://perma.cc/8TWU-UZH8].

[68] *See* Queenie Wong, *Why Facial Recognition's Racial Bias Problem Is So Hard to Crack*, CNET (Mar. 27, 2019, 7:00 AM), https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack/ [https://perma.cc/LGA3-7PSX] (highlighting Microsoft's claims that it "reduced error rates for women and darker-skinned men by up to [twenty] times").

[69] *See id.* A third reason that may explain the "demographic differential" in facial recognition technology is that the algorithm itself is not race blind: it takes race into account. Then, due to either skewed data or programming bias, the algorithm produces less accurate results for certain demographics. Some types of facial recognition

Despite attempts to identify reasons why algorithms may give biased results and the subsequent attempts to correct algorithms through better data or better programming, the problem of "demographic differentials" has proven intractable.[70] In a 2019 congressional hearing on facial recognition, the director of the Information Technology Lab at NIST said that it is unlikely that facial recognition technology will *ever* perform equally well across groups of people.[71] Even Idemia, a company whose algorithm was tested by NIST in its 2019 audit and was found to have a lower inaccuracy rate across demographics than the other algorithms tested,[72] still tested with an error rate that was ten times worse for black women than the error rate for white women.[73]

The unknown factor that has proven so difficult to correct is the same factor that made facial recognition technology so much better (for white males) over the past five years: artificial intelligence.[74] Now, instead of using the algorithm as it was designed by the programmer, the algorithm "learns" from new images and corrects it-

technology do code for race, labeling faces as "white" or "black" in their processes for matching, but whether race is actually used as a factor in the code was not tested in NIST's report. *See* Patrick J. Grother, Mei L. Ngan, Kayee K. Hanaoka, Nat'l Inst. of Standards & Tech., Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification 3, 20 (Nov. 2018), https://doi.org/10.6028/NIST.IR.8238 [https://perma.cc/FNH8-WHQY].

[70] *See* Wong, *supra* note 68.

[71] Jack Corrigan, *Experts Tell Congress Bias Problem May Be Here to Stay*, Nextgov (July 10, 2019), https://www.nextgov.com/cio-briefing/2019/07/experts-tell-congress-facial-recognitions-bias-problem-may-be-here-stay/158320/ [https://perma.cc/S4BG-K8NC].

[72] *See* Grother et al., *supra* note 3, at 8.

[73] Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, Wired (July 22, 2019, 7:00 AM), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/ [https://perma.cc/3PY7-VCLZ] (noting also that Idemia software is used by the FBI). *But see* Stephane Gentric, Research Unit Manager, Senior Expert, Idemia, *Face Recognition Evaluation @ Idemia* (April 4, 2018), https://nigos.nist.gov/ifpc2018/presentations/44_gentric_Idemia_IFPC.pdf [https://perma.cc/6JLW-RYVS] (claiming that Idemia has the same error rate for black and white people as well as males and females); Liz Do, *Study Takes AIM at Biased AI Facial-Recognition Technology*, phys.org (Feb. 12, 2019), https://phys.org/news/2019-02-aim-biased-ai-facial-recognition-technology.html [https://perma.cc/ES5X-RJ28] (discussing how Amazon's Recognition software, formerly used by police in Orlando, Florida, had nearly 100% accuracy with light-skinned men, but misclassified darker-skinned women as men 31% of the time); Anita Chabria, *Facial Recognition Software Mistook 1 in 5 California Lawmakers for Criminals, Says ACLU*, L.A. Times (Aug. 13, 2019, 5:00 AM), https://www.latimes.com/california/story/2019-08-12/facial-recognition-software-mistook-1-in-5-california-lawmakers-for-criminals-says-aclu [https://perma.cc/A46C-4CVZ].

[74] *See* Grother et al., *supra* note 69, at 2; *see also Information Access Division*, Nat'l Inst. of Standards & Tech., https://www.nist.gov/itl/iad [https://perma.cc/FH57-N3XQ] (describing how NIST is helping facial-recognition technology make strides via machine learning and deep neural networks); Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, N.Y. Times (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/B2U6-GQ25].

self to produce more accurate results.[75] But facial recognition technology that uses deep neural networks ("DNN") to identify faces will ultimately have unpredictable flaws because the original programmers do not know exactly which attributes the network has learned to produce the correct result.[76] A DNN might use background, color, or texture in the photograph instead of facial features: characteristics that may come up with the right result sometimes but can easily lead to inaccurate and unpredictable results.[77] For example, a DNN trained to recognize animals might correctly label a panda, but then if it is shown an image of random pixels, the next time it "sees" the image of a panda, it might mislabel it as a gibbon.[78] It is unclear why the image of random pixels will change the algorithm's output.[79]

Such unknown variables and consequent mistakes make it very difficult to correct the algorithm for demographic differentials. As long as the algorithm correctly identifies some percentage of images in a dataset (despite how homogenous the dataset, and despite how egregious the wrong answers are (e.g., Google's mistake)), companies selling their facial recognition technology can tout the positives and bury the negatives due to a lack of regulation governing standards it must meet in order to be sold.[80] The market does not self-correct in this case because there is little incentive for the employer to gauge how accurate the technology is. For most jobs, there will be more qualified applicants than vacancies. Even if the technology produces outcomes favoring one group over another, the employer will still accomplish the goal of filling the position with an applicant with no criminal background, and one person will get the job.

In Cathy O'Neill's pioneering book, *Weapons of Math Destruction*, she posits that algorithms should be judged by weighing the relative harms of false positives and false negatives.[81] A false positive for the applicant means that the applicant does not get the job and is shut out from consideration from ever getting the job. A false negative for the applicant means someone whose picture should have matched some-

[75] *See* Sean Gerrish, How Smart Machines Think loc. 426 (2018) (ebook); *see also* Douglas Heaven, *Why Deep-Learning AIs are So Easy to Fool*, Nature (Oct. 9, 2019), https://www.nature.com/articles/d41586-019-03013-5 [https://perma.cc/JYP3-Q9B4] (explaining how deep neural networks use large data sets to make new connections in an electronic neural network to achieve a desired result).

[76] *See* Heaven, *supra* note 75.

[77] *See id.* at 3.

[78] Ian J. Goodfellow, Jonathon Shlens & Christian Szegedy, *Explaining and Harnessing Adversarial Examples*, ICLR 2015, 3 (Mar. 20, 2015), https://arxiv.org/pdf/1412.6572.pdf [https://perma.cc/KC5T-GK2W].

[79] *See* Heaven, *supra* note 75, at 3 (noting also a DNN that labeled a dragonfly as a manhole and a mushroom as a pretzel).

[80] Other than, generally, the FTC's general jurisdiction over false advertising claims. *See generally* Chris Jay Hoofnagle, Federal Trade Commission: Privacy Law and Policy 119 (2016).

[81] Cathy O'Neill, Weapons of Math Destruction 199 (2016).

one with a criminal background gets the job. From the employer's perspective, the relative harm of a false negative is much greater than that of a false positive. But for the applicant with a clean record, the relative harm of being unfairly shut out by a false positive is much greater.

The purpose of anti-discrimination law is to ensure that employers do not use unjustified means when reaching those outcomes and to balance the relative harms that come from any employment practice. Currently, African Americans, women, and people with darker skin have a much higher risk of a false positive and of being shut out from job consideration with a false positive. Employers actually have a higher risk of a false negative if they use facial recognition technology than if they do not; the inaccuracy of some matches (both false negatives and false positives) will skew the data. The relative harm of the false positive is something that the EEOC should focus its enforcement on to keep from entrenching automated discrimination in the job market.

III. Use of Facial Recognition Technology in Background Checks Violates Anti-Discrimination Law

Title VII of the Civil Rights Act of 1964 prohibits employers from making employment decisions because of an individual's sex or race, or to limit, segregate, or classify employees because of race or sex in any way which would deprive or tend to deprive any individual of employment opportunities.[82]

Generally, courts test for the presence of employment discrimination with one of two separate inquiries: Whether the employer was intentionally motivated by race or sex in making an adverse employment determination, or whether a facially neutral practice had a discriminatory effect—or a disparate impact—on a plaintiff member of a protected class.[83] The use of facial recognition technology in background checks certainly implicates disparate impact discrimination.

[82] 42 U.S.C. § 2000e-2(a) (2012) (stating protected classes also include color, religion, and national origin). Under Title VII of the Civil Rights Act of 1964, it is illegal for an employer to discriminate against any individual with respect to compensation, terms, conditions or privileges of employment because of the individual's race, color, religion, sex or national origin, or to limit, segregate or classify his employees or applicants for employment in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of the individual's race, color, religion, sex or national origin. *Id.*

[83] *See generally* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Cal. L. Rev. 671, 694 (2016).

A. *Disparate Impact Discrimination: The Effects of Using Facial Recognition Technology*

When employers use facial recognition as part of the background check to screen employees in the onboarding process, they will inevitably violate Title VII due to the inaccuracies of the algorithms' performance and the disparate impact the technology has on members of protected classes.

The standard for disparate impact discrimination is a burden-shifting standard: (1) The plaintiff files suit and bears the burden of production and persuasion to establish that an employment practice has a discriminatory effect on a protected class.[84] If the plaintiff fails at this stage, the employer prevails. (2) If the plaintiff fulfills her burden, the employer then must demonstrate that the practice is "job-related and consistent with business necessity" (per statute in 1991).[85] If the employer fails at this stage, the plaintiff prevails. (3) The plaintiff must then prove that the employer's interest could be served equally effectively by an alternative employment practice with less of a discriminatory impact.[86]

1. Discriminatory Effect

Companies such as Wag! openly tell a job candidate that they will be submitting a photograph that will be run through facial recognition technology in the candidate's background check, and obtain the candidate's consent to do so, so the process is known to the candidate.[87] A candidate facing adverse action from a potential employer may not know the specific algorithm that the company is using for its facial recognition component of the background check, but the 2019 NIST report has shown that when matching a known face to a group of other known faces in a large database, such as a mug shot database, the algorithms that were tested generally provide more false positive matches (and thus more flags when compared with a criminal database) for women, American Indians, people of African descent, and people of Asian descent, and no vendor nor algorithm has come up with a solution to the problem of demographic inaccuracy.[88]

The employer may claim that the individual algorithm used by the background check vendor was not a part of the NIST study, and therefore cannot be assumed to have a discriminatory effect, but due to the

[84] *See* Griggs v. Duke Power Co., 401 U.S. 424, 430–31 (1971).

[85] *See id.* at 431–32; 42 U.S.C. § 12112(4)(A) (1988).

[86] *See Griggs*, 401 U.S. at 433.

[87] *Wag + Vetty – Background Screening*, WAG!, https://vetty.co/wagvetty-background-screening/ [https://perma.cc/8N5Z-U34P].

[88] *See* GROTHER ET AL., *supra* note 3, at 2; *see also Facial Recognition Technology Falsely Identifies Famous Athletes*, ACLU MASS. (Oct. 21, 2019), https://www.aclum.org/en/news/facial-recognition-technology-falsely-identifies-famous-athletes [https://perma.cc/P7PN-FDUD].

intractability of the inaccuracy issue and the fact that no company has volunteered an algorithm to NIST without demographic inaccuracy, it is unlikely that any facial recognition software would not have a discriminatory effect, especially considering the director of NIST admitted in a congressional hearing that it is unlikely that facial recognition technology would *ever* perform equally well across groups of people.[89]

The discriminatory effect on women, people of African and Asian descent, and American Indians also may be stronger than an analysis that just focuses on the facial recognition algorithm of the background check will reveal. In the Georgetown Perpetual Lineup study, researchers found that facial recognition databases used by law enforcement often do not limit enrollment based on arrests without charges or not-guilty verdicts,[90] meaning that a false match to someone in the database may not even be flagging someone with a criminal record, but rather someone who was arrested for any reason (be it a political protest or a false accusation). This kind of match may be accurate, i.e., matching an image to a person of the correct identity in the database. But the flag itself will be inaccurate, reporting a criminal background for someone without one. Because African Americans are overrepresented in the criminal justice system, they will be affected not only by algorithmic inaccuracy but by accurate matches to background falsely flagged as criminal.[91] When the database is stacked with photos of African Americans, and the algorithm has trained itself to provide false positive matches for photos of African Americans, the impact the use of such software has on African Americans is exponentially greater than a white male would face.

Additionally, the facial recognition algorithms that law enforcement agencies use to initially identify their dataset are also subject to inaccuracies, and indeed, make no guarantee of the accuracy of their products.[92] If the inaccuracy of such algorithms leads to false positives in the database, the database itself may be corrupted by containing multiple people labeled with one identity. When the background check facial recognition algorithm with a propensity for false positive matches for African American women, for example, then runs a check on this data, there will be an exponential chance that an African American woman will be matched to at least one face that is labeled with a criminal identity. Inaccuracies thus have a multiplying effect, and inaccuracies correlated to demographics have an unfair effect on protected class members.

The use of facial recognition software in background checks can be compared to how courts have treated employers' advertising and

[89] *See* Corrigan, *supra* note 71.

[90] *See* Garvie et al., *supra* note 9, at 24, 30.

[91] *See id.* at 53.

[92] *See id.* at 46 (discussing Face First contract with San Diego Association of Governments).

recruiting practices as evidence of discriminatory effect. The statutory text of Title VII allows courts to consider an employer's advertising and recruiting practices as evidence of employment discrimination.[93] Courts have held employers liable for both advertisement placement (e.g., an advertisement for non-management roles is placed in a female-only help wanted column)[94] as well as word of mouth hiring practices (e.g., not informing a black teacher of job opportunities and vacancies after she requested them, when word of mouth was the only way to know of openings).[95]

Compared to these cases that analyze advertising placement or word of mouth, the use of facial recognition technology as a screening tool in background checks before a candidate begins employment is a more direct barrier to employment and a clearer adverse action. With advertising placements, the employers argued that the EEOC failed to consider that women might not want the job and would not apply, weeding themselves out through "self-selection," but the court did not find that argument persuasive when the company advertised sex-specific roles to women in "female-only" help wanted columns in newspapers.[96] In the facial recognition context, self-selection is not a factor: Those who apply for the job have already self-selected for the job, not against it. Weeding people out by using facial recognition technology in the background check process similarly guarantees an uneven playing ground. Instead of advertising non-management roles exclusively to women, the company now allows everyone to apply, but weeds out women (or American Indians or people of African descent) at the background check stage.

2. Job-Related

If the court finds that the plaintiff has met his or her burden in proving a discriminatory effect, the employer may argue that the practice of using facial recognition in background checks is job-related and consistent with business necessity because the usual background checks are not as accurate and it is necessary to hire the best employees without problematic backgrounds. For example, using facial recognition would be consistent with business necessity when hiring for jobs such as dog walker, which is a position of trust and care that someone hires someone for, and which includes duties such as potentially enter-

[93] *See* Pauline T. Kim & Sharion Scott, *Discrimination in Online Employment Recruiting*, 63 St. Louis U. L.J. 93, 107 (2018).

[94] In *Capaci v. Katz & Besthoff, Inc.*, the EEOC supported a claim that the employer did not promote females at the same rate as males by citing to its advertising practices. 711 F.2d 647, 658–59. (5th Cir. 1983). The company advertised non-management jobs in "female" newspaper help wanted columns and placed management advertisements in male help wanted columns. *Id.*; *see also* Kim & Scott, *supra* note 93, at 110.

[95] *See* United States v. City of Warren, 138 F.3d 1083, 1088–90 (6th Cir. 1998).

[96] *Capaci*, 711 F.2d at 653, 658–59.

ing the employer's home when no one else is home. Employers may also argue that using algorithmic decision-making is more objective than using a human to review background checks.

The standard that courts use to evaluate an employer's profferred business necessity reason is a loose standard, which asks whether the practice is sufficiently "job-related."[97] For example, the Eighth Circuit requires that hiring criteria bear a "manifest relationship" to employment, and the Third Circuit requires "employers show that a discriminatory hiring policy accurately—but not perfectly—ascertains an applicant's ability to perform successfully the job in question."[98] Under these loose standards, algorithmic decision making, if based on seeking traits that are "job-related," will probably be accepted as "business necessity."[99]

However, facial recognition technology is different in that its use actually undermines the business necessity of verifying identity and matching a person with a criminal background. The plaintiff may argue that this use of facial recognition technology does not achieve the job-related business necessity claimed by the employer because the technology performs less accurately on members of protected classes and therefore actually undermines the task of hiring the right employee for the job.

3. Alternative Non-Discriminatory Means

In order to prove that the employer's interest could be served equally effectively by an alternative employment practice, the plaintiff may then argue that the same purpose is effected by a traditional background check that screens names and social security numbers, without the added component of adding someone's physical appearance and potential matches with mug shots into the mix. The practice is not only inconsistent with the business necessity of accurate background checks; the practice actually makes those background checks more inaccurate, particularly for American Indians, Asian women, and black women.[100] Using facial recognition technology that produces a likely match is less likely to catch true matches that would not be otherwise caught by a search of name, birthday, and social security number, and in fact has been shown to catch more false positives.[101] Additionally, there is nothing that guarantees that algorithmic decision-making is less biased or more objective than human review.[102]

[97] *See, e.g.*, Barocas & Selbst, *supra* note 83, at 705.

[98] *Id.* at 705, n.171; Gallagher v. Magner, 619 F.3d 823, 834 (8th Cir. 2010); El v. Se. Pa. Transport. Auth., 479 F.3d 232, 242 (3d Cir. 2007).

[99] Barocas & Selbst, *supra* note 83, at 706 ("The threshold issue is clearly whether the sought-after trait—the target variable—is job related, regardless of the machinery used to predict it.").

[100] *See* Gebhart, *supra* note 36.

[101] *See* GROTHER ET AL., *supra* note 3.

[102] *See* Confone, *supra* note 14, at 1394–406.

B. *EEOC Guidance on Background Checks and Pre-Employment Inquiries*

The EEOC should issue guidance cautioning employers that use of facial recognition technology in making employment decisions (including its use in background checks) may subject employers to lawsuits under Title VII.[103] EEOC rules, like rules issued from other federal agencies, fill the gaps between orders given in a statutory scheme by telling private entities how they can comply. Guidance then fills the gaps between administrative rules.[104] Such guidance would likely have the effect both of fewer employers using facial recognition technology in background checks, and preventing employers from being sued by job candidates solely because of the use of a technology that does not further their purpose in flagging employees with criminal backgrounds.

The EEOC has already issued guidance on pre-employment inquiries, recommending that employers not ask for photographs of applicants, and if one is needed for identification purposes, to request it after the employment offer has been extended and accepted.[105] The guidance specifies that information regarding race, sex, national origin, and religion are irrelevant in determining whether the person is qualified for the job.[106] Inquiries that relate to or disproportionately screen out candidates based on race, color, sex, national origin, or religion may be used as evidence of an employer's intent to discriminate, unless the questions have a business purpose.[107] EEOC guidance also makes clear that employers must not use information they receive in background checks, from any source, to discriminate, emphasizing that employers must "take special care" when basing employment decisions on background problems that have a disproportionate impact on people of a certain race, color, national origin, sex, or religion.[108] If employers do use information from background checks to make an adverse employment decision, the Federal Credit Reporting Act ("FCRA") obligates them to notify the applicant that he or she was rejected because of information in the background check report, in-

[103] Senator Kamala Harris has also proposed that the EEOC issue such guidance. Letter from Senator Kamala Harris to the Honorable Victoria Lipnic (Sept. 17, 2018), https://www.scribd.com/document/388920670/SenHarris-EEOC-Facial-Recognition-2 [https://perma.cc/46P9-78A3].

[104] Nicholas R. Parillo, *Federal Agency Guidance and the Power to Bind: An Empirical Study of Agencies and Industries*, 36 Yale J. On Reg. 165, 167–69 (2019).

[105] *Prohibited Employment Policies/Practices: Pre-Employment Inquiries*, U.S. Equal Employment Opportunities Comm'n, https://www.eeoc.gov/prohibited-employment-policiespractices#pre-employment_inquiries [https://perma.cc/A6LA-NLZD].

[106] *Id.*

[107] *Id.*

[108] *Background Checks: What Employers Need to Know*, U.S. Equal Emp. Opportunities Comm'n (Mar. 11, 2014), https://www.eeoc.gov/eeoc/publications/background_checks_employers.cfm [https://perma.cc/W4M6-2RBN].

cluding the contact information for the company that sold the report.[109]

Using facial recognition technology to analyze images of a candidate is no different than directly asking candidates for a photograph and making a hiring decision that takes that photograph into account. The request for a photograph alone is not sufficient to make the employer liable for employment discrimination, but without a legitimate business reason that could not be served by alternative means, employers leave themselves open to liability through Title VII suits.

By issuing guidance, the EEOC can put employers on notice that facial recognition technology is not a special, objective way to use information about appearance to make employment decisions. Rather, like any other method of making employment decisions, its use is subject to scrutiny under existing anti-discrimination law by the EEOC and potential plaintiffs.

Issuing guidance about facial recognition technology would fit into the EEOC's past practices.[110] The EEOC has previously cautioned employers against requesting photographs in resumes,[111] indiscriminately using big data,[112] and using criminal background checks generally.[113] The guideline on the use of criminal background checks states

[109] *Id.*

[110] *See generally* Michael Selmi, *The Value of the EEOC: Reexamining the Agency's Role in Employment Discrimination Law*, 57 Ohio St. L.J. 1 (1996) (discussing the role of the EEOC in employment discrimination claims).

[111] *See, e.g.*, Letter from U.S. Equal Employment Opportunity Commission's Assistant Legal Counsel Carol R. Miaskoff to the Public (Oct. 5, 2004) (on file on the EEOC website), https://www.eeoc.gov/foia/eeoc-informal-discussion-letter-119 [https://perma.cc/TT2B-66V4]; *Prohibited Employment Policies/Practices: Pre-Employment Inquiries*, *supra* note 105 ("[E]mployers should not ask for a photograph of an applicant. If needed for identification purposes, a photograph may be obtained after an offer of employment is made and accepted.").

[112] Press Release from the EEOC, *Use of Big Data Has Implications for Equal Employment, Panel Tells EEOC* (Oct. 13, 2016) (on file on the EEOC website), https://www.eeoc.gov/eeoc/newsroom/release/10-13-16.cfm [https://perma.cc/8ZDD-5ZC9].

[113] *See, e.g.*, *Background Checks: What Employers Need to Know*, *supra* note 108 ("Take special care when basing employment decisions on background problems that may be more common among people of a certain race, color, national origin, sex, or religion; among people who have a disability; or among people age 40 or older. For example, employers should not use a policy or practice that excludes people with certain criminal records if the policy or practice significantly disadvantages individuals of a particular race, national origin, or another protected characteristic, and does not accurately predict who will be a responsible, reliable, or safe employee. In legal terms, the policy or practice has a "disparate impact" and is not "job related and consistent with business necessity."); *Pre-Employment Inquiries and Arrest & Conviction*, U.S. Equal Emp. Opportunities Comm'n, https://www.eeoc.gov/laws/practices/inquiries_arrest_conviction.cfm [https://perma.cc/WJ7L-GNP2]; *Enforcement Guidance on the Consideration of Arrest and Conviction Records in Employment Decisions Under Title VII of the Civil Rights Act*, U.S. Equal Emp. Opportunities Comm'n (Apr. 25, 2012), https://www.eeoc.gov/laws/guidance/arrest_conviction.cfm [https://perma.cc/569G-9Y4K].

that an arrest should be treated differently from a conviction. It is generally permissible to screen based on criminal background checks if the employer "develops a targeted screen considering the nature of the crime, the time elapsed and the nature of the job." However, in the facial recognition context, even more so than in a regular background check, there is no guarantee of a targeted screen. An algorithm searching through law-enforcement databases flags applicants based on mere arrest records because these photograph records are readily available, not convictions.[114] Facial recognition makes use of several tactics that the EEOC has already warned against in screening applicants: making employment decisions based on photographs, and using a broad-based screen to eliminate applicants with an arrest, not just a conviction.

C. *Employers Who Use Facial Recognition Technology in Background Checks May Face EEOC Litigation Under Title VII*

In addition to providing guidance to employers, the EEOC should use its enforcement authority to file lawsuits against employers who use facial recognition technology in background checks. The EEOC will play an especially important role in these kinds of cases because, as discussed above,[115] applicants who submit to facial recognition technology in background checks may have little sense of why they were rejected, and thus will not have the motive to sue to get discovery. Plaintiffs, and their potential attorneys, may face too much uncertainty to invest resources in beginning the litigation process. This is particularly the case after the 2011 Supreme Court decision that made it more difficult for private plaintiffs to bring claims of systemic discrimination and raised the standard for certifying class action lawsuits.[116]

The EEOC may begin enforcement through its administrative process, investigating charges of employment discrimination that include systemic discrimination.[117] The EEOC will be able to invest resources in addressing the problem that plaintiffs may not be able or willing to address due to the uncertainty they face when they are not hired. Through its investigation process, the EEOC can analyze the hiring data from employers that have used facial recognition technology and determine whether its use results in significant statistical disparities

[114] *See* Garvie et al., *supra* note 9, at 28.

[115] *See supra* Part II.A.

[116] *See* Pauline T. Kim, *Addressing Systemic Discrimination: Public Enforcement and the Role of the EEOC*, 95 B.U. L. Rev. 1133, 1134 (2015); Wal-Mart Stores, Inc. v. Dukes, 131 S. Ct. 2541 (2011).

[117] *See Administrative Enforcement and Litigation*, EQUAL EMP. OPPORTUNITY COMM'N (2020), https://www.eeoc.gov/eeoc/enforcement_litigation.cfm [https://perma.cc/D6NE-6NBH].

for different groups of protected class members. The NIST data analyzed algorithms that were voluntarily submitted by companies, and the algorithms significantly underperformed. The EEOC may discover that a company's use of facial recognition technology that was not voluntarily submitted for NIST audit has even worse effects on job applicants, thereby sparking an interest in auditing and improvement of the facial recognition technology it uses before selling it to employers.

The EEOC may also litigate when it does not resolve charges through its administrative processes, exposing employers to litigation.[118] Such public enforcement of civil rights is dependent on the political will of the presidential administration;[119] however, even administrations with substandard records on civil rights enforcement[120] may find that due to the employment crisis caused by the COVID-19 pandemic,[121] there is political will to take down such automated barriers to employment in order to ease the crisis.

Employers themselves should be wary of the use of facial recognition technology in hiring, and not only due to the employment discrimination liability they may face, and not only through the use of the software. Even just a trial run for the use of facial recognition technology may result in liability. If an employer wants to perform a trial run with a new vendor who uses facial recognition technology, then discovers that the algorithm has a disparate impact on a protected class and the majority of people who pass the background check are white men, throwing the results out on the basis of a protected characteristic can itself be a basis for disparate impact liability.[122] In *Ricci v. DeStefano*, the Supreme Court held that when an employer refused to certify exam results that would have resulted in "too many whites" receiving promotions,[123] such "express, race-based decisionmaking violate[d] Title VII's command that employers cannot take adverse employment actions because of an individual's race."[124] Here, if an employer used

[118] *See id.*

[119] *See, e.g.*, Michael Waterstone, *A New Vision of Public Enforcement*, 92 MINN. L. REV. 434, 436 (2007).

[120] *See, e.g.*, Jessica Huseman & Annie Waldman, *Trump Administration Quietly Rolls Back Civil Rights Efforts Across Federal Government*, PROPUBLICA (June 15, 2017), https://www.propublica.org/article/trump-administration-rolls-back-civil-rights-efforts-federal-government [https://perma.cc/D4P9-TGS8]; *Trump Administration Civil and Human Rights Rollbacks, 2017–2020*, LEADERSHIP CONF. ON CIV. & HUM. RTS. (May 13, 2020), https://civilrights.org/trump-rollbacks/ [https://perma.cc/7FSR-T3FE].

[121] *See, e.g.*, Nelson D. Schwartz, '*Nowhere to Hide' as Unemployment Permeates the Economy*, N.Y. TIMES (Apr. 16, 2020), https://www.nytimes.com/2020/04/16/business/economy/unemployment-numbers-coronavirus.html [https://perma.cc/CY44-FR4N].

[122] *See* Ricci v. DeStefano, 557 U.S. 557, 562–63 (2009).

[123] *Id.* at 579 (quoting Ricci v. DeStefano, 554 F. Supp. 2d 142, 152 (D. Conn. 2006)).

[124] *Id.* at 579 (citing 42 U.S.C. § 2000e-2(a)(1)); *see also id.* at 581–82 (allowing race-based decisionmaking based on a good faith belief that such decisionmaking

facial recognition software as part of a background check, then discovered that the result was to not offer employment to any minority candidates, the employer would not be able to "re-screen" the minority applicants without scrutiny from majority groups who would not benefit from the rescreening. And if, on the other hand, the hiring process overall resulted in more members of the protected class being hired than non-members, if facial recognition software has a discriminatory effect against individual members of the protected class, the employer can still be found liable.[125]

Depending on the scale of an employer's hiring practices, the liabilities an employer may face may be significant. If there were a class action lawsuit for all candidates who applied for a particular position and were subject to facial recognition software, the employer would have the burden of proving that each individual member of the class was not affected. Otherwise, in a pattern or practice of discrimination suit, each member of the class is presumed to be the victim of discrimination.[126]

The employer would also not be spared from a disparate impact challenge by adding subjective criteria (meaning criteria that is not standardized but is rather based on the exercise of personal judgment), such as an interview with a current employee as part of the hiring process, in addition to passing the facial recognition criteria.[127] Subjective criteria, as well as objective criteria such as aptitude tests, are also subject to disparate impact analysis.[128]

Employers who nonetheless insist on using facial recognition technology may argue that if candidates give consent to use their photo in a facial recognition process as part of hiring, giving consent may prevent the candidates from claiming that the process is discriminatory. But here, unlike in other contexts where signing terms and conditions cleanse questionable practices, the Court has held that if a practice is discriminatory, it cannot be bargained away.[129] Even with the candidates' consent, an employer who uses facial recognition technology in

avoided disparate impact liability and would lead to racial quota and other impermissible race-based action).

[125] *See* Connecticut v. Teal, 457 U.S. 440, 452 (1982). When the employer imposed, as an absolute condition for consideration for promotion, that applicants pass a written test that excluded blacks in disproportionate numbers and that was not job related, the employer was still held to have violated Title VII even though the "bottom line result" of the promotion practice was to hire a higher proportion of blacks than whites. *Id.* at 451.

[126] *See* Int'l Bhd. of Teamsters v. United States, 431 U.S. 324, 360 (1977).

[127] *See* Watson v. Fort Worth Bank & Tr., 487 U.S. 977, 991 (1988).

[128] *Id.* at 900.

[129] *See* Alexander v. Gardner-Denver Co., 415 U.S. 36, 51 (1974). An employee who must arbitrate a discrimination claim under a collective bargaining agreement may still bring Title VII claims in federal court because the right to a discrimination-free workplace cannot be bargained away. *Id.* at 52.

background checks faces potential liability under Title VII.[130] Consent to the use of facial recognition in a background check does not mean consent to discrimination.

IV. Unjustified Means

Because of the disadvantages and legal liabilities employers may face based on their use of facial recognition technology in background checks, the use of the technology seems to be more trouble than it is worth to employers as a screening tool: the means do not justify any end, as they make the results of the background check less accurate. Although vendors may tout the high accuracy of their facial recognition algorithms, the majority of algorithms have not been independently tested. Of those that have been independently tested by NIST, most show major inaccuracies when handling photographs of individuals who are not white men.[131] Both the legal and the technical disadvantages seem to outweigh any advantage in using facial recognition technology as a background check screening tool.

This is not to say that all facial recognition technology is inherently and irredeemably biased or discriminatory. Facial recognition models that use enormous amounts of data to analyze distances between facial features, such as the local feature analysis method, may not have the same discriminatory effect as facial recognition that uses principal component analysis, which uses relatively few data points in order to speed up the matching process and increase the efficiency of the model.[132] It is possible that local feature analysis algorithms would produce output that is similarly accurate across demographics. But such a method would require a vast amount of computer processing power and a way of correcting the images for face position, and may not yet be commercially viable. Perhaps with further advancement in computer processing power, facial recognition analysis can change the inquiry back to which face is most like the target face, instead of which face is most likely to match.

As the technology currently stands and is sold to employers, facial recognition use in background checks is discriminatory. The Supreme Court recognized in 1973 in *McDonnell Douglas* that the purpose of Congress in enacting Title VII was "to assure equality of employment opportunities and to eliminate those discriminatory practices and devices which have fostered racially stratified job environments to the disadvantage of minority citizens."[133] Using facial recognition technol-

[130] In addition to any potential liability under the FCRA, which may be between $100 and $1,000 per violation. *See* Neumeyer, *supra* note 7.

[131] *See, e.g.*, Grother et al., *supra* note 3, at 2–3.

[132] The NIST report did not examine the underlying code to assess why these demographic differentials were being produced. *See id.* at 9.

[133] McDonnell Douglas Corp. v. Green, 411 U.S. 792, 800 (1973) (citations omitted).

ogy in background checks does the opposite: it provides inequality of employment opportunities and creates a resurgence in discriminatory practices which foster racially stratified job environments to the disadvantage of minority citizens.