Facial Recognition Technology

Last year, facial recognition software built by Gfycat, a technology startup based in Palo Alto, failed to distinguish Asian celebrities, as well as its own Asian employees.[i] Although the team eventually reduced the error rates for identifying Asian faces, this situation illustrates a larger problem facing other companies that compete in the global facial recognition technology market, which is growing by 16.6% each year and is expected to be worth $7 billion by 2024.[ii]

Facial recognition is a type of biometric technology that analyzes images of human faces for the purpose of identification and/or classification.[iii] While this technology has existed since the 1980s, it has been transformed in recent years by the pairing of deep learning with an unprecedented amount of data that can be inexpensively stored and analyzed with the help of cloud computing.[iv] Modern facial recognition systems are often based on neural sets and use various methods to analyze faces. To develop algorithms capable of identifying and classifying faces accurately, software engineers "train" them with massive data sets of facial images. For two of the technology's most common applications – "one-to-one matching" (the act of verifying that the photo of a person matches a different photo of the same person in a database) and "one-to-many matching" (the act of determining whether the person in a photo has any matches in a database) – it is important to produce as few "false positives," or false identifications, as possible.[v]

Evidence of Bias

Many facial recognition companies are still in the process of refining their business models, but most focus on licensing their software to customers, such as high schools, retailers, and law enforcement agencies.[vi] Despite the increasing prevalence of facial recognition technology in society, studies show that it is less accurate for people of color and women. In an MIT Media Lab study, computer systems using facial images to recognize skin color and gender could correctly classify lighter-skinned men 99% of the time, whereas the same systems could only correctly classify darker-skinned women as little as 65% of the time.[vii] While numerous factors contribute to algorithmic bias, one of the major culprits is existing benchmark data sets, which overrepresent lighter-skinned men and underrepresent darker-skinned people in general.[viii]

A different study found that two facial recognition services, Face++ and Microsoft AI, interpret facial expressions differently by race and assign more negative emotion to African American faces.[ix] In addition, the American Civil Liberties Union conducted a test in which Amazon's facial recognition service incorrectly matched 28 members of Congress with mugshots – disproportionately misclassifying members who are people of color.[x] Most recently, the National Institute of Standards and Technology (NIST) published a report about the effect of demographics on the performance of 189 facial recognition algorithms submitted by 99 developers, who altogether represent the majority of the industry.[xi] Researchers found that

algorithms developed in the United States produced higher rates of false positives in one-to-one matching for Asians, African Americans, and native groups (including Pacific Islanders), putting members of these communities at a higher risk of experiencing a data security threat. Researchers also observed higher rates of false positives across all algorithms in one-to-many matching for African American women, which puts them at a higher risk of being falsely accused of a crime.

Consequences of Flawed Technology

The deployment of flawed facial recognition technology is detrimental to broad swaths of the United States population – not only people of color and women, but also elderly people and children.[xii] Concerning the Asian American and Pacific Islander (AAPI) community, the MIT Media Lab study's results suggest that darker-skinned community members, particularly those who present themselves as women, are at a higher risk of being misidentified. NIST's findings about AAPIs are also troubling because in "[one-to-one verification] applications where subjects apply for some benefit more than once under different biographic identities e.g. visa-shopping, driving license issuance, benefits fraud, an otherwise undetected false positive might lead to various downstream consequences such as financial loss."[xiii]

Despite evidence of bias in facial recognition systems, more and more law enforcement and immigration enforcement agencies are using the technology as a surveillance tool. For instance, in the absence of federal facial recognition laws, federal agencies have forged working relationships with officials at departments of motor vehicles in states like Utah, where Federal Bureau of Investigation (FBI) and Immigration and Customs Enforcement (ICE) agents logged over 1,000 facial recognition searches between 2015 and 2017.[xiv] In addition, in fiscal year 2018 alone, the FBI ran over 52,000 searches – an average of over 4,000 searches per month.[xv] This level of activity is deeply concerning, given both the well-documented existence of bias and a report commissioned by Scotland Yard in 2019 which found that 81% of suspects flagged by the London Metropolitan Police's facial recognition system were innocent.[xvi] If law enforcement officers in the United States begin depending heavily on flawed technology to initiate immediate-response and street-level interactions, they might end up subverting due process protections, arresting innocent individuals, and damaging community trust.[xvii] In a similar vein, flawed technology could lead immigration enforcement officers to target individuals who happen to resemble undocumented suspects for detention and deportation.[xviii]

In addition to these concerns, the deployment of facial recognition technology as a surveillance tool at public events could threaten First Amendment protections. For example, in a presentation from 2010, the FBI expressed a desire to use its Next Generation Identification (NGI) biometric database to track people's movements to and from "critical events," such as political rallies.[xix] Moreover, during protests in the wake of Freddie Gray's death in 2015, Baltimore police officers and a social media intelligence company analyzed social media posts and ran photos through a facial recognition system to identify and arrest protestors with outstanding warrants.[xx] Such incidents demonstrate the technology's potential to deter participation in First Amendment-related activities, in spite of past Supreme Court rulings affirming that an individual's right to anonymity is a subset of their right to free speech and association.[xxi] Whereas members of a crowd previously had a reasonable expectation of anonymity and thus privacy, the deployment of facial recognition surveillance may lead them to

fear scrutiny and retaliation due to their association with a certain ideology, movement, or social group. This chilling effect may have a particularly grave impact on historically monitored communities of color, immigrant communities, and religious groups, causing them to feel increasingly reluctant to exercise their freedoms of speech, assembly, and religion.

---

[i] Tom Simonite, "How Coders Are Fighting Bias in Facial Recognition Software," Wired (Mar. 29, 2018), https://www.wired.com/story/how-coders-are-fighting-bias-in-facial-recognition-software/.
[ii] "Facial Recognition Market worth $7.0 billion by 2024," MarketsandMarkets (Jun. 27, 2019), https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp.
[iii] "Face Recognition Technology," American Civil Liberties Union, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology.
[iv] Jeff John Roberts, "The Business of Your Face," Fortune (Mar. 27, 2019), http://fortune.com/longform/facial-recognition/.
[v] "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," National Institute of Standards and Technology (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.
[vi] Jeff John Roberts, "The Business of Your Face," Fortune (Mar. 27, 2019), http://fortune.com/longform/facial-recognition/.
[vii] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[viii] *Ibid.*
[ix] Lauren Rhue, "Racial Influence on Automated Perceptions of Emotions," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765.
[x] Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots," American Civil Liberties Union (Jul. 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.
[xi] "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," National Institute of Standards and Technology (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.
[xii] Drew Harwell, "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use," *The Washington Post* (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.
[xiii] Patrick Grother, Mei Ngan, and Kayee Hanaoka, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," National Institute of Standards and Technology (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[xiv] Drew Harwell, "FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches," *The Washington Post* (Jul. 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/?mc_cid=ea937c8839&mc_eid=3ef2e44055&noredirect=on&utm_term=.eabb4bec89af.
[xv] "Facing the Future of Surveillance," The Constitution Project's Task Force on Facial Recognition Surveillance and Jake Laperruque (Mar. 9, 2019), https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/#heading-3.
[xvi] Guy Davies, "Over 80% of facial recognition suspects flagged by London's Met Police were innocent, report says," ABC News (Jul. 4, 2019), https://abcnews.go.com/International/80-facial-recognition-suspects-flagged-londons-met-police/story?id=64129255.
[xvii] "Facing the Future of Surveillance," The Constitution Project's Task Force on Facial Recognition Surveillance and Jake Laperruque (Mar. 9, 2019), https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/#heading-3.
[xviii] Bill Chappell, "ICE Uses Facial Recognition To Sift State Driver's License Records, Researchers Say," NPR (Jul. 8, 2019), https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers-sa.
[xix] Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology," Electronic Frontier Foundation (Feb. 12, 2018), https://www.eff.org/wp/law-enforcement-use-face-recognition.
[xx] Russell Brandom, "Facebook, Twitter, and Instagram surveillance tool was used to arrest Baltimore protestors," The Verge (Oct. 11, 2016), https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api.
[xxi] *See Buckley v. American Constitutional Law Foundation Inc; NAACP v. Alabama*