

# Police Use of Facial Recognition Technology and Racial Bias – An Assessment of Criticisms of Its Current Use

Seppy Pour

School of Law, University of Sydney, Sydney, Australia

**Email address:**

seppypour@gmail.com

**To cite this article:**

Seppy Pour. Police Use of Facial Recognition Technology and Racial Bias – An Assessment of Criticisms of Its Current Use. *American Journal of Artificial Intelligence*. Vol. 7, No. 1, 2023, pp. 17-23. doi: 10.11648/j.ajai.20230701.13

**Received:** May 3, 2023; **Accepted:** May 25, 2023; **Published:** June 15, 2023

---

**Abstract:** Law enforcement has transformed drastically by advances in technology. Law enforcement bodies around the world have adopted facial recognition capabilities powered by artificial intelligence and contend that facial recognition technology is an effective tool in preventing, disrupting, investigating, and responding to crime. As the practice has grown, so have criticisms of its use and policing outcomes. Criticisms relate to the violation of civil liberties, namely the potential for abuse, propensity for inaccuracies, and improper use. In an effort to assess the validity of these criticisms, this paper examines the link between facial recognition technology and racial bias through an analysis of existing research and the use of a case study of an American municipality that has banned the use of facial recognition technology by police. Studies to date demonstrate a propensity for algorithms to mirror the biases of the datasets on which they are trained, including racial and gender biases; rates of match inaccuracy were consistently seen in relation to black persons, particularly black females. In addition to academic research, multiple examples of misidentifications of black citizens in the United States, along with related commentary from human rights and civil liberties groups, suggests that these concerns are translating into real world injustices. This paper validates concerns with the use of facial recognition technology for law enforcement purposes in the absence of adequate governance mechanisms.

**Keywords:** Artificial Intelligence, Policing, Facial Recognition, Crime, Law Enforcement, Justice, Race

---

## 1. Introduction

Law enforcement has transformed drastically by advances in technology [4]. Police, like the rest of society, have been confronted by an array of new challenges and opportunities in an era of rapid technological change [10]. These advances have brought about the potential for significant improvements to operational efficiency and outcomes [8], particularly during a time when technological advances have similarly given rise to greater demand for police accountability [29].

This technological boom has resulted in the advent of artificial intelligence-led policing. Law enforcement bodies around the world have adopted facial recognition capabilities powered by artificial intelligence [27] and contend that facial recognition technology is an effective tool in preventing, disrupting, investigating, and responding to crime [45].

The use of facial recognition as a form of biometrics outside law enforcement has also expanded proportionately; applications include password verification, social media functionality, and in retail and advertising [23]. Most uses are

generally uncontroversial – self-excluded problem gamblers for example are currently refused entry from gaming venues with facial recognition used, with consent, to identify them [18]. But as the practice has grown in the context of law enforcement, so have criticisms of its use and policing outcomes [36]. Among the many objections is its high rate of inaccuracy, particularly when used in relation to racial minorities [12].

It is necessary for the purposes of this paper to define some key terms. ‘Facial analysis’ broadly describes any diagnostic method capable of structural analysis of a person’s face [39]. ‘Facial recognition’ is any technology which utilizes facial analysis capabilities to identify or verify the identity of a person, typically from a still image or video footage [39]. ‘Artificial intelligence’ is the underlying algorithmic tool which enables facial recognition technology [11].

In this paper, the link between facial recognition technology and racial bias will be reviewed through an analysis of existing research. The review will consider a recent case study in which the use of facial recognition technology by law

enforcement was banned by jurisdiction officials. It will also analyze academic research which has attempted to highlight the propensity for racial bias and the circumstances in which such outcomes have arisen. It is intended that this paper will provide a historical account of the research into the intersection of facial recognition technology and racial bias, demonstrating that there is concern for the use of facial recognition technology in the absence of adequate governance mechanisms.

## 2. The Inaugural Ban on Facial Recognition

Facial recognition technology has existed since the mid-20<sup>th</sup> century [48]. The original approach designed by Woodrow Bledsoe involved manually calculating the distance between the facial features in a suspect photo and loading these dimensions into a computer for pattern matching against a database of mugshots. As early as 1966, Bledsoe noted the difficulties of such an approach to facial recognition:

“This recognition problem is made difficult by the great variability in head rotation and tilt, lighting intensity and angle, facial expression, aging, etc. Some other attempts at facial recognition by machine have allowed for little or no variability in these quantities... In particular, the correlation is very low between two pictures of the same person with two different head rotations [48].”

As we will see in the following parts of this paper, the difficulties identified by Bledsoe remain relevant to this day.

In May 2019, the city of San Francisco, CA banned by city ordinance the use of non-pre-approved facial recognition technology by law enforcement agencies [6]. The move, which was decided almost unanimously by the city’s Board of Supervisors, enshrined San Francisco as the first major city in the US to prohibit the tactic. Since then, other jurisdictions have gone on to ban or limit the use of facial recognition for various purposes [15].

The rationale for the ban can be deduced by examining the city ordinance [38]. As one of the earliest examples of an official ban on facial recognition, this rationale will underpin the discussion in this paper.

## 3. The Propensity for Facial Recognition Technology to Endanger Civil Rights and Civil Liberties

The ordinance, dubbed the ‘Stop Secret Surveillance’ ordinance, listed in its general findings that:

“(d) The propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring [38].”

This finding is not without validity. A seminal analysis by Phillips et al found that facial recognition technologies

developed in France, Germany and United States correctly identified Caucasian persons more accurately than East Asian persons; those developed in China, Japan and South Korea identified East Asian persons more readily [24]. The authors therefore deduced that the efficacy of a facial recognition algorithm was influenced by the origin of its developers and the demographic makeup of the database on which it operates [24].

Numerous studies have since bolstered these findings. Klare et al’s analysis found that facial recognition algorithms demonstrated lower accuracy on female cohorts (compared to male cohorts), black persons (compared to Caucasian and Hispanic persons), and 18-30-year-olds (compared to 30-50 year olds and 50-70 year olds) [19]. This discrepancy was consistently observed across six facial recognition technologies, in both those trainable vs untrainable and those commercially available vs non-commercially available [19]. Facial recognition tests on identical twins have also exhibited lower rates of accuracy when comparing footage taken during dissimilar periods (i.e. two still images or videos taken a long time apart), subjects not maintaining a neutral expression, and in differing lighting conditions [47].

Similar shortcomings have been identified through work undertaken by the National Institute of Standards and Technology (NIST) which conducts voluntary tests of commercially available facial recognition tools every four years [46]. The NIST regularly hosts competitions to compare the efficacy of facial recognition algorithms against human facial reviewers [44]. Phillips and O’Toole’s systematic analysis these competition results found that while facial recognition technology was superior to human reviewers at matching frontal faces in still images, human reviewers fared far greater when analyzing video footage or complex still images [25]. Academics have therefore surmised that the most accurate facial recognition outcomes are obtained when human reviewers and facial recognition technology is used in tandem [26].

## 4. Robust Transparency, Oversight, and Accountability Measures

The ordinance further endorses the view that:

“(e) Legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any surveillance technology is deployed [38].”

On 23 February 2018, Buolamwini and Gebru presented at the Conference on Fairness, Accountability and Transparency a paper that would go on to become a landmark study on the effectiveness of facial recognition technology. The paper, entitled *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification (Gender Shades)*, represented the first intersectional analysis of three commercially available facial analysis technologies [40]. The study observed stark differences in the technologies’ ability to recognize lighter-toned males, lighter-toned females,

darker-toned males, and darker-toned females (the study groups). While there were negligible error rates in relation to lighter-toned males and lighter-toned females across all three algorithms, error rates were observed in relation to darker-toned males and significantly more so in relation to darker-toned females. Accordingly, the authors concluded that all three algorithms performed better on male faces than female faces and on lighter faces than darker faces. Buolamwini and Gebru additionally note that since default camera settings are optimized for lighter skin, accuracy rates are further skewed against darker-toned persons.

The NIST's 2019 quadrennial analysis of facial recognition algorithms confirmed the *Gender Shades* findings. The authors noted the "recent expansion in the availability, capability, and use of face recognition" and that this expansion had been "accompanied by assertions that demographic dependencies could lead to accuracy variation and potential bias" [14]. The findings included a higher false match rate in relation to faces from East African, West African, and Caribbean person groups compared to those from East Asian or Eastern Europe groups; false match rates were higher for the East Asian person group than the Eastern European group (however this divergence was lower for algorithms developed in China). False matches were consistently more prevalent for women than men across all algorithms regardless of origin, although the effect was less profound than that based on skin tone. Additionally, false positives were higher for both genders in the 12-20-year-old and 65-and-over age groups regardless of skin tone.

As a result of the academic publication of *Gender Shades* (as well as a website infographing its findings) [40], the three commercial facial recognition algorithms tested by Buolamwini and Gebru were notified of the embedded bias of their respective products. To analyze the impact of publicly demonstrating such shortcomings, Buolamwini and Raji retested the three algorithms roughly seven months following the publication of *Gender Shades (Actionable Audits)* [42]. All three proprietors (the Target Corporations), namely Microsoft, Megvii and IBM, demonstrated an improvement in the accuracy of their algorithms: all three showed less accuracy difference between male vs female and lighter tone vs darker tone study groups. Unsurprisingly, all three still demonstrated their highest error rates in relation to the darker-toned female subject group. The lowest error rates were still observed in relation to lighter-toned male subject group.

In addition to the existing three algorithms which were re-tested, Buolamwini and Gebru added to this audit two previously untested facial recognition algorithms: Amazon's 'Rekognition' and Kairos (the Non-Target Corporations). The initial test on the Non-Target Corporations showed that their error rates were considerably higher than the Target Corporations at the time of the analysis but were comparable to the error rates exhibited by the Target Corporations in the *Gender Shades* study. The Non-Target Corporations mirrored the findings of the Target Corporations – Rekognition and Kairos performed better on male faces than female faces and

on lighter-toned faces than darker-toned faces. The Non-Target Corporations showed the worst performance for darker-toned females sub-group.

As concluded by Buolamwini and Raji, it can be deduced that the work undertaken through *Gender Shades* has had the effect of encouraging corporations into prioritizing the reduction of racial and gender bias in their products. Moreover, the study's contribution to public discourse and corresponding media attention would presumably have had the added effect of encouraging other product providers to scrutinize their algorithms despite not being directly audited by the authors. Notwithstanding the positive impacts of *Gender Shades*, public scrutiny of error-prone algorithms is not always enough to motivate improvement, as discussed in the following section.

## 5. Intimidate and Oppress Certain Communities and Groups

The Stop Secret Surveillance ordinance unsurprisingly includes in its general findings section:

"(c) While surveillance technology may threaten the privacy of all of us, surveillance efforts have historically been used to intimidate and oppress certain communities and groups more than others, *including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective* (emphasis added) [38]."

The potential for false matches discussed in the previous section is particularly unsettling given the highly documented disparities in policing strategies and outcomes.

The link between law enforcement and racial bias is well documented. Racial bias within law enforcement has been highlighted in previous research, particularly among white male police officers [28]. Analysis of common police practices have also revealed disproportionate effects of policing on racial minorities [28]. Disproportionality has been observed at various contact points between police and people of color, including street stops [9], drug enforcement strategies [21], vehicle pullovers [20], and the quantity and attitudes of officers deployed in communities of color [34]. In the Australian context, for example, Indigenous Australians are roughly 20 times more likely to be arrested than their non-Indigenous counterparts [30]. This over-representation has been attributed to historical police practices and crime strategies, including when police make the decision to make an arrest and the number of officers deployed to locations of high Indigeneity [30]. Police have therefore historically failed to use their discretion appropriately to reduce Indigenous representation within the criminal justice system [5].

### 5.1. Robert Julian-Borchak Williams [17]

Wrongful arrests of people of color based on inaccurate facial recognition analysis are not unheard of. One of the more high-profile incidents involved Robert Julian-Borchak Williams of Farmington Hills, MI. Williams was apprehended

in January 2020 when Detroit Police, then investigating the theft of five watches worth approximately \$US3,800, received a ‘match’ on an image of a suspect taken from a security video pertaining to the case. Upon receiving the facial analysis results, two officers attended Williams’ home and placed him under arrest. When Williams’ wife asked where he was being taken, one of the officers responded, “Google it”. At the station, Williams was photographed, fingerprinted, and had his DNA swabbed before being detained overnight. He was questioned – all based on nothing but an alleged match of his face with that of a suspect in a video. Upon being shown still images from the security footage, Williams strongly denied that he was the man in the picture. He reportedly picked up the still image, held it next to his face and said to the officers, “You think all black men look alike?”. Little did Williams know that in this case, it wasn’t the officers who made the identification.

## 5.2. Post Gender Shades

Stories like Williams’ are not unique [13]. And to avoid doubt, it should be mentioned that Williams’ case and many others like it have occurred in the 2020s, following the publication of *Gender Shades* and *Actionable Audits*. These cases all have something else in common: lack of transparency and oversight. And while individual police departments may choose to implement department-level policies or procedures on the use of facial recognition technologies, there is little regulation at present governing the use of facial recognition technology at state or federal levels in most jurisdictions. The haste with which facial recognition technology has technologically advanced and subsequently adopted by law enforcement means that the legal system has failed to keep up.

Academics and human rights activists are not the only ones advocating for better governance of facial recognition technology. Microsoft, one of the early developers of commercially available facial recognition software, has publicly stated that the technology issues “heighten responsibility for tech companies that create these products” and accordingly advocated for “thoughtful government regulation and for the development of norms around acceptable uses” [32]. Microsoft has subsequently gone on to acknowledge the racial bias in facial recognition technology and called for improved transparency and the use of human review of facial recognition analysis [33]. Google, whose facial recognition software has previously mixed up images of black people with gorillas [31], has similarly vowed not to sell its facial recognition technology product until the underlying technology is adequately regulated [22].

In its address to the public, Microsoft called on the government to regulate the proper use of facial recognition technology, rather than “to ask unelected companies to regulate [the governance space]” because “even if one or several tech companies alter their practices, problems will remain if others do not” [33]. The company was remarkably foresighted in this respect. Following the publication of *Gender Shades*, a distinct reduction in error rates in the Target Corporation’s algorithm error rates could be seen [40]. Unlike

the Target Corporations, however, Amazon, one of the two previously untested companies included in *Actionable Audits*, has had a significantly different response to the claims about the accuracy of its service offering.

On 26 January 2019, Amazon published its response to *Actionable Audits* (the Response) [37]. The Response accused *Actionable Audits* of being misleading and drawing false conclusions. The Response effectively obfuscated *Actionable Audits*’ findings against Rekognition in three ways. Firstly, it argued that ‘facial analysis’ and ‘facial recognition’ are “completely different in terms of their underlying technology”, suggesting that the entire premise of *Actionable Audits* was misguided. Secondly, it claimed that Buolamwini and Raji had tested an outdated version of Rekognition that lacked a number of improvements introduced by Amazon in November 2018. Thirdly, the Response claimed that Amazon’s own “extensive” internal testing had produced “no significant difference in accuracy with respect to gender [or race] classification”. The author claimed that Amazon had undertaken a test of facial recognition involving a “Megaface dataset of 1 million images... and found exactly zero false positive matches”.

While the Amazon response concludes, “we are very interested in working with academics in establishing a series of standardized tests for facial analysis and facial recognition”, Buolamwini has publicly stated that Amazon’s response to her work has been “one of denial, deflection, and delay” [39]. For Buolamwini, it is imperative for facial recognition technology to be independently tested by external parties. She states that she “time and time again [finds] that the internal accuracy rates if reported by companies seem to be at odds with external accuracy rates reported by independent third parties”. In other words, such impressive results can be willfully obtained by using low quality baseline benchmarks. Accordingly, developers of facial recognition technologies should be compelled to undergo external audit for evaluation in “real-world cases with the results submitted for public scrutiny”.

## 6. Meaningful Public Input

But in a world where commercial interests largely dictate corporate decision making, should accountability lie with software developers? Arguably so, but as Microsoft suggested in its public address, placing the onus of responsibility on governments would be far more effective in meeting public goals of a healthier dynamic for consumers and developers alike [32]. The Stop Secret Surveillance ordinance addresses community consultation as follows:

“(e) Whenever possible, decisions regarding if and how surveillance technologies should be funded, acquired, or used, and whether data from such technologies should be shared, should be made only after meaningful public input has been solicited and given significant weight [38].”

It must, however, be understood that this adequate governance is twofold. Firstly, the design and implementation of overseeing legislation must be undertaken by the legislature. In the US and

Australian contexts, this would be the responsibility of both the state government (to the extent that facial recognition use relates to policing, corrections, and any other state jurisdictional matters) and the federal government. Regulations would require extensive consultation with industry groups, law enforcement officials, and civil rights groups to develop a well-balanced governance framework with adequate safeguards. The Australian Human Rights Commission has twice called for a halt to the government's use of facial recognition technology until adequate protections are put in place [1].

Secondly, day-to-day accountability of facial recognition must become a reality before it can be validly used by law enforcement, particularly in the legal context, because accountability goes beyond simply auditing a facial recognition algorithm. This is because the use of facial recognition by law enforcement agencies is also largely opaque and unaccountable. Consider how the use of facial recognition would occur in practice: an officer may 'identify' person as a suspect by virtue of an algorithm presenting the person as a 'match'. The officer makes an arrest based on that intelligence and, in the absence of any indisputable evidence to the contrary, that individual becomes a suspect and investigatory resources are largely put towards proving that individual's culpability. Because police tactics are typically not submitted as evidence in criminal trials, the technique is not subject to the same level of public or judicial scrutiny as other forms of intelligence and evidence gathering. The practice is therefore largely undocumented and untested in the public domain.

If one were to apply this impediment to the Robert Julian-Borchak Williams case study, we realize that Williams could not have reasonably known that his identification was made by a computer algorithm. In fact, according to the American Civil Liberties Union (ACLU) who represented Williams in his criminal case, Williams was only made aware of the use of facial recognition thanks to a sarcastic comment from one of the investigating officers that "the computer must have gotten it wrong" [43]. Williams also had an alibi at the time of the alleged offense, but this was simply ignored. The ACLU raised procedural fairness issues concerning the inability to challenge facial recognition results, both through a lack of knowledge on how particular algorithms work and because most defendants do not even know that a match was the basis for police suspicion. While facial recognition results are sometimes likened to the results of fingerprinting of DNA analysis, facial recognition technology is largely unexamined thus far and can be undertaken in secret [2].

Further raising roadblocks in practice is police departments resisting attempts by civil rights and privacy advocates to bring light to how and when facial recognition technology is used. In one high-profile example, a black man in Florida was convicted of supplying drugs to undercover officers after facial recognition was used to identify him [7]. Detectives in this case received multiple potential matches from a photo of the suspect, but the defendant was never given access to photos of the other matches. Despite multiple appeals arguing that this undermined the defendant's right to receive evidence favorable to the accused, the photos have not been turned over. In New York, the

New York Police Department (NYPD) went to great legal lengths to claw back documentation relating to its use of facial recognition technology that it had accidentally disclosed to the Georgetown Center on Privacy and Technology through administrative error [3]. The NYPD was successful in its legal action but was criticized for "inconsistently and selectively disclosing information" and being "mystifying [in] what [it] was trying to keep from the public".

## 7. Conclusion

The Stop Secret Surveillance ordinance imposed in San Francisco represents a progressive movement against the unknowns of facial recognition technology. Analysis of the ordinance demonstrates a clear concern for the lack of checks and balances in the use of facial recognition technology, its demonstrated tendency result in racial bias, its potential for abuse, and the lack of public consultation in its adoption. Despite the many unknowns of facial recognition, there is adequate evidence to suggest that these are valid concerns.

This paper reviewed the most influential studies to date on the accuracy rates of facial recognition technologies. These studies consistently demonstrated a propensity for algorithms to mirror the biases of the datasets on which they are trained, including any in-built racial or gender biases. Beyond the academic analyses, multiple examples of misidentifications of black citizens in the US, with related commentary from human rights and civil liberties groups, suggests that these concerns are translating into real world injustices.

Facial analysis and facial recognition technology has existed since the 1960s, but their current forms are a relatively new concept. Their design, capabilities, accuracy, versatility, and uses are rapidly evolving. With this evolution has come many questions and concerns regarding the risks of this type of technology. Notwithstanding the tremendous law enforcement value it provides, these questions are valid and must be addressed before facial recognition is used for any purpose which could result in the deprivation of an individual's liberty.

## References

- [1] Bajkowski, Julian, 'Human Right Commission wants moratorium on expanding facial recognition', *itnews* (online, 17 December 2019) <<https://www.itnews.com.au/news/human-rights-commission-wants-moratorium-on-expanding-facial-recognition-535684>>
- [2] Brown, Stephen Rex, 'A \$50 crack sale in Florida could yield significant ruling on facial recognition', *NY Daily News* (online, 22 March 2018) <<https://www.nydailynews.com/news/crime/50-crack-sale-florida-lead-facial-recognition-change-article-1.3888958>>
- [3] Brown, Stephen Rex, 'NYPD claws back documents on facial recognition it accidentally disclosed to privacy researchers', *NY Daily News* (online, 14 April 2019) <<https://www.nydailynews.com/new-york/ny-nypd-facial-recognition-disclosures-20190414-ifwgro76cje5tgiyq6wqsty7ou-story.html>>

- [4] Chan, Janet, 'The technological game: How information technology is transforming police practice' (2001) 1 (2) *Criminal Justice* 139.
- [5] Crehan, A Corbo, "'Appropriate" Police Discretion and Indigenous Over-Representation in the Criminal Justice System' (2010) 11 (1) *Australian Journal of Professional and Applied Ethics* 1.
- [6] Conger, Kate, Fausset, Richard and Kovalski, Serge F, 'San Francisco Bans Facial Recognition Technology', *The New York Times* (online, 14 May 2019) <<https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>>
- [7] Conarck, Ben, 'Court denies facial recognition evidence appeal', *The Florida Times-Union* (online, 23 January 2019) <<https://www.jacksonville.com/story/news/crime/2019/01/23/florida-court-prosecutors-had-no-obligation-to-turn-over-facial-recognition-evidence/6215668007>>
- [8] Ericson, Richard V and Haggerty, Kevin D, *Policing the Risk Society* (University of Toronto Press, 1997).
- [9] Fagan, Jeffrey, Braga, Anthony A, Brunson, Rod K and Pattavina, April, 'Stops and Stares: Street Stops, Surveillance, and Race in the New Policing' (2016) 43 *Fordham Urban Law Journal* 539.
- [10] Ferguson, Andrew, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press, 2017).
- [11] Ford, Trenton W, 'It's time to address facial recognition, the most troubling law enforcement AI tool', *Bulletin of the Atomic Scientists* (online, 10 November 2021) <<https://thebulletin.org/2021/11/its-time-to-address-facial-recognition-the-most-troubling-law-enforcement-ai-tool>>
- [12] Garvie, Clare and Frankle, Jonathan, 'Facial-Recognition Software Might Have a Racial Bias Problem', *The Atlantic* (online, 8 April 2016) <<https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991>>
- [13] General, John and Sarlin, Jon, 'A false facial recognition match sent this innocent Black man to jail', *CNN* (online, 29 April 2021) <<https://edition.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html>>
- [14] Grother, Patrick, Ngan, Mei and Hanaoka, Kayee, 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects', *National Institute of Standards and Technology* (Report, 19 December 2019).
- [15] Hamilton, Brent and Berry, Kate, 'Portland Becomes First Jurisdiction to Ban Certain Uses of Facial Recognition by Private Businesses', *Davis Wright Tremain LLP* (Web Page, 21 January 2021) <<https://www.dwt.com/blogs/privacy--security-law-blog/2021/01/portland-facial-recognition-ban>>
- [16] Hendry, Justin, 'Human Rights Commission calls for temporary ban on 'high-risk' govt facial recognition', *itnews* (online, 28 May 2021) <<https://www.itnews.com.au/news/human-rights-commission-calls-for-temporary-ban-on-high-risk-govt-facial-recognition-565173>>
- [17] Hill, Kashmir, 'Wrongfully Accused by an Algorithm', *The New York Times* (online, 24 June 2020) <<https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>>
- [18] Kidd, Jessica, 'NSW Pubs and clubs to install facial recognition technology to help stop self-excluded gamblers', *ABC News* (online, 19 October 2022) <<https://www.abc.net.au/news/2022-10-19/pubs-clubs-install-facial-recognition-tech-problem-gambling/101549802>>
- [19] Klare, Brendan, Burge, Mark J, Klontz, Joshua C, Vorder Bruegge, Richard W and Jain, Anil K, 'Face Recognition Performance: Role of Demographic Information' (2012) 7 (6) *IEEE Transactions on Information Forensics and Security* 1789.
- [20] Lundman, Richard J and Kaufman, Robert L, 'Driving While Black: Effects of Race, Ethnicity, and Gender on Citizen Self-Reports of Traffic Stops and Police Actions' (2003) 41 (1) *Criminology* 195.
- [21] Mitchell, Ojmarrh and Caudy, Michael, 'Examining Racial Disparities in Drug Arrests' (2015) 32 (2) *Justice Quarterly* 288.
- [22] Nieva, Richard, 'Google vows not to sell its facial recognition technology for now', *CNET* (online, 13 December 2018).
- [23] Parmar, Divyarajsinh N and Mehta, Brijesh B, 'Face Recognition Methods & Applications' (2014) 4 (1) *International Journal of Computer Applications in Technology* 84.
- [24] Phillips, P Jonathan, Jiang, Fang, Narvekar, Abhijit, Ayyad, Julianne and O'Toole, Alice J, 'An Other-Race Effect for Face Recognition Algorithms' (2011) 8 (2) *ACM Transactions on Applied Perception* 1.
- [25] Phillips, P Jonathan and O'Toole, Alice J, 'Comparison of human and computer performance across face recognition experiments' (2014) 32 *Image and Vision Computing* 74.
- [26] Phillips, P Jonathan, Yates, Amy N, Hu, Ying and O'Toole, Alice J, 'Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms' (2018) 115 (24) *Psychological and Cognitive Sciences* 6171.
- [27] Rainie, Lee, Funk, Cary, Anderson, Monica and Tyson, Alec, 'Public more likely to see facial recognition use by police as good, rather than bad for society', *Pew Research Centre* (online, 17 March 2022) <<https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society>>
- [28] Roscigno, Vincent J and Preto-Hodge, Kayla, 'Racist Cops, Vested "Blue" Interests, or Both? Evidence from Four Decades of the General Social Survey' (2021) 7 *Socius: Sociological Research for a Dynamic World* 1.
- [29] Rossler, Michael, 'The Impact of Police Technology Adoption on Social Control, Police Accountability, and Police Legitimacy' in Cara Rabe-Hemp & Nancy Lind (ed), *Political Authority, Social Control, and Public Policy* (Emerald Publishing, 2019) 209.
- [30] Simmons, Amy, "'Over-policing to blame' for Indigenous prison rates", *ABC News* (online, 25 June 2009) <<https://www.abc.net.au/news/2009-06-25/over-policing-to-blame-for-indigenous-prison-rates/1332486>>
- [31] Simonite, Tom, 'When It Comes to Gorillas, Google Photos Remains Blind', *Wired* (online, 11 January 2010) <<https://www.wired.com/story/when-it-comes-to-gorillas-google-photos-remains-blind>>

- [32] Smith, Brad, 'Facial recognition technology: The need for public regulation and corporate responsibility', *Microsoft On the Issues* (Web Page, 13 July 2018) <<https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility>>
- [33] Smith, Brad, 'Facial recognition: It's time for action', *Microsoft On the Issues* (Web Page, 6 December 2018) <<https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action>>
- [34] Smyton, Robin, 'How Racial Segregation and Policing Intersect in America', *TuftsNow* (online, 17 June 2020) <<https://now.tufts.edu/2020/06/17/how-racial-segregation-and-policing-intersect-america>>
- [35] Stokes, Elaisha, 'Wrongful arrest exposes racial bias in facial recognition technology', *CBS News* (online, 19 November 2020) <<https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime>>.
- [36] Valentino-DeVries, Jennifer, 'How the Police Use Facial Recognition, and Where It Falls Short', *The New York Times* (online, 12 January 2020) <[nytimes.com/2020/01/12/technology/facial-recognition-police.html](https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html)>
- [37] Wood, Matt, 'Thought on Recent Research Paper and Associated Article on Amazon Rekognition', *Amazon Web Services* (Web Page, 26 January 2019) <<https://aws.amazon.com/blogs/machine-learning/thoughts-on-recent-research-paper-and-associated-article-on-amazon-rekognition>>
- [38] 'Acquisition of Surveillance Technology' (City Ordinance, 5 June 2019) <<https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A>>
- [39] Buolamwini, Joy, 'Response: Racial and Gender bias in Amazon Rekognition — Commercial AI System for Analyzing Faces.' *Hackernoon* (Web Page, 26 January 2019) <<https://hackernoon.com/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced>>
- [40] Buolamwini, Joy and Gebru, Timnit, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (Conference Paper, Conference on Fairness, Accountability, and Transparency, 23 February 2018).
- [41] Buolamwini, Joy, Gebru, Timnit, Raynham, Helen, Raji, Deborah, and Zuckerman, Ethan, 'Gender Shades', *MIT Media Lab* (Web Page) <<http://gendershades.org/overview.html>>
- [42] Buolamwini, Joy and Raji, Inioluwa Deborah, 'Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products' (Conference Paper, AAAI/ACM Conference on AI, Ethics, and Society, January 2019).
- [43] Burton-Harris, Victoria and Mayor, Philip, 'Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart', *ACLU* (Web Page, 24 June 2020) <<https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart>>
- [44] 'Face Challenges', *National Institute of Standards and Technologies* (Web Page, 27 March 2019) <<https://www.nist.gov/programs-projects/face-challenges>>
- [45] 'Facial Recognition', *NSW Police Force* (Web Page) <[https://www.police.nsw.gov.au/crime/terrorism/terrorism\\_categories/facial\\_recognition](https://www.police.nsw.gov.au/crime/terrorism/terrorism_categories/facial_recognition)>
- [46] 'Face Recognition Vendor Test (FRVT)', *National Institute of Standards and Technologies* (Web Page, 30 November 2020) <<https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt>>
- [47] Phillips, P Jonathan, Flynn, Patrick J, Bowyer, Kevin W, Vorder Bruegge, Richard W, Grother, Patrick J, Quinn, George W and Pruitt, Matthew, 'Distinguishing Identical Twins by Face Recognition' (Conference Paper, International Conference on Automatic Face and Gesture Recognition, 21 March 2011).
- [48] 'Woodrow Bledsoe Originates of Automated Facial Recognition', *History of Information* (Web Page) <<https://www.historyofinformation.com/detail.php?entryid=2495>>