ACADEMIC SENATE
OF
THE CALIFORNIA STATE UNIVERSITY

AS-3469-21/FA (Rev)
January 21-22, 2021

CALL FOR A MORATORIUM ON ALGORITHMIC IMAGE RECOGNITION TECHNOLOGIES IN THE CSU OUTSIDE OF ACADEMIC RESEARCH

RESOLVED: That the ASCSU call for an immediate moratorium on any use of facial recognition technology in the CSU, with the exception of academic research; and be it further

RESOLVED: That the ASCSU call for an immediate moratorium on the use of any algorithmic image recognition technology with campus video surveillance; and be it further

RESOLVED: That the ASCSU call for the CSU to add prohibitions on the use of CSU image or biometric data in training image recognition algorithms to all future contracts with vendors receiving access to CSU image or biometric data; and be it further

RESOLVED: That the ASCSU distribute this resolution to the CSU Board of Trustees, CSU Chancellor, CSU campus Presidents, CSU campus Senate Chairs, CSU Chief Information Officers, CSU Provosts/Vice Presidents of Academic Affairs, California Faculty Association (CFA), California State Student Association (CSSA), and the CSU Emeritus and Retired Faculty & Staff Association (CSU-ERFSA).

RATIONALE: *This call has two grounds. First, machine learning algorithms reflect biases in the data they are trained on; racist inputs entail racist outputs. Mechanized discrimination will occur without careful engineering and auditing. The required technical, legal, policy, and regulatory infrastructure does not yet exist.*[1] *Second, many uses of algorithmic image analysis technologies threaten values at the core of the CSU's mission.*

Bias

A recent National Institute for Standards and Technology study of the top facial recognition algorithms reports high accuracy for white cisgendered males but high error rates for people of color, women, non-gender conforming persons, children, and the elderly.[2] *The Association for Computing Machinery concluded that "the technology*

---

[1] https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/
https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology

[2] *NIST Face Recognition Vendor Test (FRVT) Part 3: Demographic effects*
https://doi.org/10.6028/NIST.IR.8280 https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

too often produces results demonstrating clear bias based on ethnic, racial, gender, and other human characteristics recognizable by computer systems" and called for "an immediate suspension of the current and future private and governmental use of facial recognition technologies in all circumstances known or reasonably foreseeable to be prejudicial to established human and legal rights".[3] Similar concerns apply to other forms of algorithmic image analysis (e.g., attention detection, emotion identification, behavior analysis, gait analysis, and some object recognition systems). Research on the use of facial recognition in schools gives urgency to these concerns.[4]

Use with campus video surveillance

In the abstract, allowing campus police to identify individuals with restraining or stay-away orders is attractive. However, given facial recognition's disproportionately high error rates, the costs of erroneous identification will fall primarily upon for non-white, non-cisgendered, and female members of our campus communities.[5] Evaluating these risks requires considering the larger social context. Being contacted by an officer or having to wait for admittance by a security guard while others pass through may be a nuisance to a white cisgendered man. To a student or employee of color who has been disproportionately subjected to traffic stops[6], followed in stores by security guards[7], and otherwise treated with unjustified suspicion, it may be evidence that they are not welcome in the CSU.

Moreover, people overestimate the reliability of computerized systems.[8] Officers dispatched to an algorithmic (mis)identification will tend to arrive primed to deal

---

[3] https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf This also provides detailed guidance to policymakers.

[4] Some of this evidence is summarized in http://stpp.fordschool.umich.edu/technology-assessment. See also https://www.edweek.org/technology/facial-recognition-tech-in-schools-prompts-lawsuit-renewed-racial-bias-concerns/2020/06

[5] https://www.nbcnews.com/tech/security/facial-recognition-leads-first-wrongful-u-s-arrests-activists-say-n1231971

[6] See, inter alia., https://openpolicing.stanford.edu/findings, Pierson, E., Simoiu, C., Overgoor, J. et al. A large-scale analysis of racial disparities in police stops across the United States. Nat Hum Behav **4,** 736–745 (2020). https://doi.org/10.1038/s41562-020-0858-1, and Baumgartner, F., Epp, D., & Shoub, K. (2018). Suspect Citizens: What 20 Million Traffic Stops Tell Us About Policing and Race. Cambridge: Cambridge University Press. doi:10.1017/9781108553599.

[7] Cassi Pittman. "Shopping while Black": Black consumers' management of racial stigma and racial profiling in retail settings. Journal of Consumer Culture, 2017; 146954051771777 DOI: 10.1177/1469540517717777. Summarized in https://www.theguardian.com/commentisfree/2019/jun/24/shopping-while-black-yes-bias-against-black-customers-is-real

[8] Infamously, in 1988 the U.S.S. Vincennes shot down a civilian Iranian airliner which its Aegis system had mistakenly identified as a threat. Nearby warships had correctly identified the plane as civilian but yielded to the automated system's judgement. See Gray, C. H., 1997. "AI at War: The Aegis System in Combat," Directions and Implications of Advanced Computing, D. Schuler, (ed.), New York: Ablex, pp. 62–79.

with a potential threat. This may increase the chance of violence or tragedy. Such increased risk may be small; it is nonetheless unjustifiable.

Privacy implications beyond the university

Many companies, including those with objectionable missions[9], have an intense interest in obtaining data which accurately links images and identity. Thus, any image or biometric data which is shared from CSU systems may be used to violate a student's privacy far beyond their time at the CSU. Laws and norms lag technological progress. Thus the potential for harm from undreamt uses of such data is real, if hard to amortize.

Surveillance and the academic mission

The development of an authentic autonomous self and the free exploration of ideas are central to the CSU's mission. Surveillance, even when well-intentioned, prompts self-censorship and conformity to the perceived expectations of the surveillant.[10] That is antithetical to these aims.[11] Among many examples, students, especially those who are gender non-conforming, report altering their appearance and behavior after the adoption of video surveillance in U.K. schools.

Approved – March 18-19, 2021

[9] *The notorious Clearview AI (https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html) and purveyors of stalkware (https://stopstalkerware.org/) are merely the tip of this execrable iceberg.*

[10] *This was the point of Bentham's Panopticon. See https://www.ucl.ac.uk/bentham-project/who-was-jeremy-bentham/panopticon*

[11] *https://www.hrw.org/news/2019/06/21/facial-recognition-technology-us-schools-threatens-rights#. The Cameras in the Classroom report (http://stpp.fordschool.umich.edu/technology-assessment) gives a detailed survey of these issues.*