PROJECT ON GOVERNMENT OVERSIGHT

Thank you for the opportunity to submit a statement to the House Judiciary Committee Subcommittee on Crime, Terrorism, and Homeland Security regarding its hearing, "Facial Recognition Technology: Examining Its Use by Law Enforcement."

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. The Constitution Project at POGO strives to protect constitutional rights and principles, including guarding against improper and overbroad surveillance such as unchecked face recognition. In 2019, the Constitution Project 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 surveillance.[1] It concluded that any law enforcement use of face recognition should be subject to strong limits, and provided a set of policy recommendations.

Face recognition surveillance poses two distinct but equally important dangers: It can be immensely harmful when it does not function properly, and it can also be immensely harmful when it does. Face recognition misidentifications can lead to improper targeting, needless police action, and wrongful arrests. Innocent individuals could face jail time or be pressured to take a plea deal, all without knowing charges were based upon a poor face recognition match. But making face recognition more accurate will not alleviate the danger it poses to civil rights and civil liberties. Absent strong limits, face recognition opens the doors to pervasive surveillance and abuse, and it allows the government to warp discretion into a tool for malicious and selective targeting.

Correcting Common Misconceptions about Face Recognition Surveillance

As lawmakers consider what safeguards to place on face recognition surveillance, it is important to recognize common misconceptions about law enforcement use of the technology and the damage it causes. This section corrects four key misconceptions about face recognition and explains why the realities about it require urgent action by Congress.

Face recognition does not work in a monolithic way; in reality, its ability to function—and the limits of its functionality—are highly situational.

Face recognition is frequently portrayed in crime dramas—and more disturbingly, by vendors selling the technology—as a technology that can be applied to photos in any situation, with consistently accurate results. In reality, face recognition's ability to deliver reliable matches depends upon a range of factors.

[1] Task Force on Facial Recognition Surveillance, Project On Government Oversight, *Facing the Future of Surveillance* (March 4, 2019), https://www.pogo.org/report/2019/03/facing-thee -future-of-surveillance/.

The quality of face recognition algorithms can vary significantly. Notably, many algorithms misidentify women and people of color at a higher rate than other people. 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.[2] 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.[3] Failure to recognize the significance of this problem—and account for it in selection and review of software, training, and auditing—will undermine investigations and seriously harm civil rights.

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.[4] 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.[5]

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—a metric used to compare which proposed matches within a system are more likely to be accurate—can undermine reliability of results. The lower the confidence threshold, the more likely the "match" is actually a false positive. So, if law enforcement

---

[2] Patrick Grother, Mei Ngan, Kayee Hanaoka, National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 (December 19, 2019), 2, https://doi.org/10.6028/NIST.IR.8280; Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research*, vol. 81 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Joy Buolamwini and Inioluwa Deborah Raji, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products," *AIES '19: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* (2019), https://www.media.mit.edu/publications/actionable-auditing-investigating-the-impact-of-publicly-naming-biased-performance-results-of-commercial-ai-products/; Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots," American Civil Liberties Union, July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognitionfalsely-matched-28; Brendan Klare et al., "Face Recognition Performance: Role of Demographic Information," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6 (December 2012), http://openbiometrics.org/publications/klare2012demographics.pdf.

[3] Grother, Ngan, Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, 2 [see note 2].

[4] Task Force on Facial Recognition Surveillance, Facing the Future of Surveillance, Sec. II [see note 1].

[5] "CCTV feeds facial recognition systems for law enforcement," *Biometric Technology Today*, vol. 2015, no. 4 (April 2015): 3, https://www.sciencedirect.com/science/article/abs/pii/S0969476515300539.

entities set face recognition systems to always return potential matches—no matter how low confidence the threshold—they will receive untrustworthy data. Troublingly, some law enforcement entities do just that.[6]

For example, one police department designed its face recognition system so that for field use it "dropped the search-confidence percentages and designed the system to return five results, every time," meaning results would come back as top possible matches even if they were unreliable, introducing the likelihood that officers would receive untrustworthy information amid encounters with individuals.[7]

Disturbingly, the vendors that sell face recognition software often exaggerate how broadly the technology functions, thereby encouraging irresponsible law enforcement use that will lead to misidentifications.

One major vendor boasts in marketing materials that "facial recognition gives officers the power to instantly identify suspects. … Officers can simply use their mobile phones to snap a photograph of a suspect from a safe distance. If that individual is in their database, it can then positively identify that person in seconds with a high degree of accuracy."[8] This is an inflated characterization given the limits that lighting and angle would impose in such a situation. Other vendors claim face recognition would offer a positive identification—rather than provide a set of possible but uncertain matches—but that claim is at odds with how most responsibly designed face recognition systems operate in practice.[9]

Clearview AI's pitches to law enforcement—obtained through public records requests by *BuzzFeed*—are shockingly boastful. The company claims to have "the most accurate facial identification software worldwide" and to consistently produce accurate results "in less than five seconds." The company even goes so far as to tell law enforcement that using its software will make them "realize you were the crazy one" for not believing face recognition would perform

---

[6] Jim Trainum, "Facial Recognition Surveillance Doesn't Necessarily Make You Safer," Project On Government Oversight, July 22, 2019, https://www.pogo.org/analysis/2019/07/facial-recognition-surveillance-doesnt-necessarily-make-you-safer/; According to then-FBI Deputy Assistant Director Kimberly Del Greco, its system is set up so that it "returns a gallery of 'candidate' photos [reference photos] of 2-50 individuals (the default is 20)." *Facial Recognition Technology (Part II): Ensuring Transparency in Government Use*: *Hearing before the House Committee on Oversight*, 116th Cong. (June 4, 2019) (statement by Kimberly Del Greco, Deputy Assistant Director, FBI Criminal Justice Information Services Division), https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use.

[7] Drew Harwell, "Oregon became a testing ground for Amazon's facial recognition policing. But what if Rekognition gets it wrong?" *Washington Post*, April 30, 2019, https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/.

[8] "For Law Enforcement, The Cost of a False Arrest is More Than Just Bad Press," FaceFirst, October 20, 2017, https://www.facefirst.com/blog/law-enforcement-cost-false-arrest-far-just-bad-press/.

[9] Cognitec states that its software can be used for "fast identification of suspects and efficient crime investigations." Cognitec, "Applications: Law enforcement," https://www.cognitec.com/law-enforcement.html (accessed July 9, 2021); As of August 2019, DataWorks Plus promised law enforcement "reliable identification through facial recognition technology" and that its software "uses facial recognition technology to positively match photos of an individual by identifying key characteristics of the facial image" with capabilities such as "discovering a person's identity during investigations." DataWorks Plus, "Facial Recognition Technology & Case Management," http://web.archive.org/web/20190811221236/http://www.dataworksplus.com:80/faceplus.html.

the same as it does in outlandish TV depictions like "NCIS, CSI, Blue Bloods."[10] 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.

In the absence of safeguards to address this range of misidentification risks, face recognition will continue to provoke errors, harm innocent individuals, and exacerbate inequalities in how different communities are policed.

Face recognition is not a risk-free tool if law enforcement just uses it for leads; face recognition still can, and does, mislead law enforcement.

It is important to resist the temptation to shrug off the risks of misidentification based on law enforcement claims that face recognition is just used for leads, rather than as the backbone of a prosecution.[13] Using untrustworthy information as the foundation of investigations is always dangerous, regardless of whether that information is introduced in court.

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

[10] Jake Laperruque, "Face Recognition Is Far from the Sci-Fi Super-Tool Its Sellers Claim," Project On Government Oversight, April 16, 2021, https://www.pogo.org/analysis/2021/04/face-recognition-is-far-from-the-sci-fi-super-tool-its-sellers-claim/.
[11] "Clearview FAQ," Clearview, https://s3.documentcloud.org/documents/20531944/north-miami-fl-clearview_faq.pdf.
[12] Jake Laperruque, "About-Face: Examining Amazon's Shifting Story on Facial Recognition Accuracy," Project On Government Oversight, April 10, 2019, https://www.pogo.org/analysis/2019/04/about-face-examining-amazon-shifting-story-on-facial-recognition-accuracy.
[13] For example, during a 2020 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 someone." *Oversight of the Federal Bureau of Investigation: Hearing before the House Judiciary Committee*, 116th Cong. (February 5, 2020), 4:53:28, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=2780.

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.

There are already at least three documented cases in which individuals have been improperly arrested based on face recognition misidentifications.[16] It is unlikely that Robert Williams, Michael Oliver, and Nijeer Parks are the only individuals who have been wrongfully arrested because of such errors. According to a 2020 *New York Times* investigation of face recognition systems in Florida, "Although officials said investigators could not rely on face recognition results to make an arrest, documents suggested that on occasion officers gathered no other evidence."[17] Because face recognition is frequently hidden from defendants,[18] there are likely more instances where face recognition led to the arrest of innocent individuals—some of whom may have felt pressured to accept a plea bargain—that we are unaware of.

Individuals could also be charged in part based on how a match produced by a face recognition system affects the direction of an investigation early on, especially when having a match promotes confirmation bias or sloppy follow-up. For example, in one incident, New York City Police Department officers allegedly took a single possible face recognition match, and then texted a witness, "Is this the guy…?" along with the photo, rather than following proper procedure to use a photo array.[19]

Even without leading to improper arrests, face recognition misidentifications can cause serious harm. Being targeted in an investigation can also be disruptive and potentially traumatic, and can endanger individuals even if charges or a conviction never follow.

By holding up the notion that *face recognition is just used for leads* as a virtue, law enforcement actually places this technology in a limbo where its "results still can play a significant role in investigations, though, without the judicial scrutiny applied to more

---

[14] President's Council of Advisors on Science and Technology, *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods* (September 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

[15] Joseph Stromberg, "Lie detectors: Why they don't work, and why police use them anyway," *Vox*, December 15, 2014, https://www.vox.com/2014/8/14/5999119/polygraphs-lie-detectors-do-they-work.

[16] Kashmir Hill, "Wrongfully Accused By An Algorithm," *New York Times*, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; K. Holt, "Facial recognition linked to a second wrongful arrest by Detroit police," *Engadget*, July 10, 2020, https://www.engadget.com/facial-recognition-false-match-wrongful-arrest-224053761.html; Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *New York Times*, December 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[17] Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short," *New York Times*, January 12, 2020, https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

[18] In some jurisdictions, law enforcement uses facial recognition thousands of times per month, but defendants almost never receive notice of its use in investigations. Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short" [see note 17].

[19] Clare Garvie, "Garbage In, Garbage Out: Face Recognition on Flawed Data," Georgetown Law Center on Privacy & Technology, May 16, 2019, https://www.flawedfacedata.com/.

proven forensic technologies."[20] It is vital that better safeguards be put into place to prevent improper reliance on this technology, and to ensure that defendants are not deprived of their right to review potentially exculpatory evidence.

The risk that face recognition surveillance will be abused is not hypothetical; the technology has already been abused to target and hamper First Amendment-protected activities.

Face recognition has already been misused to identify peaceful protesters and to facilitate selective prosecution against protesters.

According to a *South Florida Sun Sentinel* investigation, in 2020, law enforcement repeatedly used face recognition to identify and catalog peaceful protesters. Fort Lauderdale police ran numerous face recognition searches to identify people who might be a "possible protest organizer" or an "associate of protest organizer" at a Juneteenth event to promote defunding the police. Boca Raton police also ran face recognition scans on half a dozen occasions throughout May 2020 targeting protesters during peaceful events. And the Broward Sheriff's Office ran nearly 20 face recognition searches during this same time period for the purpose of "intelligence" collection, rather than to investigate any criminal offense.[21]

Face recognition has been abused for selective targeting, with law enforcement using the technology to rapidly scan protests for individuals with active bench warrants for unrelated offenses. Several years ago, Baltimore police used face recognition amid protests to find individuals with "outstanding warrants and arrest[ed] them directly from the crowd," in a selective effort that appeared to be aimed at disrupting, punishing, and discouraging demonstrators from protesting.[22]

Absent strong rules, these problems will continue to occur. Face recognition could be used to identify and catalog every attendee at a religious service or political rally, akin to a hyper-powered version of the "mosque crawlers" the New York Police Department deployed for its surveillance of Muslim Americans,[23] or the plants and informants the FBI used to spy on activists as part of COINTELPRO.[24] Face recognition could catalog who goes to a health clinic,

---

[20] Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short" [see note 17].
[21] Joanne Cavanaugh Simpson and Marc Freeman, "South Florida police quietly ran facial recognition scans to identify peaceful protestors. Is that legal?" *South Florida Sun Sentinel*, June 26, 2021, https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sll5uuaqfbeba32rndlv3xwxi-htmlstory.html.
[22] Kevin Rector and Alison Knezevich, "Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest," *Baltimore Sun*, October 11, 2016, https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html.
[23] Research found that the NYPD Muslim surveillance program resulted in "a striking self-censorship of political speech and activism. Conversations relating to foreign policy, civil rights and activism are all deemed off-limits" and expression of religious identity was also severely chilled as "parents discourage their children from being active in Muslim student groups, protests, or other activism, believing that these activities would threaten to expose them to government scrutiny." Diala Shamas and Nermeen Arastu, *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, (2013), 4, https://www.law.cuny.edu/wp-content/uploads/page-assets/academics/clinics/immigration/clear/Mapping-Muslims.pdf.
[24] "FBI Records: The Vault: COINTELPRO," Federal Bureau of Investigation, https://vault.fbi.gov/cointel-pro (accessed July 9, 2021).

substance abuse treatment center, or union meeting. These kinds of sensitive data about people's lives could be stockpiled and used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to evaluations for civil service employment opportunities. And even absent such malicious actions, research has shown that surveillance does in fact chill participation in basic activities, especially when directed at sensitive activities and groups vulnerable to persecution.

The dangers face recognition pose cannot be solved by just restricting use of the most egregious companies and error-prone algorithms; even the most well-designed systems create danger.

When crafting safeguards against face recognition surveillance, lawmakers should not limit their focus just to egregious situations. As the problems described above show, even well-designed systems can cause serious problems.

One face recognition vendor that has garnered significant attention is Clearview AI. Unlike other face recognition systems, Clearview AI builds its reference photo database by scraping billions of photos from social media sites.[25] This practice violates the terms of use for the websites hosting the photos and, more importantly, violates the consent and expectations of privacy of users who place images on their account with the promise that they will not be grabbed en masse and misused. Countering this tactic of mass scraping for biometric scanning may require specific legislative rules.[26]

However, even if law enforcement were totally cut off from using Clearview AI, the general dangers that face recognition surveillance creates would remain. Face recognition systems built on reference photo databases of mugshots or driver's license photos, for instance, can still produce misidentifications for a variety of reasons, and cause serious harms when law enforcement relies on those misidentifications. And face recognition systems built on those same databases can be abused to catalog sensitive activity.

Additionally, while the propensity of many face recognition systems to misidentify people of color at higher rates should be a top priority for lawmakers to address, it is only one of many dangers misidentification poses. Even if systems improved to the point of eliminating algorithmic bias, risks of error will still persist. Because misidentification is often due to poor image quality, even the most reliable systems will remain vulnerable to error. And as long as inequalities exist across our criminal justice system, we can expect the harms of face recognition misidentification to continue to be disproportionately borne by people of color.

Priorities for Lawmakers in Responding to Face Recognition Surveillance

The need for lawmakers to impose strong limits on face recognition is urgent. In the absence of safeguards, roughly half of all adults in the United States already have pre-identified photos

[25] Jake Laperruque, "Danger Isn't Just from Government Abuse: Face Recognition in the Hands of Stalkers, Harassers, and Vigilantes," Project On Government Oversight, June 10, 2021, https://www.pogo.org/analysis/2021/06/danger-isnt-just-from-government-abuse/.
[26] Laperruque, "Danger Isn't Just from Government Abuse" [see note 25].

in databases used for law enforcement face recognition searches, and at least a quarter of the nation's state or local police departments possess the ability to run face recognition searches either directly or via a partnering agency.[27] Meanwhile, even more pervasive face recognition systems are being implemented. Numerous cities have developed plans or implemented pilot programs for untargeted face recognition which scan every person within a crowd who passes by the frame of a camera and provide an alert if anyone scanned is identified as a match against preexisting watchlists.[28]

We are beginning to see significant action to limit face recognition: Over a dozen cities have banned law enforcement use of the technology,[29] and multiple states have recently passed laws that require court approval before law enforcement can run face recognition scans and that limit its use to investigating violent felonies.[30] But for the vast majority of Americans, face recognition can still be deployed against them absent any rules or safeguards.

The most straightforward solution at this time would be to press pause on face recognition surveillance, enacting a national moratorium on its use, as the Facial Recognition and Biometric Technology Moratorium Act would do.[31]

If Congress does not pursue a full moratorium, there are still safeguards that can limit the dangers face recognition surveillance poses. Preventing irresponsible use of face recognition and reliance on misidentifications necessitates transparency requirements, testing and accuracy standards, rules for training and use, limits on how much weight investigators place on matches, and disclosure to defendants. Guarding against abuse and dragnet collection of sensitive information requires meaningful rules for independent authorization—such as a warrant requirement—and limiting use to investigating serious offenses. The Constitution Project's task force report on face recognition examines many of these policies in detail.[32]

Finally, it is vital that any action Congress takes does not preempt restrictions on face recognition passed at the state and municipal level. Many communities have already made clear that they want law enforcement use of face recognition to be fully prohibited, and their preference should be respected. Other cities and states may wish to implement additional restrictions on face recognition that Congress does not consider; this could be especially valuable given rapid developments in how the technology is used. Federal legislation on face recognition can only aid civil rights and civil liberties if it makes clear that separate limits at the state and local level will not be overridden.

---

[27] Clare Garvie, Alvaro Bedoya, Jonathan Frankle, Georgetown Law Center on Privacy & Technology, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (October 18, 2016), 8, 25, https://www.perpetuallineup.org/.

[28] Clare Garvie and Laura Moy, Georgetown Law Center on Privacy & Technology, *America Under Watch: Face Surveillance in the United States*, (May 16, 2019), https://www.americaunderwatch.com/.

[29] Shannon Flynn, "13 Cities Where Police Are Banned From Using Facial Recognition Tech," *Innovation and Tech Today*, November 18, 2020, https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/.

[30] S. 2963, 191st Gen. Ct., 2nd Sess. (MA 2020); H.P. 1174, 130th Leg., 1st Spec. Sess. (ME 2021).

[31] Facial Recognition and Biometric Technology Moratorium Act of 2021, S. 2052, 117th Cong., (2021), https://www.congress.gov/117/bills/s2052/BILLS-117s2052is.pdf.

[32] Task Force on Facial Recognition Surveillance, *Facing the Future of Surveillance* [see note 1].