[External]: Supplemental Written Testimony for Commission on Facial Recognition

Julie Bernstein <julie.bernstein.borhani@gmail.com>

Sun 8/1/2021 11:34 PM

To: Williams, Dianna (HOU) <Dianna.Williams@mahouse.gov>

You don't often get email from julie.bernstein.borhani@gmail.com. Learn why this is important

Supplementary Written Evidence for the Commission on Facial Recognition

Dear Chairman Eldridge, Representative Day, and Committee Members,

After listening to the July 30, 2021 commission hearing, I am concerned by the discrepancies between information provided by Clearview AI experts and people who have been studying facial recognition technology. I wanted to provide additional information on several areas of discrepancy, including the lower accuracy in matching women and people of color, the impact of image quality on matching, and the role of systems settings. I also wanted to provide additional documentation for other testimony delivered at the meeting.

Jake Lapperuque, who testified to you, provided written testimony to the House Judiciary Committee Congressional hearing on Crime, Terrorism and National Security. He wrote that: “Studies by the National Institute of Standards and Technology; the Massachusetts Institute of Technology, Microsoft, and AI Now Institute researchers; the American Civil Liberties Union; and an FBI expert all concluded that face recognition systems misidentify women and people of color more frequently. Most recently, the National Institute of Standards and Technology found that some systems were 100 times more likely to misidentify people of East Asian and African descent than white people.”

On Friday, I pointed out that even under the highly controlled conditions of photographing applicants and using Rekognition software at the RMV, there is still an almost 20% error rate in confirming identifications. Lapperuque elaborated:

“Image quality can also significantly impact accuracy of matches. Sets of reference images — databases containing previously identified faces—in face recognition systems are typically high-resolution photos of a person directly facing a camera at close range, such as for a mug shot photo. But probe images—from which law enforcement seeks to identify individuals—are derived from a wide range of situations, which creates the potential for low image quality and erroneous results.”

“Bad lighting, indirect angles, distance, poor camera quality, and low image resolution all make misidentifications more likely. These poor image conditions are more common when photos and videos are taken in public, such as with a CCTV camera. But these low-quality images often serve as probe images for face recognition scans, without due consideration for their diminished utility.”

“Even when using more effective software and higher quality images, system settings can make face recognition matches prone to misidentification. For example, the way law enforcement sets confidence thresholds…can undermine reliability of results.”

A “Comprehensive Review on Face Recognition Methods and Factors Affecting Facial Recognition”, conducted by two researchers in 2020, affirms Lapperuque’s testimony.

Lapperuque also documented the misleading and inconsistent instructions provided to law enforcement by top developers of facial recognition software. 'An FAQ the company provided to law enforcement claims, "a photo should work even if the suspect grows a beard, wears glasses, or appears in bad lighting," then adds, "you will almost never get a false positive. You will either get a correct match or no result."[11] This is a false and incredibly dangerous claim. If law enforcement takes it as true, they may be inclined to put immense weight on *any* face recognition match they receive through Clearview AI software.'

'And at the same time Amazon publicly stated law enforcement clients should set the company's face recognition software to only return matches based on a 99% confidence threshold, it was advising at least one department to deploy a top-five-match system that would always return results, even if possible matches were well below that 99% threshold.[12] This augments the risk that misidentifications will be presented to law enforcement as matches.'

After a massive data breach, BuzzFeed reviewed data and reached out to law enforcement agencies disclosed to be using Clearview AI's database. It learned that "officials at a number of those places initially had no idea their employees were using the software or denied ever trying the facial recognition tool. Some of those people later admitted that Clearview accounts did exist within their organizations after follow-up questions from BuzzFeed News led them to query their workers."

Furthermore, Clearview AI recently attempted to dodge a potential class-action lawsuit filed against it in Illinois for scraping of publicly available photos, location data, and other information from a variety of websites and social media platforms in violation of the state's law, which requires companies to obtain permission from people before harvesting and selling access to this data. The Seventh Circuit rejected Clearview's argument.

Ira Grant and Nathan Tamulis of CPCS discussed the importance of the proper use of any forensic technique. This has been driven home by the recent class action lawsuit accusing the Massachusetts Department of Corrections of using a notoriously unreliable field test to detect contraband drugs as well as the fact that the William A. Hinton State Laboratory Institute improperly processed drug tests for nine years.

The importance of limiting the use of facial recognition technology to when it is absolutely necessary cannot be overstated especially as the state deploys CCTVs and other technology such as red light cameras whose image quality is unreliable. The Springfield Real-Time Analysis Center has deployed 300 cameras in Springfield including the recently added 250 near Union Station. Recently, Acting Mayor Kim Janey paused an RFP for 1000 surveillance cameras in Metro Boston in response to an outcry by civil rights group. Furthermore, law enforcement has access to footage from Amazon Ring cameras and surveillance drones n neighborhoods throughout Massachusetts.

As Lappereque wrote "The simple fact is, unreliable investigative tools and techniques—even if just used for leads and taken alongside other potentially exonerating evidence—can lead to the arrest of innocent individuals, a problem we have seen again and again with flawed technologies ranging from outdated forensics[14] to unreliable polygraph tests.[15] If standard law enforcement policy was to base investigations on smudged fingerprints or contaminated DNA samples, it would be of little comfort that this tainted evidence was just used for leads."

It is also imperative to ensure that facial recognition is not used to identify protesters as has been documented to have occurred in California, Florida, Illinois, Maryland, New Mexico, Pennsylvania.

- https://www.vice.com/en/article/3aqpmj/six-federal-agencies-used-facial-recognition-on-george-floyd-protestors

- https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sll5uuaqfbeba32rndlv3xwxi-htmlstory.html.
- https://www.citizensforethics.org/reports-investigations/crew-investigations/emails-show-deas-covert-surveillance-of-racial-justice-protesters-in-philadelphia-chicago-albuquerque/?link_id=1&can_id=307f3beb18b704c1c016d36c46d3a2f6&source=email-transparench
- https://www.eff.org/deeplinks/2020/07/san-francisco-police-accessed-business-district-camera-network-spy-protestorsand https://www.eff.org/cases/williams-v-san-francisco
- https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests

Thank you for considering this material.

Julie Bernstein

--
Julie Bernstein
Please reply to: julie.bernstein@alum.mit.edu