Massachusetts Pirate Party Facial Recognition Commission Testimony

James O'Keefe <jokeefe@jamesokeefe.org>

Wed 8/4/2021 8:38 PM

To: Manning, Jacqueline O. (HOU) <Jacqueline.O.Manning@mahouse.gov>

You don't often get email from jokeefe@jamesokeefe.org. Learn why this is important

Dear Ms. Manning,

Included below is the testimony I presented last Friday before the Facial Recognition Commission. Thank you for forwarding it on to the commissioners.

peace,

James O'Keefe

Captain, Massachusetts Pirate Party / masspirates.org
w: jamesokeefe.org e: jokeefe@jamesokeefe.org m: 617-447-0210
GPG key fingerprint: 9F7C 6B6C EA9F E2D3 6489 B826 A8B0 F73D AAFF 1FEC

Encrypt your communications. See https://prism-break.org/ for a list of tools you can use.

Thank you Chairs Eldridge and Day and the Facial Recognition Commission for the opportunity to be heard on this issue. My name is James O’Keefe, I live in Somerville, and, for thirty one years, I have tested computer software for a living. I speak to you as Chair of the Massachusetts Pirate Party.

The Pirate Party strongly urges you to ban state and local government use of dangerous, racially-biased facial recognition software. It will be used to criminalize innocent civilians, and is inherently biased against people with darker skin. (1) Such surveillance software is racist, period.

Facial recognition software relies on machine learning systems to find matches and make connections between the faces given to them and the faces they analyzed in their training data. When that training data is biased, as it often is, then the results will be biased. As we say in the software industry: Garbage In Garbage Out. Even if the percentage of false positives is low, they add up to real people wrongly accused when police perform millions of searches.

We see this problem most starkly in criminal risk assessment algorithms (2) where for how long a person is sentenced depends, in part, on a digital black box. Police in Louisiana (3) and elsewhere, use racially-biased predictive policing software to determine where to allocate police. The working of such black boxes is protected by Intellectual Privilege laws that neither the defense nor prosecution has the right to analyze to understand how it made its decision. Facial recognition software is another such black box that can lead to innocent people being misidentified, arrested (4) and, potentially, shot or killed by a police officer.

Just this week, ShotSpotter was embroiled in a scandal after it was revealed that they alter records and falsify gunshot reports at the behest of police departments seeking to brutalize their own citizens. (5) (6) There is no reason that the findings of facial recognition technology could not be altered to provide a match where there wasn't one. It would be a black box and too many will claim "the algorithm is never wrong". Such technology is unproven, unreliable, and ineffective and must not be used.

Increasingly, state and local governments roll out yet more surveillance cameras. (7) (8) Amazon and other vendors use fear, of packages being stolen, of attackers, and of our neighbors, to promote home use of their surveillance cameras. Amazon keeps its surveillance recordings, makes them easily available to police and encourages police to help them sell such cameras. Increasingly, government and corporations are networking these cameras together.

When combined with facial recognition software, such a network could be capable of identifying where people go and who they meet. Having a permanent record of our comings and goings is not something a free society does, even if access to that record is behind a warrant requirement. People will misuse such a surveillance network. It could be police claiming exigent circumstances to do a search that someone paid them to do or to benefit their white supremacist allies. (9) It could be an employee of the outsourced surveillance service engaging in stalking or LoveInt, as we learned from the Snowden revelations. (10) It could certainly be malicious hackers finding a backdoor into the surveillance network. (11) (12) We know it can happen, because all of these cases have already happened.

If you build a surveillance network, it will be misused. Banning state and local government use of facial recognition software is one important means to guarantee our freedom to go where we choose without fear of constant surveillance.

The ability of the government and private agencies to stockpile every detail of a person's day is an unfathomable violation of our right to privacy. It is now trivial for businesses to track every step a person takes on the Internet through their entire day. Everything you own with an Internet connection is monitoring everything you do. The least consideration we deserve is to not have our government benefit from this panopticon at our expense.

You have the power to prevent racially-biased, discriminatory surveillance technology from being used to track ordinary people as we go about our lives, including at schools, outside healthcare facilities, and at public demonstrations.

We respectfully urge you to bring this harmful technology under democratic control and to ban its use by state and local governments.

Thank you for allowing me to testify. I will email our testimony with references to you as requested.

1. https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/
2. https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai/
3. https://atlasofsurveillance.org/es/a/aos5393-benton-county-sheriff-s-office-predictive-policing
4. https://arstechnica.com/tech-policy/2020/06/police-arrested-wrong-man-based-on-facial-recognition-fail-aclu-says/
5. https://www.vice.com/en/article/qj8xbq/police-are-telling-shotspotter-to-alter-evidence-from-gunshot-detecting-ai
6. https://www.techdirt.com/articles/20210726/17334947254/shotspotter-again-spotted-altering-shots-spots-to-better-serve-police-narratives.shtml
7. https://www.wcvb.com/article/lawrence-massachusetts-invests-dollar300000-in-new-citywide-surveillance-system/27229266
8. https://cctv.masspirates.org
9. https://www.cnn.com/2021/06/03/politics/supreme-court-cybercrime-law-case/index.html
10. https://www.berkshireeagle.com/crime/lanesborough-officer-fired-over-improper-use-of-criminal-records-database/article_68f289a8-f3b4-11eb-b060-7f33ddf5645d.html
11. https://www.bbc.com/news/technology-51658111
12. https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats