2-21-2022

Facial Recognition Technology: Issues, Legislation, and a Need for Education

Ivan Bohorquez

CICLR Feb 21 5 min read

Facial Recognition Technology: Issues, Legislation, and a Need for Education

By: Ivan Bohorquez

Artificial Intelligence ("AI") could be understood as information gathered through the use of technical machines that focus on cognition.[1] At the micro-level, some examples of AI collecting devices include emotional detection tools, [2]numberplate recognition devices, social network analysis devices, and – most known – Facial Recognition Technologies. [3] Facial Recognition Technologies ("FRT") compile and analyze human faces and are often used to build complex systems of identification and tracking.[4] AI and FRT have been employed by various industries, including the advertising industry,[5] the government,[6] and the criminal legal system.[7]

Proponents of the use of FRT in law enforcement suggest that the use of facial recognition technologies may assist in crime reduction by helping identify individuals suspected of violating the law.[8] However, the use of AI and FRT is not immune from error. In a 2019 study sponsored by the United States Department of Commerce, the National Institute of Standards and Technology ("NIST") studied 189 software algorithms from 99 developers on the ability of an algorithm behind a FRT program to either match an individual's picture across two distinct platforms, or match an individual's picture

to any finding in a database.[9] The research took into consideration age, sex, and either race or country of birth, and assessed how each algorithm performed on images of people from various groups. Pertinently, the findings suggested a wide range of accuracy and found: (1) with one-to-one matching, there were higher rates of false positives for Asian and African American faces when compared to Caucasians; (2) the United States-developed algorithms demonstrated similarly high rates of false positives in one-to-one matching for Asians, African Americans, and Native groups; and (3) as to the one-to-many matching, there were higher rates of false positives for African American females.[10]

The breadth of the study must be confined by noting that there was a large amount of different algorithms being tested; accordingly, different algorithms performed differently. The findings do not seem to suggest an outright abandonment of such technology, but rather point to the discrepancies that must be accounted for – particularly when considering civil liberties.

Emphasizing the horrendous abuse and negligent reliance associated with FRT is the case of Mr. Robert Julian-Borchack Williams, a Black man who was arrested outside his home in Detroit after a detective used a FRT that incorrectly identified him.[11] Mr. Williams was arrested in front of his wife and children after a surveillance image from 2018 identified him as a perpetrator behind video recorded watch thefts.[12] Notably, a detective involved admitted, "the computer got it wrong."[13]

The NIST study and Mr. Williams' case support the contention that the use of AI and FRT must be scrutinized, yet it is unclear whether a universal standard or principle will be used to guide usage, or whether distinct governing bodies and courts will respond. Until now, the former appears too idealistic – yet it does appear that principles have been published that fall in line with adherence to a universal standard.[14] The latter has been gaining momentum. For example, legislative actions across several towns, cities, and states, including California and Massachusetts, have banned the government's use of face recognition.[15] Most recently, both chambers of the state legislature in Maine unanimously passed a bill rejecting biased surveillance technologies.[16] As patch work legislation has begun to gain momentum, federal legislation, titled the Facial Recognition and Biometric Technology Moratorium Act of 2020,[17] has been introduced to prevent the government from using facial recognition tools. The legislation would: (1) prohibit the use of facial recognition technology by federal entities; (2) prohibit the use of other biometric technologies; (3) condition federal funding to state and local entities based on their own moratoria of biometric technologies (which includes FRTs); (4) prohibit the use of federal money on biometric surveillance technologies; (5) prohibit the use of information collected via such technologies in violation of the act in judicial proceedings; (6) provide a right of action for people whose rights have been violated as a result of violating the act; and (7) allow states and localities to enact their own laws regarding the use of biometric technologies.[18]

The legislation passed in several states and the Facial Recognition and Biometric Technology legislation all recognize the pitfalls of relying on facial recognition devices and lay out concrete steps to remedy its potentially abusive use. Whether states begin implementing protective legislation against the use of facial recognition technology partly depends on educating the populace of its detrimental consequences, not just a focus on the potential "benefits."

Ivan A. Bohorquez is a 2L at Cardozo Law School interested in Privacy, Labor and Employment, Real Estate, and Tax. Prior, Ivan was a Civil Legal Advocate at the Bronx Defenders for three years after graduating from Manhattan College in 2016 with a bachelor's degree in International Relations (concentrating in Latin America & the Caribbean).

[1] Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. Davis L. R. 399, 404 (2017), https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Calo.pdf. ("There is no straightforward, consensus definition of artificial intelligence. AI is best understood as a set of techniques aimed at approximating some aspect of human or animal cognition using machines.").

[2] Katherine B. Forrest, *You Can Run But You Cannot Hide: AI Tools That Do More Than Recognize Your Face*, N.Y.L.J. (Mar. 29, 2021), https://www.law.com/newyorklawjournal/2021/03/29/you-can-run-but-you-cannot-hide-ai-tools-that-do-more-than-recognize-your-face/.
[3] Julian Hayes & Andrew Watson, *Police Use of Biometric Technology*, BCL Solicitors LLP (May 2021), https://www.bcl.com/police-use-of-biometric-technology-julian-hayes-and-andrew-watson-write-for-police-professional/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration.
[4] *Facial Recognition Technology*, Am. Civ. Liberties Union, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology (last visited Oct. 30, 2021).
[5] Kiely Kuligowski, *Facial Recognition Advertising: The New Way to Target Ads at Consumers,* Bus. News Daily (July 18, 2019), https://www.businessnewsdaily.com/15213-walgreens-facial-recognition.html.
[6] U.S. Gov't Accountability Off., **GAO-21-105309,** *Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees* (2021), https://www.gao.gov/products/gao-21-105309 ("In June 2021, GAO reported the results of its survey of 42 federal agencies that employ law enforcement officers about their use of facial recognition technology. Twenty reported owning systems with the technology or using systems owned by other entities, such as state, local, and non-government entities [].").
[7] *Id.*
[8] Lauren Feiner & Annie Palmer, *Rules Around Facial Recognition and Policing Remain Blurry*, CNBC (June 12, 2021, 9:30 AM), https://www.cnbc.com/2021/06/12/a-year-later-tech-companies-calls-to-regulate-facial-recognition-met-with-little-progress.html.
[9] *NIST Study Evaluates Effect of Race, Age, Sex on Face Recognition Software*, Nat'l. Inst. of Standards & Tech. (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.
[10]*Id.*
[11] Bobby Allyn, *'The Computer Got it Wrong': How Facial Recognition Led to False Arrest Of Black Man*, NPR (June 24, 2020, 8:00 AM), https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig.
[12] *Id.*
[13] *Id.*
[14] U.N. Conference on Trade and Development, *Technology and Innovation Report 2021*, at viii, U.N. Doc. UNCTAD/TIR/2020, https://unctad.org/system/files/official-document/tir2020_en.pdf (suggesting that technological innovation must be geared toward reducing inequalities, adopting newer technology while mastering preexisting ones, and mitigating risks – particularly by strengthening social protections).
[15] *The Fight to Stop Face Recognition Technology*, Am. Civ. Liberties Union, https://www.aclu.org/news/topic/stopping-face-recognition-surveillance/?redirect=facerecognition (last visited Oct. 30, 2021).
[16] Alison Beyea & Michael Kebede, *Maine's Facial Recognition Law Shows Bipartisan Support for Protecting Privacy*, Tech. Crunch (July 20, 2021, 3:14 PM), https://techcrunch.com/2021/07/20/maines-facial-recognition-law-shows-bipartisan-support-for-protecting-privacy/.
[17] Facial Recognition and Biometric Technology Moratorium Act of 2020, S.4084, 116th Cong. (2019-2020).
[18] Press Release, Senator Ed Markey, Senators Markey, Merkley Lead Colleagues on Legislation to Ban Government Use of Facial Recognition, other Biometric Technology (June 15, 2021), https://www.markey.senate.gov/news/press-releases/senators-markey-merkley-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology.