PROJECT ON GOVERNMENT OVERSIGHT

Testimony of Jake Laperruque, Senior Counsel
The Constitution Project at the Project On Government Oversight,
before the Presidential Commission on Law Enforcement and Administration of Justice's Technology Working Group
on Law Enforcement Use of Facial Recognition
April 22, 2020

Thank you for the opportunity to testify before the Presidential Commission on Law Enforcement and Administration of Justice's Technology Working Group on the issue of law enforcement use of facial recognition technology.

I am Jake Laperruque, senior counsel for The Constitution Project at the Project On Government Oversight (POGO). 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 facial recognition surveillance.

Last year, our organization convened a task force of expert stakeholders including law enforcement officials, academics, tech experts, and civil rights and civil liberties advocates to examine the impact of facial recognition surveillance.[1] This group concluded that if law enforcement uses facial recognition, its use of the technology should be subject to checks and limits. The task force also provided a set of recommendations for implementing these changes.

Facial recognition is an immensely powerful technology. It offers some opportunities to streamline operations and aid law enforcement, such as confirming identifications during booking, preventing forgery of IDs, and finding missing persons. However, it also creates unprecedented potential for surveillance. Authoritarian regimes such as those in China and Russia have already shown how facial recognition can be used to stockpile records of individuals' daily lives and suppress vital activities such as protests.[2] But abuse is not limited to

[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-the-future-of-surveillance/

[2] Paul Mozour and Aaron Krolik, "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers," *New York Times*, December 17, 2019. https://www.nytimes.com/2019/12/17/technology/china-surveillance.html; Paul Mozour, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *New York Times*, April 14, 2019. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; James Vincent, "Moscow rolls out live facial recognition system with an app to alert police," *Verge*, January 30, 2020. https://www.theverge.com/2020/1/30/21115119/moscow-live-facial-recognition-roll-out-ntechlab-deployment

those nations; misuse of facial recognition has already occurred in the United States.[3] Further, facial recognition can be highly prone to error based on circumstance and manner of use. Misidentifications pose a serious threat to public safety, civil liberties, effective law enforcement operations, and police-community relations.

In order to prevent these harms, if law enforcement intends to use facial recognition, it should abide by three overall principles, and implement policies in conjunction with these principles. First, facial recognition must be viewed as a technology that fundamentally alters police power, and should not be brought into use without public debate. Second, facial recognition must be treated as a forensic tool that requires careful use and precise application, not an all-purpose tool that can be wielded bluntly or casually. And third, facial recognition must be checked by limits that will prevent improper applications and abuse.

Facial Recognition Fundamentally Alters Police Power, and Requires Public Debate

Facial recognition technology does not merely offer a slight increase in police capabilities, but rather can profoundly redefine the power of police in unprecedented ways.

One misconception about facial recognition is that it is comparable to a police officer possessing photographic memory. It is worth noting, first, that not only is photographic memory extremely rare in adults, its limits in accuracy and scale make perfect recall of a large quantity of images and corresponding names virtually impossible.[4]

But even it was possible for a person to have flawless and limitless photographic memory, it would be impossible to for them to process images on a scale comparable with facial recognition systems. For example, Texas police can use facial recognition to search over 24 million mugshots and 24 million DMV photographs.[5] If an officer with perfect photographic memory processed one photo per second, it would take over 555 days of photo review to process all these images. Facial recognition systems conduct this review nearly instantaneously. This technology is fundamentally different from human analysis, and it should be treated as such in formulating new rules and guidelines.

Facial recognition also differs from other identification tools in important ways. It allows law enforcement to identify individuals absent notification or consent, a significant departure from traditional ways of checking identification. And while stopping someone on the street and

[3] 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

[4] William Lee Adams, "The Truth About Photographic Memory," *Psychology Today*, June 9, 2016. https://www.psychologytoday.com/us/articles/200603/the-truth-about-photographic-memory; Alan Searleman, "Is here such a thing as photographic memory? And if so, can it be learned?" *Scientific American*, March 12, 2007. https://www.scientificamerican.com/article/is-there-such-a-thing-as/

[5] Center on Privacy & Technology at Georgetown Law, "The Perpetual Line-Up: Texas Department of Public Safety (DPS)," September 2016. https://www.perpetuallineup.org/sites/default/files/2016-10/21_Texas.pdf

checking their identification requires reasonable suspicion,[6] the vast majority of law enforcement entities that use facial recognition are not required to possess *any* suspicion of wrongdoing.[7]

Facial recognition also fundamentally differs from other noninteractive identification tools such as fingerprint and DNA collection. Facial recognition scans can be conducted on a far vaster scale than identification checks can be done through these established methods. Additionally, whereas individuals' fingerprints and DNA profiles typically are not held by law enforcement absent an arrest, many law enforcement agencies are able to conduct face recognition scans using images in a state's DMV database,[8] or conduct scans of anyone who has a Facebook or Instagram profile.[9]

Absent limits, these factors open the door to abuse and monitoring of the population on a massive scale. The Supreme Court has imposed limits on law enforcement's use of cellphone location monitoring, another relatively new technology, by requiring law enforcement to obtain a warrant before using this form of surveillance in order to protect the constitutional right to privacy, even in public. As the court noted in its 2018 *Carpenter v. United States* decision, "as technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[10]

All branches and levels of government should similarly strive to preserve the right to privacy when considering implementing innovative surveillance technologies such as facial recognition.

If law enforcement wishes to use facial recognition, it should not simply adopt this technology without the input and consent of communities. Rather, law enforcement bodies should announce their desire to use facial recognition before they begin implementing systems, and allow the community to debate the issue and decide what limits it wants on the technology. Creating a facial recognition system absent public notification or input can lead to confusion and mistrust.[11]

Face Recognition Must Be Treated as a Forensic Tool Requiring Careful Use and Precise Application

---

[6] *Terry v. Ohio*, 392 U.S. 1 (1968).

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

[8] Garvie, Bedoya, Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Sec. I [see note 7].

[9] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *New York Times*, February 10, 2020. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[10] *Carpenter v. United States*, 138 S. Ct. 2206 (2018). [Internal citations omitted]

[11] For example, in Detroit development and implementation of the city's facial recognition system before public debate led to concern and questions over whether facial recognition was built into the city's Green Light and traffic cameras. Michael E. Duggan, "Mayor Duggan: I Oppose Use of Facial Recognition Technology for Surveillance," City of Detroit, July 18, 2019. https://detroitmi.gov/news/mayor-duggan-i-oppose-use-facial-recognition-technology-surveillance.

Facial recognition's potential for misidentification and user error makes the prospect of law enforcement using it on a large scale all the more worrisome. Like any forensic tool, it should be used carefully and precisely. In order to minimize the frequency of misidentifications, law enforcement must be aware of this tool's limits and the factors that may affect accuracy; rules and guidelines should be enacted that promote careful and precise application rather than casual use.

Misidentifications are among the most prevalent and troubling risks face recognition creates. If law enforcement does not mitigate the risk of misidentifications in its use of this technology, face recognition will likely endanger public safety, civil liberties, and police-community relations by implicating improperly identified individuals in investigations or police action. The effectiveness of facial recognition is highly dependent on circumstances. Poor use-practices and unreasonable applications can significantly diminish accuracy.

Face recognition's tendency to misidentify women and people of color at a higher rate than other people is an acute concern. 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.[12] 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.[13] 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.

The accuracy of face recognition in general is also subject to technical limitations. Because the technology centers on comparing features in photographs, image quality is essential to obtaining reliable results.[14] Specifically, face recognition compares "probe" images, from which law enforcement seeks to identify individuals, to reference images, which contain previously identified faces.[15] Reference images are typically high-resolution photos of a person directly

---

[12] 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.

[13] Grother, Ngan, Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, 2 [see note 12].

[14] Task Force on Facial Recognition Surveillance, *Facing the Future of Surveillance* [see note 1]; Garvie, Bedoya, Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Sec. V [see note 7].

[15] Garvie, Bedoya, Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Sec. III [see note 7].

facing a camera at close range, such as for a mug shot photo. But probe images are derived from a huge range of situations, which creates potential for low image quality and erroneous results.

Bad lighting, indirect angles, distance, poor camera quality, and low image resolution all will undermine reliability of matches.[16] And these poor image conditions are much more likely when photos and videos are taken in public, such as with a CCTV camera. However, images like these often serve as face recognition probe images used in investigations, without due consideration for their diminished utility.[17]

Law enforcement should also be aware that vendors may exaggerate their technology's capabilities and may fail to highlight its limits in order to advertise their product as more broadly useful than it truly is. 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."[18] This is a highly inflated characterization given the limits that lighting and angle would impose in such a situation. Many other vendors also claim facial 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 facial recognition systems operate in practice.[19]

The reliability of face recognition also varies based upon the confidence threshold of potential matches.[20] 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 "match" is actually a false positive. So, if law enforcement 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.[21]

---

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

[17] "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

[18] Jesse Davis West, "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/

[19] Cognitec states that its software can be used for "fast *identification of suspects* and efficient crime investigations." [Emphasis added] Cognitec, "Applications: Law enforcement." https://www.cognitec.com/law-enforcement.html (accessed April 20, 2020); and, as of August 2019, Dataworks Plus promised law enforcement "reliable candidates 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." [Emphasis added] Dataworks Plus, "Facial Recognition Technology & Case Management."
http://web.archive.org/web/20190811221236/http://www.dataworksplus.com:80/faceplus.html

[20] 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-recognitionaccuracy/

[21] 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 so that it "returns a gallery of 'candidate' photos [reference photos] of 2-50 individuals (the default is 20)." House Committee

For example, one police department designed its facial 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.[22] This risk could be eliminated by employing minimum accuracy standards that prevent low confidence threshold "matches" from appearing.

This is another area where law enforcement should be wary that vendors may downplay facial recognition's limits. An investigation by the outlet *Gizmodo* revealed that even as Amazon stated publicly that it recommended its law enforcement clients only use its systems when it found matches with 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.[23]

Finally, there are numerous irresponsible techniques for using facial recognition that severely undercut its reliability and exacerbate the risks of misidentification. Some law enforcement agencies have engaged in the highly questionable practice of scanning police sketches of suspects in lieu of using actual probe images of suspects; using computer editing to artificially fill in pieces of a face that were not caught on camera; or even discarding the desired individual's photo entirely, in favor using a photo of a celebrity lookalike.[24] The police chief of a major department last year went so far as to defend entirely building half of individuals' faces from artificial imaging for facial recognition scans, claiming it was a valid use of the system.[25] Asking systems to analyze inauthentic and manufactured data will produce inauthentic and unreliable results. Computer programs do not see faces the way humans do. Artificially adding data to be used in a face recognition scan is the equivalent to drawing in lines on a smudged fingerprint.

---

on Oversight and Reform. *Facial Recognition Technology (Part II): Ensuring Transparency in Government Use: Hearing before the House Committee on Oversight*, 116th Cong. (June 4, 2019). https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use.

[22] 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/

[23] 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/

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

[25] In an op-ed advocating for its facial recognition system, then-New York City Police Commissioner James O'Neill stated, "The system can also create a mirror image of the right side of a face if we have only the left side, for example, to produce a 3-D model." This is not a reliable use, given that facial recognition systems examine the full contours of individuals' faces, and that most individuals' faces are actually not symmetrical. James O'Neill, "How Facial Recognition Makes You Safer," *New York Times*, June 9, 2019. https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html

It is important to resist the temptation to shrug off the risks misidentification poses by claiming that facial recognition could just be used for leads, rather than as the backbone of a prosecution.[26] 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 disruptive and potentially traumatic, and can raise the prospect of an individual being harmed even if charges or a conviction never follow. And an individual could in fact be charged in part based on how a match produced by a facial 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 reported incident, New York City Police Department officers took a single possible match from a facial recognition system, and then texted a witness, "Is this the guy…?" along with the photo, rather than following proper procedure by using a photo array.[27] In this situation, facial recognition played a major role in an arrest, and it is far from an isolated incident.[28]

Law enforcement must make responsible decisions about how they use facial recognition with the knowledge that a host of factors—reliability of the algorithm in general and specifically for the demographics of the suspect, image quality, whether the image has been altered, and the confidence threshold permitted—affect whether the "matches" their systems produce are well founded or implicate innocent individuals.

Law enforcement should not rely on a technology with significant, known, and still-unmitigated flaws for investigative work. If law enforcement uses facial recognition, this use must be within the bounds of policies that limit use to proper situations and prevent irresponsible applications.

Finally, real-time facial recognition poses uniquely significant accuracy problems. This type of system does not attempt to identify a single probe image. Rather, real-time facial recognition scans every person in a crowd caught on camera by a video feed, and produces an alert if anyone scanned is identified as a match against a preexisting watchlist.

Real-time face recognition takes all the misidentification risks of using standard facial recognition and multiplies them by conducting scans of groups of individuals. Early testing has

---

[26] 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 Investigation: Hearing before the House Judiciary Committee*, 116th Cong. (February 5, 2020). https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=2780

[27] Garvie, "Garbage In, Garbage Out: Face Recognition on Flawed Data," [see note 24].

[28] 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 ("Although officials said investigators could not rely on facial recognition results to make an arrest, documents suggested that on occasion officers gathered no other evidence.")

shown these risks are not hypothetical. In pilot programs in the United Kingdom, South Wales police had a 91% error rate and London Metropolitan Police had a 98% error rate.[29]

Given that real-time face recognition is far more likely to produce misidentifications than genuine matches, its implementation should be kept on hold. In its current state real-time face recognition will only serve to endanger innocent individuals and undermine public trust in law enforcement.

Facial Recognition Should Be Checked by Limits to Prevent Improper Applications and Abuse

In addition to facial recognition's accuracy problems, use of the technology remains unchecked by necessary rules or policies to prevent improper applications and abuse—this must change if law enforcement wishes to use this technology. As the Supreme Court recently noted, the right to privacy—and the role of privacy rights in limiting government surveillance—does in fact extend to public places.[30] Protecting this right—and establishing guardrails that prevent the government from stockpiling information about the intimate details of its citizens' lives—is essential to the functioning of democratic society.

Recent American history shows significant abuses of surveillance powers that targeted individuals based on race, religious affiliation, and political activity.[31] Facial recognition could easily be exploited to target individuals in the same way.

Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and catalog individuals' engagement in these First Amendment-protected activities. Using facial recognition with no restrictions to curb abuse presents the potential that discretion could become a tool for selective prosecution. The ability to effortlessly pull up potential facial recognition matches for individuals with an active bench warrant for a low-level offense has in fact already led to abusive targeting, such as against individuals attending protests, political events, and religious ceremonies. Several years ago, Baltimore police used facial recognition amid protests to find individuals with "outstanding

[29] Big Brother Watch, *Face Off: The Lawless Growth of Facial Recognition in UK Policing* (May 2018), 3-4. https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

[30] *Carpenter v. United States*, 138 S. Ct. 2206 (2018). ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." [Internal quotes omitted])

[31] Diala Shamas and Nermeen Arastu, Creating Law Enforcement Accountability & Responsibility Project, Asian American Legal Defense and Education Fund, and Muslim American Civil Liberties Coalition, *Mapping Muslims: NYPD Spying and its Impact on American Muslims* (June 28, 2012). https://www.law.cuny.edu/wp-content/uploads/page-assets/academics/clinics/immigration/clear/Mapping-Muslims.pdf; *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities,* S. Rep. No. 94-755 (1976). https://www.intelligence.senate.gov/resources/intelligence-related-commissions

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.[32]

Many other areas of people's lives are also vulnerable to invasive facial recognition surveillance. With facial recognition, the government could potentially catalog everyone who goes to a mental health clinic, seeks help at a substance abuse treatment center, or attends a 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.

Even without abuse occurring, the mere ability to collect and freely use this type of highly personal and sensitive information could chill participation in political, religious, and a variety of other constitutionally protected activities. Research has shown that surveillance does in fact chill participation in basic activities, especially when directed at sensitive activities and groups vulnerable to persecution.[33]

In order to prevent and mitigate the numerous harms that could result from improper and unfettered use of facial recognition, it is necessary to place regulations on how facial recognition is used. Fortunately, strong rules that will prevent abuse and build public confidence can be enacted in a manner that will not undercut the uses of facial recognition that offer the most potential value.

The most important limitation to place on the use of facial recognition to prevent misuse is a warrant requirement. Probable cause warrants are our most important shield against improper surveillance, providing both independent oversight and ensuring that invasive surveillance is directed only at individuals suspected of wrongdoing. This is why there are warrant requirements for use of powerful electronic surveillance tools such as wiretapping, cellphone location tracking, thermal imaging devices, GPS tracking devices, and cell-site simulators. Indeed, neither the public nor the courts would find it acceptable for law enforcement to track someone's cellphone for a month absent any authorization or limits, even if law enforcement stated that this surveillance would just be used for leads.

A warrant rule would provide significant benefits in preventing facial recognition from being used to catalog sensitive but innocuous activities and associations, and would increase public trust that law enforcement was using the technology responsibly. And because most investigative applications of facial recognition focus on identifying an individual whose image is recorded in commission of a crime, meeting this requirement should not be a significant barrier to legitimate use. A warrant requirement could also include reasonable exceptions modeled on existing rules,

---

[32] 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

[33] 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." *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, 4.

such as those governing identification of victims and missing persons, as well as exceptions that could be made in exigent circumstances.

Another critical regulation to prevent abuse is a requirement that use of facial recognition be limited to investigation of serious offenses. Such a rule is necessary to prevent law enforcement from using the unprecedented discretionary power facial recognition offers for selective enforcement, as occurred during the Baltimore protests.[34] This rule would also be a key means of ensuring that law enforcement uses this tool exclusively in cases that receive the highest level of scrutiny and review. And it would prevent facial recognition from being used for dragnet surveillance, something that is already occurring in China as facial recognition constantly monitors all public activity, ostensibly in an effort to curb petty offenses.[35]

POGO's task force on facial recognition recommended that departments center a serious crime limit on Uniform Crime Reporting Title 1 crimes, with some additions and deviations.[36] This would allow law enforcement to use facial recognition in order to respond to significant crimes and threats, while limiting the risk of selective enforcement and abuse.

Finally, it is essential that defendants are given notice when facial recognition is used as a basis for their arrest and prosecution. This must occur even if facial recognition is used as the basis for obtaining future evidence, rather than itself serving as direct evidence in court proceedings. In some jurisdictions, law enforcement uses facial recognition thousands of times per month, but defendants almost never receive notice of its use in investigations.[37] As the *New York Times* described in a detailed investigation of how law enforcement agencies use facial recognition:

> Any technological findings presented as evidence are subject to analysis through special hearings, but facial recognition results have never been deemed reliable enough to stand up to such questioning. The results still can play a significant role in investigations, though, without the judicial scrutiny applied to more proven forensic technologies …. In some of the Florida cases The Times reviewed, the technology was not mentioned in initial warrants or affidavits. Instead, detectives noted "investigative mean" or an "attempt to identify" in court documents, while logging the matters as facial recognition wins in the Pinellas County records.[38]

As discussed above, the reliability of facial recognition is highly dependent upon circumstance and manner of use. While enacting the recommendations provided in reference to this issue

---

[34] This risk is acute because bench warrants can be for minor offenses, and apply to huge portions of a community. For example, a 2015 Department of Justice investigation revealed that Ferguson, Missouri, had active, outstanding municipal arrest warrants—mostly for minor offenses such as unpaid fines for traffic violations—for 16,000 people in a municipality with a population of 21,000. Department of Justice Civil Rights Division, *Investigation of the Ferguson Police Department*, (March 4, 2015) 3-6, 55. https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf

[35] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *New York Times*, July 8, 2018. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html

[36] Task Force on Facial Recognition Surveillance, *Facing the Future of Surveillance*, Sec. IV III [see note 1].

[37] Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short" [see note 28].

[38] Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short" [see note 28].

would mitigate risk, defendants still have the right to review whether it was used in a proper manner with reasonably reliable results, as with any other forensic technology.

Recommendations

POGO offers the following recommendation on use of the technology, which are largely based on the limits recommended by our Task Force on Facial Recognition.

In order to enhance community confidence in law enforcement and any use of facial recognition technology, we recommend that if law enforcement entities wish to use facial recognition, they do the following:

1. **Encourage community debate before deploying facial recognition.** Law enforcement entities should inform their local community of their intention to use facial recognition before implementing a system, and facilitate a public debate so that their adoption of facial recognition is preceded by establishment of community-based standards.

In order to reduce the risk misidentifications, improve accuracy, and ensure proper treatment of facial recognition as a forensic technology, we recommend that if law enforcement entities use facial recognition, they do the following:

2. **Require independent testing and prioritize high accuracy standards.** Law enforcement should only use software that is regularly tested by independently entities—such as the National Institute of Standards and Technology—and have higher levels of accuracy both in general and among various demographic groups.
3. **Require extensive training for officers using facial recognition.** Before allowing an officer to use a facial recognition system, departments should require extensive training on the technology, including on its overall limits, the impact of image quality, the impact of confidence thresholds, and the tendency for higher rates of error for certain demographic groups.
4. **Treat facial recognition as a forensic tool rather than an all-purpose tool.** Use specially trained and designated staff that are not involved in investigations related to the scans they run.
5. **Do not use unreliable matches with low confidence thresholds.** Require high confidence thresholds in order to use potential matches, and do not deploy standards that automatically return a set number of matches even if they have a low confidence threshold.
6. **Prohibit the use of junk science methods based on artificial imagery.** Prohibit the use of facial recognition with images that are partially computer generated, or images such as sketches or images of lookalikes that are not photographs of the individual being sought.
7. **Require independent verification of matches.** Require independent verification of matches produced by facial recognition, and place a limit on the value matches can have—such as considering them equivalent to an anonymous 911 call—as the basis for officers' actions and investigations.

8. **Prohibit the use of real-time facial recognition.** Real-time facial recognition and crowd scanning should not be permitted while this form of facial recognition is so prone to error.

In order to provide proper safeguards against abuse and improper targeting that invasive surveillance tools such as facial recognition can be misappropriated for, we recommend that if law enforcement entities use facial recognition, they do the following:

9. **Require probable cause warrants.** Law enforcement should be required to obtain a probable cause warrant from a judge in order to use facial recognition for investigative purposes. Exceptions can be made for situations such as identifying victims, locating missing persons, or responding to exigent circumstances.
10. **Establish a serious crimes limit.** Use of facial recognition should be limited to serious crimes, such as Uniform Crime Reporting Title 1 crimes.
11. **Require disclosure to defendants.** Defendants should receive notice whenever facial recognition was used in an investigation that led to their prosecution, including when facial recognition served as the basis for obtaining derivative evidence.
12. **Require strict auditing with public transparency.** Law enforcement should maintain a regular auditing system with public reporting on results to ensure these rules are followed and the public has confidence in them, and publish reports on how often facial recognition is sought and used.