January 15, 2022

Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Ave.
Washington, D.C. 20504

INTRODUCTION

The National Association of Criminal Defense Lawyers (NACDL) is the preeminent organization in the U.S. advancing the goal of the criminal defense bar to ensure justice and due process for persons charged with a crime or wrongdoing. NACDL serves as a leader, alongside diverse coalitions, in identifying and reforming flaws and inequities in the criminal legal system; redressing systemic racism; and ensuring our members and others in the criminal defense bar are fully equipped to serve all accused persons at the highest level. NACDL is concerned that the rapid deployment of untested and unregulated technologies will entrench and exacerbate the racial disparities that have existed for as long as the criminal legal system, and that these technologies will undermine efforts for reform. For the reasons below, the Office of Science and Technology Policy (OSTP) should not endorse any state-sponsored biometric-tracking, -storing, or -sharing technologies nor capabilities.

The below comment focuses primarily on face recognition software because it is currently the most studied biometric technology with the most widely available analyses. That said, the entire spectrum of biometric surveillance technologies—including (but not limited to) facial recognition, gait recognition, iris and retinal scanning, keystroke dynamics, and voice recognition—poses enormous risk to already over-policed communities, depriving them of due process and reinforcing racist police practices. Advances in technology will only magnify these problems while raising additional privacy concerns associated with real-time and historical searches of videos and images.

To date, it has been difficult for defense lawyers to challenge the use of face recognition or other biometrics. When law enforcement uses such technologies, they do so surreptitiously, affording the accused and their defense counsel no notice whatsoever nor any opportunity to challenge its use. Even when notice is given, the defense is often denied needed discovery due to claims of "trade secrets" and proprietary software, leaving them unable to scrutinize and validate the tools used against their clients. These clandestine police practices impermissibly interfere with the accused's constitutional rights to a fair trial and to confront the witnesses against them.

Biometric technologies are powerful and invasive tools, especially in the hands of law enforcement. Before regulating or disseminating such tools, the Administration should first consider whether such tools have any place in law enforcement. NACDL believes they do not, and OSTP's primary recommendation regarding law enforcement's use of biometric surveillance technologies should be one of outright prohibition. And if such technology is used by law enforcement, it must be disclosed to the accused—and their defense counsel—with full transparency. NACDL's recommendations beyond a prohibition are not an endorsement of the use of such technology. Rather, they are made with the understanding that many law enforcement agencies are already using such technologies, and notice and transparency for the accused and their defense counsel are important mitigation measures.

COMMENT

Biometric surveillance technologies are incredibly powerful tools. They are also notoriously inaccurate in identifying people, particularly women and Black, Indigenous, and People of Color ("BIPOC") individuals. Even if these tools were 100% accurate, the persistent and invasive nature of the surveillance would still raise grave constitutional concerns. And in the hands of law enforcement agents—i.e., those capable of depriving people of their liberty and even their lives—these tools do more harm than good. This is especially true for BIPOC communities, who are already subjected to racially biased policing and surveillance.[1]

Biometric surveillance does not solve any longstanding problem in the criminal legal system; rather, it entrenches racist practices already thriving within it.[2] Before our society adopts

[1] *See generally* NAT'L ASS'N OF CRIM. DEF. LAW., GARBAGE IN, GOSPEL OUT (2021), https://www.nacdl.org/Document/GarbageInGospelOutDataDrivenPolicingTechnologies.

[2] *Id.* at 16-17.

new technology to solve an alleged problem, it is important that we understand both the problem(s) that new technology is attempting to solve and its supposed ability to solve it. We should not put the proverbial cart before the horse, asking what uses we can conjure for this new, potentially omniscient technology. Instead, we must first spend as much time and resources as necessary to properly identify and frame those problems that need solving. Only after that can we begin trying to determine whether the technology at issue can solve that thoroughly identified—and understood—problem.

There is simply no data to back up the idea that biometric technologies, as they currently exist or perhaps ever, are the right tools for "reducing crime" even though they are often promoted as doing exactly that. Because biometric surveillance technology like facial recognition performs worse with darker skinned individuals and women[3]—and due to racist policing practices and the racially biased databases these surveillance technologies reference[4]—the more plausible result of its rollout is to exacerbate the over-policing of BIPOC communities and feed mass incarceration.

It is also important to note that *people* write the code underlying these algorithms and *people* choose the datasets used to train them. Because *people* harbor implicit bias, and because datasets reflect past bias, the computer's instructions (i.e., its code) are tainted with what's referred to as algorithmic bias.[5] Ultimately, people are fallible. And within the criminal legal system,[6] that fallibility can determine whether someone is deprived of their liberties. The Administration should hold off on using any biometric surveillance technology that is not yet fully understood nor serves as a clear solution to a stated problem. To do otherwise gives far too much power to private companies that are designing a dangerous (and profitable)[7] "solution" without an identified problem.

[3] *See* sources cited *infra* note 8.

[4] *See* Najibi, *infra* note 8.

[5] *See, e.g.*, Rebecca Heilweil, *Why Algorithms Can Be Racist and Sexist*, VOX: RECODE (Feb. 18, 2020, 12:20 PM), https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency.

[6] Outside the criminal legal system context, biometric algorithm inaccuracies can cause drastically negative consequences in areas like unemployment insurance. *See* Todd Feathers, *Facial Recognition Failures Are Locking People out of Unemployment Systems*, VICE: MOTHERBOARD (June 18, 2021, 3:27 PM), https://www.vice.com/en/article/5dbywn/facial-recognition-failures-are-locking-people-out-of-unemployment-systems.

[7] *See* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 19, 20 (2017), https://www.nyulawreview.org/wp-content/uploads/2017/08/NYULawReviewOnline-92-Joh_0.pdf ("Through different mechanisms intended to promote their own interests and profits, these [surveillance technology] companies exert control over the police long after their products have been adopted.").

NACDL acknowledges that many law enforcement agencies are already using biometric surveillance tools for all types of offenses, including low-level crimes and misdemeanors. While we oppose all biometric surveillance for all offenses, its use for low-level offenses is particularly harmful to BIPOC communities because racist police practices result in BIPOC being more frequently stopped, questioned, and arrested by law enforcement. This creates a pernicious feedback loop: BIPOC who live in over-policed communities are stopped by police at a disproportionately higher rate, regardless of offense severity; their biometrics are run against face image databases using algorithms that perform poorly with darker skin tones and women, meaning they're more likely to result in false positives; the arrest data gets fed back into law enforcements' data-driven police practices and further entrenches the biased policing of BIPOC communities, increasing the chances these individuals will again be stopped and queried against these databases in the future.

1. Facial recognition algorithms misidentify BIPOC and women's faces at a much higher rate, exacerbating an already discriminatory policing system that preys on multi-marginalized communities.

By now, it is well documented that facial recognition algorithms' performance varies based on age, skin tone, and gender. Time and again, studies have shown these algorithms' ability to match faces drops significantly when tasked with analyzing younger individuals, darker skinned individuals and women, with the worst error rates occurring for women of color.[8] This is extremely concerning, given the also well documented policing practices that disproportionately target BIPOC communities, particularly Black people.[9]

The fact cross-racial eyewitness identification has proven deeply problematic also plays a role here. Eyewitness identifications are notoriously unreliable, even more so when they are

[8] *See, e.g.*, Alex Najibi, *Racial Discrimination in Face Recognition Technology*, HARV. GRADUATE SCH. SCI. NEWS (SPECIAL EDITION) (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ ("A growing body of research exposes divergent error rates across demographic groups, with the poorest accuracy consistently found in subjects who are female, Black, and 18-30 years old. . . . [F]ace recognition technologies across 189 algorithms are least accurate on women of color."); *see also* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACHINE LEARNING RES. 1 (2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[9] *See, e.g.*, *Fatal Force*, WASH. POST, https://www.washingtonpost.com/graphics/investigations/police-shootings-database/ (last updated Jan. 15, 2022); Lynne Peeples, *What the Data Say About Police Brutality and Racial Bias — and Which Reforms Might Work*, NATURE (June 19, 2020), https://www.nature.com/articles/d41586-020-01846-z (last updated May 26, 2021).

cross-racial.[10] Facial recognition systems, by design, seek a face in the referenced database(s) that looks like the one law enforcement agents are trying to find.[11] In other words, the system searches for a doppelganger. Furthermore, these systems (at least in the U.S.) are trained on datasets made up of primarily white, male faces.[12] As a result, facial recognition systems regularly misidentify BIPOC—especially darker-skinned women.[13]

It doesn't take much imagination,[14] then, to see where too hastily implementing facial recognition or other biometric surveillance technologies could lead: When law enforcement agencies rely on facial recognition systems that by design find a person who looks like the referenced photo and misidentify BIPOC faces at a higher rate—and then show that "match" to an eyewitness for cross-racial identification purposes—the potential for an inaccurate identification, already high, is compounded. Inevitably, people will be mis-identified, charged, and prosecuted, and the inequities faced by BIPOC communities in the criminal legal system will be exacerbated.[15]

2. <u>Mugshot databases disproportionately include Black faces, and, regardless, the faces queried against them and other databases are disproportionately BIPOC individuals' faces.</u>

The facial recognition techniques most widely used today involve either: 1) "face matching," the practice of comparing an unknown person's faceprint against a database of

[10] *See, e.g.*, Jed S. Rakoff & Elizabeth F. Loftus, *The Intractability of Inaccurate Eyewitness Identification*, 147 DAEDALUS 90 (2018), https://doi.org/10.1162/daed_a_00522; Laura Connelly, *Cross-Racial Identifications: Solutions to the "They All Look Alike" Effect*, 21 MICH. J. RACE & L. 125 (2015), https://repository.law.umich.edu/mjrl/vol21/iss1/5; Michael Barbella, *More Than Meets the Eye in Cross-Racial IDs*, N.J. ST. B. FOUND. (May 7, 2021), https://njsbf.org/2021/05/07/more-than-meets-the-eye-in-cross-racial-ids/.

[11] The photo of the unknown person whose identity law enforcement is trying to determine is typically called the "probe" photo.

[12] Buolamwini & Gebru, *supra* note 8; *see also* Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

[13] *See* sources cited *supra* note 8.

[14] To be frank, it takes no imagination. Shoddy police work coupled with overreliance on facial recognition's false promise of accuracy has already caused mistaken arrests that result in nights spent in a holding cell and trauma to both the arrestee and those close to them, not to mention time spent away from home and work at things like arraignments and other court hearings. *See* Robert Williams, *I Did Nothing Wrong. I Was Arrested Anyway.*, ACLU (July 15, 2021), https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway.

[15] This potential is all the more problematic because some who advocate for increasing the use of computers in policing tout the incorrect idea that because a computer makes the decision, it is somehow more objective than were a person to do so. As stated above, computer code is *created by people* who are just as guilty as anyone of exercising implicit bias. *See* Heilweil, *supra* note 5.

known faceprints to determine the unknown person's identity;[16] or 2) "face verification," the type of facial recognition that, for example, unlocks a smartphone when it recognizes the user's face.[17]

Due to historically racist policing practices, mugshot databases are themselves discriminatory, overrepresenting BIPOC because they are overpoliced and therefore arrested at higher rates.[18] Even if the referenced database were not itself discriminatory (e.g., a database of driver's license photos from one of the 32 states that permit use for facial recognition),[19] the problem persists because BIPOC—again due to racist policing practices—are stopped, arrested, and run against all databases more frequently. In other words, even if the database of faces were more representative of the country or a particular state, the faces of those who are queried against it tend to be BIPOC faces because racist police practices result in their more frequently being stopped and having their faces *inaccurately* analyzed.

Again, looking at this from a criminal legal system lens puts the concerns regarding this surveillance technology into stark relief: Members of over-policed BIPOC communities are more likely to be inaccurately matched and subject to future invasive surveillance, because the technology performs worse with darker skin tones; because BIPOC faces are disproportionately represented in mugshot databases; and, since they're more likely to be stopped or arrested, because their faces are more likely to be referenced against any database.[20]

[16] Bennett Cyphers, Adam Schwartz & Nathan Sheard, *Face Recognition Isn't Just Face Identification and Verification: It's Also Photo Clustering, Race Analysis, Real-Time Tracking, and More*, ELEC. FRONTIER FOUND.: DEEPLINKS (Oct. 7, 2021), https://www.eff.org/deeplinks/2021/10/face-recognition-isnt-just-face-identification-and-verification ("[Face matching] is often done by taking a faceprint from a new image (e.g. taken by a security camera) and comparing it against a database of 'known' faceprints (e.g. a government database of ID photos). If the unknown faceprint is similar enough to any of the known faceprints, the system returns a potential match. This is often known as 'face identification.'").

[17] *Id.* ("Face matching can also be used to figure out whether two faceprints are from the same face, without necessarily knowing whom that face belongs to. For example, a phone may check a user's face to determine whether it should unlock . . . .").

[18] *See* Radley Balko, Opinion, *There's Overwhelming Evidence that the Criminal Justice System Is Racist. Here's the Proof.*, WASH. POST (June 10, 2020), https://www.washingtonpost.com/graphics/2020/opinions/systemic-racism-police-evidence-criminal-justice-system/.

[19] As of 2019, at least 30 states' driver's license databases were available to law enforcement agencies for facial recognition searches. Clare Garvie, Opinion, *You're in a Police Lineup, Right Now*, N.Y. TIMES (Oct. 15, 2019), at 1:02, https://www.nytimes.com/2019/10/15/opinion/facial-recognition-police.html ("You could be picked out, investigated, possibly arrested and sent to jail, because you got a driver's license in one of these 32 states.").

[20] *See* Najibi, *supra* note 8 ("The Black presence in such systems creates a feed-forward loop whereby racist policing strategies lead to disproportionate arrests of Black people, who are then subject to future surveillance. . . . [I]nclusion in these monitoring databases can lead to harsher sentencing and higher bails—or denial of bail altogether.").

3. Despite our recommendations against more biometric data and surveillance tools in the State's hands, if OSTP ultimately recommends biometric regulations, it should require full transparency.

A. *No positive identification*

Currently, individual law enforcement agencies and sovereigns determine whether biometrics may serve as sufficient identification to make an arrest.[21] OSTP must ensure that any time a law enforcement agency—or any entity capable of depriving liberty—relies on biometrics, the biometric is supplemented by other, adequate investigatory material.

Given the numerous problems identified above—e.g., well-documented issues with cross-racial eyewitness identification, over-policing of multi-marginalized communities; overrepresentation of Black people's faces in mugshot databases and disproportionate querying of BIPOC faces against all other databases; biometric algorithms' potential for false positives with BIPOC faces—such biometric identification methods should never be the sole evidence that law enforcement agents rely on to arrest or search an individual.

B. *Providing notice and ending black box defenses*

When law enforcement uses biometric surveillance technology, the accused in a criminal case must be provided notice regarding such technology's use. If the accused's liberty may be determined by (fallible) computer algorithms, then the Sixth Amendment[22] and fundamental fairness require the accused be given a chance to confront the evidence against them and validate the technology. Too often where biometric surveillance is involved, prosecution and law enforcement entities bury its use by saying it was only used for lead generation purposes. This cannot continue. As per *Daubert* and *Frye* hearings, defense attorneys must be given notice and the opportunity to assist their clients in assessing the validity and reliability of the technology used to bolster the government's case.

[21] *See Facial Recognition Technology: Part II Ensuring Transparency in Government Use Before the H. Comm. on Oversight & Reform*, 116th Cong. 4 (2019) (statement of Kimberly J. Del Greco, Deputy Assistant Director, Federal Bureau of Investigation), https://www.govinfo.gov/content/pkg/CHRG-116hhrg36829/pdf/CHRG-116hhrg36829.pdf (stating the FBI "pioneered" its facial recognition practices and that "photo candidates returned are not to be considered positive identification").

[22] U.S. CONST. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him . . . .").

There is a relevant *Brady*[23] argument to make here, too: If law enforcement used facial recognition to come up with 75 potential matches for an unidentified suspect's face, the accused, under *Brady*, has the right to know about the other 74 potential matches that the system thought looked like the face in the "probe" or "source" photo as potentially exculpatory evidence. The prosecution should not be permitted to circumvent this by simply saying the technology was used only for lead generation purposes.

Relatedly, OSTP must require that when any biometric technology is used to investigate the accused, that individual has a right to fully examine the technology so they may determine whether it in fact does what the government claims. For this purpose, the accused may require and must be permitted the assistance of relevant experts. Currently, the private companies that design these algorithms and technologies have successfully hidden their code from public scrutiny by relying on trade secret law and non-disclosure agreements.[24] This "black box" strategy should never have been permitted in the first place; but it cannot continue if biometric surveillance is to be regulated by the federal government.

The constitutional imperative is clear and unavoidable: The accused must be allowed, under discovery rules, to determine how they (and not someone else with similar biometric characteristics) were identified as the suspect that law enforcement ultimately arrested and charged.

C. Validation and standardization

We recognize that OSTP may not be the entity that would ultimately standardize biometric surveillance technologies. But we note that before biometric surveillance tech is federally regulated, there is a prerequisite to determine how it will be assessed. Doing so will better prepare all stakeholders—defense counsel, prosecutors, or computer programmers and private actors who develop the code—to facilitate the inevitable validation hearings that must occur if such technology is going to be relied upon going forward.

Standardization will promote the accused's ability to subject these discriminatory surveillance technologies to *Daubert* or *Frye* evidentiary hearings aimed at determining the

[23] Brady v. Maryland, 373 U.S. 83 (1963) (holding the prosecution must disclose materially exculpatory evidence within their possession to the accused).

[24] NAT'L ASS'N OF CRIM. DEF. LAW., *supra* note 1, at 51-52; *see also* Rebecca Heilweil, *Why We Don't Know As Much As We Should About Police Surveillance Technology*, VOX: RECODE (Feb. 5, 2020, 9:00 AM), https://www.vox.com/recode/2020/2/5/21120404/police-departments-artificial-intelligence-public-records.

technology's reliability and validity. Rather than allowing companies to dictate standards through product development or allowing law enforcement agencies to determine for themselves how much of a match is adequate before pursuing a suspect, there must be some established minimum requirements for every biometric technology. Without any form of standardization for these complex technologies, there is no way defense counsel can properly assess or validate them. Such standardization will further defense attorneys' abilities to subject these technologies to validation hearings and ultimately determine whether they have any place within the criminal legal system.

CONCLUSION

Biometric surveillance technologies provide the government with an unprecedentedly powerful tool. And that tool in the State's hands can be an incredibly dangerous one, especially when it is weaponized against BIPOC communities, already subjected to biased and excessive enforcement at the hands of police.

These biometric surveillance tools do not solve any articulated problems because they were never designed to—they were conceived, coded, and marketed by private companies looking to make a profit by selling or leasing them to law enforcement agencies. They are means without ends, "solutions" without problems. The stakes here are extremely high, and not just for those who may be convicted: The repercussions from an arrest alone can cause someone to lose their job, access to housing, or even custody of their children. Unreliable pseudo-solutions that perpetuate racist police practices should not be mainstreamed.

Rather than trying to find uses for this new technology, the Administration must first identify and understand the problems within the criminal legal system that need solving. Then—and only then—can the Administration begin to select the tools, technological or otherwise, needed to fix them. Going the reverse route, the path that law enforcement is currently on, exacerbates the harmful, racist practices already present in the criminal legal system. The Administration should hold off on any endorsement or adoption of biometric surveillance tools.

NACDL recommends that OSTP refrain from promulgating or recommending any biometric surveillance regulations, as these technologies are too powerful and too unreliable. With the understanding that various jurisdictions already use these tools and to the extent that

OSTP ultimately does promulgate regulations, it is crucial that some critical requirements be met before any wider rollout is considered.

First, biometric identification methods should never be the sole basis to search or arrest someone.

Second, defense lawyers must be given notice of any technology that was part of the investigation process. Additionally, defense lawyers must be afforded the opportunity to examine the technology to assess any potential flaws and have access to other potential candidates that the technology identified who may provide exculpatory evidence. The prosecution and the companies that design these algorithms cannot be permitted to hide behind intellectual property law when life and liberty are at stake.

Finally, biometric surveillance methods must be sufficiently standardized so that proper validation hearings may be held. Only after standardization will it be possible for peer-reviewed studies to determine key metrics, such as the technology's reliability and error rates. These factors are essential for *Daubert* and *Frye* hearings and central to the accused's due process rights.