Third-Way Approaches to Facial Recognition Technology Regulation

Stuart N. Brotman
sbrotman@utk.edu

Abstract (500 Words)

The use of facial recognition systems powered by algorithms and software continues to raise controversy given their potential use by law enforcement and other government agencies. For over a decade, the Department of Commerce's National Institute for Standards and Technology (NIST) has evaluated facial recognition to identify and report gaps in its capabilities. Its most recent report in 2019 quantified the effect of age, race, and sex on facial recognition accuracy.

The greatest discrepancies that NIST measured were higher false-positive rates in women, African Americans, and particularly African American women. It noted, "False positives might present a security concern to the system owner, as they may allow access to impostors. False positives also might present privacy and civil rights and civil liberties concerns such as when matches result in additional questioning, surveillance, errors in benefit adjudication, or loss of liberty."

But on balance, NIST's finding of significant variances among different facial recognition algorithms that are used to match images against a large photo database is one that has often been overlooked. This is despite NISTR's explicit caveat that "users,

policymakers, and the public should not think of facial recognition as either always accurate or always error prone."

Major cities such as San Francisco and Boston already have imposed absolute bans on facial recognition technologies for all government agencies they control. In doing so, they largely have rejected NIST's methodological testing results.

A second regulatory option has been to enact a narrower ban on a time-limited basis (e.g., three years) so that facial recognition technologies can be more closely studied. This is the statewide approach that California took in its 2019 law that imposed a moratorium for using facial recognition with police body cameras.

The effect of both these approaches has reverberated in the private sector. Amazon established a one-year moratorium on selling facial recognition systems to police departments nationwide. IBM has halted facial recognition system sales to any government agencies. So did Microsoft, for as long as there is no federal law regulating facial recognition (but with reduced innovation, the less likely it will be for test results to demonstrate a much higher level of accuracy among different demographic groups).

This presentation will discuss some third-way thinking that would be beneficial. What meaningful guardrails can be put in place now, while leaving open the possibility that they be fortified in the future, as necessary?

For example, Utah’s recently-enacted facial recognition law places limitations on the way government entities may use image databases for facial recognition comparisons; and describes the process and requirements for conducting a facial recognition comparison, including a written request with a statement of the specific crime being investigated and a “factual narrative” establishing a “fair probability” the person is connected with the crime. A government employee can only comply with requests made for the purposes of investigating a felony, violent crime, or a threat to human life; or to identify a person who is dead, incapacitated, at-risk, or otherwise unable to provide an identity to law enforcement.