DAY ONE PROJECT

Regulating Facial Recognition Technology to Protect Civil Rights

David Lin

Summary

Facial recognition technology has become ubiquitous as a tool for law enforcement agencies, but its real efficacy and demographic equitability are still undetermined. In order to ensure accountability and transparency for this technology, the government needs to take two steps. First, the federal government should regulate what facial recognition software is permitted for federal acquisition based on algorithmic testing and guidelines by the National Institute of Standards and Technology (NIST). Second, in their annual "Data Mining Report to Congress", federal law enforcement agencies should include their facial recognition technology use and release statistics to ensure that the technology is effective and does not discriminate based on protected classes.

Challenge and Opportunity

Surveillance technology has the potential to be used effectively to combat crime. Several federal law enforcement agencies, including the F.B.I. and the Department of Homeland Security (DHS), utilize facial recognition technology to investigate suspects, identify illegal trafficking, and protect the country from terrorism. However, like most artificially intelligent technologies, it's nearly impossible to understand the mechanisms behind its decisions. This black box behavior can result in biased decision-making that escapes regulation.

In practice, false positive error rates of facial recognition algorithms used by law enforcement have reached as high as 98%.[1] While testing for bias, researchers found that major commercial facial recognition software was 33% worse at identifying women and people of color.[2] In one circumstance, an innocent black man was forced to spend the night in a detention center due to the misidentification of the state police department's facial recognition system.[3] The risks of civil rights violation are amplified in the United States where over 2,400 police agencies use the same untested facial recognition technology.[4] Nonetheless, the surging adoption by police agencies demonstrates how convenient and valuable the technology can be. This wide range of application and performance demands that facial recognition technology be effectively tested and evaluated before use.

---

[1] https://www.theregister.com/2018/05/15/met_police_slammed_inaccurate_facial_recognition/

[2] https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

[3] https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/

[4] https://www.theverge.com/2020/8/26/21402978/clearview-ai-ceo-interview-2400-police-agencies-facial-recognition

Currently, there is a patchwork of state and local legislation regulating facial recognition use. California, New Hampshire and Oregon prohibit law enforcement from using facial recognition in body cameras, while Illinois, Washington, and Texas restrict the collection and use of biometric data, including facial recognition technology.[5] These aggressive steps ban facial recognition technology rather than help AI developers and consumers be more innovative and responsible. A unifying set of legislation would benefit both parties by clarifying compliance guidelines for companies and giving confidence to law enforcement. Facial recognition regulation is an opportunity for the federal government to encourage the adoption of a new technology clearly and safely.

Plan of Action

First, facial recognition software needs to be tested for demographic differences before it's permitted for government use. NIST conducts reports on face recognition vendor tests (FRVT) to evaluate facial recognition software for accuracy variations and potential bias.[6] FRVT is an ongoing and open study of software submissions that tests across demographic groups defined by sex, age, and race or country of birth. Many facial recognition software companies have unacceptably opted not to submit their algorithms to FRVT. The federal government needs to mandate that all vendors submit their facial recognition software for NIST testing and pass evaluation before being allowed to sell their tools to federal agencies. Specifically, the Office of Federal Procurement Policy should work with a federal agency such as the DHS or DoD to amend the Federal Acquisition Regulation (FAR) with these procurement requirements.

Second, the use of facial recognition software by federal law enforcement needs to be more transparent. The Federal Agency Data Mining Reporting Act of 2007 requires federal agencies to report annually to Congress on any activity using data mining to identify criminal activity.[7] By law, the report should also include a discussion of the procedures to protect individual privacy and guard against harmful consequences. However, in the annual DHS Data Mining Report, facial recognition technology use is missing.[8] Facial recognition technology use should be included in these reports, because it fits the definition of "data mining" and has the potential to discriminate against individuals and violate civil rights. The report should include the facial recognition software, its vendor, the purpose of use, and how the data is protected. To further contribute to the discussion, federal agencies should be required to provide statistics on the efficacy of their facial recognition software in real usage. The statistics should be similar to the demographic differences presented in the FRVT, namely false positive and false negative rates across protected classes such as sex, race, and age.

These two recommendations can be summarized as follows:

1. Accountable algorithmic testing and approval: The Office of Federal Procurement Policy should amend the FAR to mandate that any facial recognition software seeking federal

[5] https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/
[6] https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing
[7] https://www.congress.gov/bill/110th-congress/senate-bill/236
[8] https://www.dhs.gov/publication/dhs-data-mining-reports

acquisition must submit their software for NIST vendor testing and gain approval before consideration. The Office of Science and Technology Policy and the Department of Commerce should continue to drive NIST to publish its FRVT results publicly and develop policy guidelines for an acceptable standard.

2. Transparent facial recognition software use: In compliance with the Federal Agency Data Mining Reporting Act of 2007, the use of facial recognition technology and any demographic differences should be reported in federal agencies' annual data mining reports. If necessary, the OSTP should send letters to agencies in noncompliance.

Frequently Asked Questions

Why should an independent evaluator such as NIST test facial recognition software instead of the AI developers?

An independent evaluator within the US Government ensures that the algorithmic testing is accurate, valid, and standardized across all facial recognition algorithms and federal agency usage. NIST has demonstrated its ability to conduct an open submission study to evaluate error rates for nearly 200 face recognition algorithms from nearly 100 developers. Their testing technique crucially does not provide training data to software and prohibit adapting to any data that they pass to the algorithms.[9] Furthermore, they use a variety of large datasets collected for authorized travel, immigration, or law enforcement processes that represent operational reality. Ultimately, it is also the government's responsibility to prevent the violation of civil rights.

What are the precedents to the proposed FAR amendment regulating facial recognition software?

FAR Part 39 regulates the acquisition of information technology and includes several clauses such as part 39.101 (c) which directly regulates information security policies and requirements according to NIST guidelines.[10] Federal agencies have the ability to propose amendments to the FAR and have even recently passed updates on FAR Part 39.[11] Through other mechanisms of federal law, the Federal Information Security Modernization Act of 2014 was passed as a response to cyber attacks on the federal government and directs the Secretary of Homeland Security to consider guidance developed by NIST.[12]

How should facial recognition software be deemed acceptable for government use?

As described in the FRVT, guidelines for acceptable facial recognition software should assess the algorithm's false positive and false negative demographic differentials. The most accurate algorithms produce fewer and more consistent errors across differentials such as race. They propose a threshold on false match rate that requires algorithms do not vary much over any demographics, with specific exceptions based on threat, risk, and cost.

Why is facial recognition use not included in the annual data mining report to Congress?

It's not clear why the use of facial recognition technology is not included in the DHS annual data mining reports. From a privacy impact perspective, recent effort by Homeland Security Investigations (HSI) assessed ICE's use of personally identifiable information (PII) in facial

---

[9] https://www.nist.gov/system/files/documents/2019/04/22/frvt_frequently_asked_questions.pdf
[10] https://www.acquisition.gov/far/part-39#FAR_39_101
[11] https://www.federalregister.gov/documents/2020/03/31/2020-05867/federal-acquisition-regulation-section-508-based-standards-in-information-and-communication
[12] https://www.congress.gov/bill/113th-congress/senate-bill/2521

recognition services (FRS).[13] From the perspective of efficacy and the risk of demographic differential, the DHS needs the same commitment to transparency.

[13] https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf