Testimony of Jake Laperruque, Senior Counsel,
The Constitution Project at the Project On Government Oversight,
before the House Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies
March 13, 2020

In Support of Limits on Funding for Face Recognition Surveillance

Thank you for the opportunity to submit testimony. In its funding of the Department of Justice, we believe the Subcommittee on Commerce, Justice, Science, and Related Agencies should restrict funding for the purchase and use of face recognition surveillance by law enforcement agencies.

The Project On Government Oversight (POGO) is a nonpartisan independent watchdog that investigates and exposes waste, corruption, abuse of power, and when the government fails to serve the public or silences those who report wrongdoing. We champion reforms to achieve a more effective, ethical, and accountable federal government that safeguards constitutional principles. The Constitution Project at POGO strives to protect individuals from improper and overbroad surveillance, including unchecked face recognition surveillance.

Face recognition poses immense risks to privacy, civil liberties, and public safety. Nonetheless, it is being rapidly deployed: Half of all American adults are enrolled in a law enforcement face recognition database, often without their knowledge.\(^1\) Last year, we convened a task force of expert stakeholders including academics, tech experts, civil rights and civil liberties advocates, and law enforcement officials to examine the impact of face recognition and how lawmakers should respond. This group concluded that Congress should place strong limits on face recognition technology.\(^2\)

Congress should continue to examine the implications of this technology, and enact restrictions to prevent harms and protect constitutional rights. While Congress, as well as state and local policymakers, works to develop proper rules and limits, it should not allow federal funds to be used indiscriminately to build law enforcement face recognition systems.

**Face recognition creates serious risks, especially of misidentification**

Misidentifications are one of the most prevalent and troubling risks face recognition creates. While many advocates for surveillance systems invoke the supposed tradeoff between liberty and security when discussing surveillance, face recognition endangers both public safety and civil liberties by implicating improperly identified individuals in investigations or police action.

Face recognition’s tendency to misidentify women and people of color at a higher rate is an acute concern. Studies by the National Institute of Standards and Technology (NIST); MIT, Microsoft, and AI Now Institute researchers; the American Civil Liberties Union; and an FBI expert all

---

\(^1\) See Clare Garvie et al., Georgetown Law Center on Privacy and Technology, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (October 18, 2016), Sec. I. [https://www.perpetuallineup.org](https://www.perpetuallineup.org)

concluded that face recognition systems misidentify women and people of color more frequently. Most recently, NIST found that some systems were 100 times more likely to misidentify people of East Asian and African descent than white people. Congress should not fund unchecked use of face recognition systems while this racial and gender disparity exists.

The general accuracy of face recognition is also subject to technical limitations. This technology centers on comparing features in photographs, therefore image quality is essential to obtaining reliable results. Specifically, face recognition compares “probe images,” from which law enforcement seeks to identify individuals, to “reference images,” which contain previously-identified faces. Reference images are typically high-resolution photos of a person directly facing a camera from a close distance, such as for a mug shot photo. But probe images are derived from a huge range of situations, creating potential for low image quality and erroneous results.

Bad lighting, indirect angles, excess distance, poor camera quality, and low image resolution all will undermine reliability of matches. These poor image conditions are much more likely to occur when photos and videos are taken in public, such as with a CCTV camera. And these low-quality images taken in public often serve as face recognition probe images used in investigations.

Without regulations, law enforcement may employ irresponsible techniques that also exacerbate the risks of misidentification. Some agencies have engaged in the highly questionable practices of scanning police sketches of suspects in lieu of actual probe images of suspects or using computer editing to artificially fill in pieces of a face that were not caught on camera. Asking systems to analyze manufactured data will produce unreliable results. Computer programs do not “see” faces the way humans do, and artificially adding data that will be part of a face recognition scan is the equivalent to drawing in lines on a smudged fingerprint.

The reliability of face recognition also varies based upon the confidence threshold of potential matches. Confidence thresholds are a metric used to compare which proposed matches within a system are more likely to be accurate. The lower the confidence threshold, the more likely the


4 Grother et al., Face Recognition Vendor Test [see note 3].

5 Task Force on Facial Recognition Surveillance, Facing the Future of Surveillance [see note 2]; Garvie et al., The Perpetual Line-Up, Sec. V [see note 1].

6 Garvie et al., The Perpetual Line-Up, Sec. III [see note 1]
7 Garvie et al., The Perpetual Line-Up, Sec. V [see note 1]
“match” is actually a false positive. So, if law enforcement set face recognition systems to always return potential matches—no matter how low confidence the threshold—they will receive untrustworthy data. Yet some law enforcement entities do just that, including the FBI. Law enforcement officials will sometimes dismiss misidentification risks by claiming face recognition is just used for leads. But using untrustworthy information as the foundation of an investigation is dangerous, regardless of whether that information is introduced in court. If law enforcement guidelines recommended basing investigations on contaminated DNA samples, it would be of little comfort that this tainted evidence was “just used for leads.” Simply being targeted in an investigation can be disturbing and disruptive and bring the prospect of being subject to harmful police action even if charges or a conviction never follow. And an individual could still be charged in part based on how a face recognition match impacts the early direction of an investigation. A technology with significant, known, and as-yet-unmitigated flaws should not be relied upon for investigative work.

One type of face recognition is especially likely to result in misidentifications: real-time scanning of crowds. Real-time face recognition systems do not attempt to identify a single probe image. Rather, these systems scan every person within a crowd that passes by the frame of a camera, and provide an alert if anyone scanned is identified as a match against a preexisting watchlist.

Real-time face recognition takes all the risks of using face recognition in an open-world setting—bad lighting, poor angles, excessive and inconsistent distances—and multiplies them by conducting scans of groups of individuals. Early results have shown the harm this could cause. In pilot programs in the United Kingdom, South Wales police had a 91% error rate and London Metropolitan Police had a 98% error rate. And finally, the problems of real-time face recognition would be magnified if it is incorporated into police body cameras, with devices scanning crowds while officers are on patrol. This would produce in-field alerts based on highly unreliable matches, and force officers to make hasty decisions in response. America’s largest producer of body cameras, Axon, initially sought to incorporate face recognition into body cameras, but data on misidentifications led the company to publicly acknowledge that this would cause more harm than good and reverse course.

12 For example, during a recent Congressional hearing FBI Director Christopher Wray responded to inquiries on face recognition by stating “We use it for lead value. We don’t use facial recognition as a basis to arrest or convict.” House Judiciary Committee. Oversight of the Federal Bureau of Investigations: Hearing before the House Judiciary Committee, 116th Cong. (February 5, 2020). https://www.c-span.org/video/?468923-1/fbi-director-wray-testifies-overight-hearing&start=14789
However, other vendors are recklessly charging ahead in efforts to build face recognition into police body cameras.\(^{15}\)

**Congress should not support adoption of unchecked face recognition**

If face recognition is deployed by law enforcement, it is vital that strong rules are in place to prevent improper use and reduce the risk of misidentifications. Accuracy standards, training, procedural limits, audits, and disclosure requirements must exist to account for racial and gender disparity in misidentifications.\(^{16}\) Rules should ensure that investigations are not premised on unreliable matches built from low-quality probe images, or matches that possess a low confidence threshold. Junk science techniques such as scanning sketches, rather than actual photos, must be prohibited.

Achieving this will require public debate, examination of risks, and careful development of policy at the local, state, and federal level. As this is occurring, Congress must not accelerate the implementation of face recognition surveillance, spurring on careless use of the technology. Yet permitting federal grant funding to be used for the purchase and development of face recognition systems does just that.

**Recommendations:**

*Congress should prohibit state and local law enforcement from using appropriated funds for the purchase or operation of face recognition technology, including prohibiting use for the purchase or operation of body cameras that incorporate real-time face recognition.*

This measure is a reasonable first step to ensure that Congress does not unwittingly put its thumb on the scale and encourage law enforcement to recklessly expand face recognition surveillance without responsible rules.

Federal funds are also a major driver of adoption of police body cameras. While dozens of law enforcement entities use federal grant funding to pay for their body camera programs, only a handful place restrictions on the use of face recognition.\(^{17}\) If Congress continues to fund body camera programs, it must prevent them from morphing into an inaccurate surveillance tool.

*Congress should prohibit the use of appropriated funds for the purchase or operation of real-time face recognition technology by federal, state, and local law enforcement.*

Given that real-time face recognition is far more likely to produce misidentifications than genuine matches, its implementation should be kept on hold. If federal law enforcement entities wish to deploy real-time face recognition, they should not be able to do so without proving to Congress that the misidentification risks it poses have dramatically decreased.


\(^{16}\) Task Force on Facial Recognition Surveillance, *Facing the Future of Surveillance* [see note 2].