NACDL
FOURTH
AMENDMENT
CENTER

March 8, 2024

Testimony of Clare Garvie
Training & Resource Counsel, Fourth Amendment Center
National Association of Criminal Defense Lawyers (NACDL)

Before the U.S. Commission on Civil Rights
Hearing on Civil Rights Implications of the Federal Use of Facial Recognition Technology

Commissioners Garza, Nourse, Gilchrist, and Adams, thank you for inviting me to testify. My name is Clare Garvie. I work with the Fourth Amendment Center at the National Association of Criminal Defense Lawyers (NACDL), which offers training and direct assistance to defense lawyers handling cases involving new surveillance tools, technologies, and tactics that infringe on the constitutional rights and liberties of people in the United States.[1] I am honored to be a part of this hearing dedicated to examining the civil rights implications of facial recognition technology, both in the criminal legal system and beyond.

I want to take this opportunity to highlight two key points relating to the use of facial recognition technology in the criminal legal system that intersect with the Commission's mandate to inform civil rights policy, enhance enforcement of federal civil rights laws, and investigate discrimination in the administration of justice.

First, facial recognition technology risks entrenching historical racial biases in the criminal legal system based on several interrelated factors: the disproportionate use of the technology in communities of color, an extension of historical over-policing; the disproportionate enrollment of people of color—particularly Black men—in facial recognition databases through reliance on mugshot databases that reflect both the legacy and ongoing reality of over-policing; and the demographically-based differential error rates that the technology continues to exhibit. Second, current police use of facial recognition lacks scientific validity. This, paired with a systematic lack of transparency around where, when, and how it is used, perpetuates due process violations that have and will continue to disproportionately impact those over-represented in the criminal legal system—communities of color and low-income individuals, particularly indigent defendants.

[1] Fourth Amendment Center, NACDL, https://www.nacdl.org/Landing/FourthAmendmentCenter.

Facial recognition represents just one of many automated tools adopted into current policing practices, one that has been employed for more than twenty years. The DOJ, and the legislative and regulatory bodies that inform its actions, should consider facial recognition a test case—and a cautionary tale—when considering the regulation and appropriate use of other automated and AI-based techniques. This should include an analysis about whether a given tool has any place in policing, or whether a ban is appropriate in the interest of protecting civil rights and liberties.[2]

1. New tools, old biases: Facial recognition entrenches and exacerbates patterns of over-policing.

Facial recognition systems risk entrenching historical patterns of over-policing Black and Brown communities in several ways.[3] First, as either a surveillance or investigative tool, we expect police facial recognition deployments to parallel existing patrol, investigation, and arrest patterns.[4] Some of the most controversial, high-risk pilot facial surveillance programs have occurred in cities with non-White populations well above the national average.[5] Facial recognition has been used to investigate events during Black Lives Matter protests; several federal agencies used facial recognition to investigate incidents that occurred during

[2] *See Resolution on Facial Recognition Technology*, NACDL (Oct. 23,2023), *available at* https://www.nacdl.org/Content/NACDL-Facial-Recognition-Resolution,-4AC-Draft ("…be it resolved that NACDL opposes the use of facial recognition technology as a police investigative tool, and believes that facial recognition should never be used for remote biometric surveillance including but not limited to in conjunction with body camera devices." *See Comments to DOJ on Policing Technologies in Executive Order 14074*, NACDL (Jan. 19, 2024), https://www.nacdl.org/Document/CommentsDOJPolicingTechnologiesEO14074-01192024.

[3] *See generally*, *NACDL Comment to Office of Science and Technology Policy*, NACDL (Jan. 15, 2022), https://www.nacdl.org/getattachment/d0b14369-8e40-444f-8f95-3335b7acc6a6/nacdl-comments-to-the-office-of-science-and-technology-policy-on-biometric-technologies-january-2022.pdf. Moreover, these factors all create a 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." *Id.* at 4.

[4] Both quantitative and qualitative studies support the assertion that race impacts policing in the U.S. For example, one study found that Black drivers are vastly more likely to be both stopped and searched than White drivers, even though Black drivers are both a smaller proportion of overall drivers and the likelihood of finding contraband was nearly equal across races. *See* George E. Higgins, et al, *The Impact of Race on Police Decision to Search During A Traffic Stop: A Facial Concerns Theory Perspective*, Journal of Contemporary Criminal Justice Vol. 28, Issue 2, 166–183 (May 2012), *available at* https://journals.sagepub.com/doi/epub/10.1177/1043986211425725. *See* Tammy Rinehart Kochel et al., *Effect of Suspect Race on Officers' Arrest Decisions*, Criminology Vol. 49, No. 2, 473–512 (2011), *available at* https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1745-9125.2011.00230.x. Pew Research reports that Black adults, particularly Black men, are about five more times likely than White adults to report being unfairly stopped by police because of their race or ethnicity. *See* Drew Desilver et al., *10 things we know about race and policing in the U.S.*, Pew research Center (June 3, 2020), https://www.pewresearch.org/short-reads/2020/06/03/10-things-we-know-about-race-and-policing-in-the-u-s/.

[5] Detroit, Chicago, Washington, D.C., and New York City all piloted real-time facial surveillance programs. *See* Clare Garvie and Laura Moy, *America Under Watch: Face Surveillance in the United States*, Georgetown Law Center on Privacy & Technology (May 16, 2019), https://www.americaunderwatch.com/.

demonstrations after George Floyd was killed in 2020 at the hands of a police officer.[6] In a rare audit of police facial recognition and automated license plate reader (ALPR) use, one city found that "people of color were between 1.5 and 2.5 times more likely to be targeted than expected by [their] presence in [the] population." The audit also found that of the women targeted, 15% were identified and tracked "for voyeuristic reasons" and "65% of teenagers [were] targeted for no reason."[7]

Second, and related, many police facial recognition systems run against arrest databases. This is the case for the FBI's Next Generation Identification Interstate Photo System (NGI IPS), composed of 30 million mugshot photos.[8] These databases reflect and carry forward the racial and other biases present in both historic and current arrest rates.[9] In 2019, the most recent year for which Uniform Crime Reporting statistics are available, Black or African American people accounted for 26.6% of all arrests, despite comprising just 13.4% of the U.S. population at the same time.[10] Who is in a facial recognition database matters; a system cannot make an identification—or misidentification—to someone not in the database.[11]

Finally, facial recognition introduces a unique additional racial bias concern. Facial recognition algorithms continue to perform differently—that is, either more or less accurately—depending on the race, sex, and/or age of the person being searched. These accuracy differentials place certain people at a higher risk of misidentification—and consequentially investigation, arrest, and criminal charges—because of who they are and what they look like.[12]

[6] *See* Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks, GAO, 17 (June 2021), https://www.gao.gov/assets/gao-21-518.pdf ("Six agencies reported using facial recognition technology during May through August 2020 to support criminal investigations related to civil unrest, riots, or protests …. Six agencies told us that they used images from these events to conduct facial recognition searches during May through August 2020 in order to assist with criminal investigations.").

[7] *See San Diego's Privacy Policy Development, Efforts & Lessons Learned*, Automated Regional Justice Information System, 11 (date unknown), *available at* https://voiceofsandiego.org/wp-content/uploads/2021/04/E5-Meaningful-Metrics-1-1.pdf.

[8] *Face/Interstate Photo System*, FBI, https://fbibiospecs.fbi.gov/biometric-modalities-1/face (last viewed Feb. 22, 2024).

[9] For a more in-depth discussion of this, *see* Clare Garvie, Alvaro Bedoya, Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy & Technology (Oct. 18, 2016), https://www.perpetuallineup.org/findings/racial-bias.

[10] *2019 Crime in the United States Table 43A*, FBI: UCR, https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/tables/table-43 (last viewed Feb. 22, 2024).

[11] The solution is not necessarily to enroll all driver's licenses or other more representative databases into a facial recognition program, something that many jurisdictions have done. This may help eliminate racial bias in the system but increases the scope of police access to biometric data far beyond what most states, and the federal government, expressly allow by law. *See, supra* note 9, https://www.perpetuallineup.org/findings/deployment.

[12] *See Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, National Academies of Sciences (NAS) (Jan. 2024), https://nap.nationalacademies.org/catalog/27397/facial-recognition-technology-current-capabilities-future-prospects-and-governance; *see* Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280*, NIST (Dec. 2019), https://doi.org/10.6028/NIST.IR.8280; *see* Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, IEEE Transactions on Biometrics, Behavior, and Identity Science (Feb. 2019), https://mdtf.org/publications/demographic-effects-image-

A National Academies of Sciences report, commissioned by the DHS Science & Technology Directorate and the FBI and published in January of this year, examines this issue in detail, summarizing a growing body of literature from the National Institute of Standards and Technology (NIST), the DHS Maryland Test Facility (MdTF), and various academic and other sources.[13] According to the authors:

> "For most algorithms, false positive rates are higher in women than men, also in the very young and old, and in particular ethnic groups. For many algorithms, these groups are Africans, African Americans, East Asians, and South Asians …. False positive rates can vary massively across groups; the ratio can be one, two, or three orders of magnitude in some demographic groups versus others; this depends strongly on the algorithm and the groups being recognized."[14]

The report cautions that these types of errors will be more common in "one-to-many" searches of large databases, precisely the conditions under which law enforcement investigative searches are run.[15]

The risk that a police facial recognition search misidentifies someone is not an abstract one. At least seven people have been wrongfully arrested because a facial recognition misidentification. Nijeer Parks of New Jersey; Michael Oliver, Robert Julian-Borchak Williams, and Porcha Woodruff of Michigan; Alonzo Sawyer of Maryland; Randal Quran Reid of Georgia; and Harvey Murphy Jr. of Texas all spent time in jail and lost wages or employment, experienced physical and psychological trauma, incurred legal fees, and suffered other negative impacts stemming directly from an algorithmic decision-making process.[16] The racial bias concern is not abstract either. Of the seven people wrongfully arrested, six are Black; five are Black men.[17]

acquisition.pdf; *see* Krishnapriya K. S. et al., *Characterizing the Variability in Face Recognition Accuracy Relative to Race*, 2019 IEEE/ CVF Conference on Computer Vision and Pattern Recognition Workshops, 2278–2285 (2019), doi:10.1109/CVPRW.2019.00281.

[13] *Id.*

[14] *Id.* at 40.

[15] *Id.*

[16] *See* Elisha Anderson, *Controversial Detroit facial recognition got him arrested for a crime he didn't commit*, DETROIT FREE PRESS, July 10, 2020, https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/; *see* Kashmir Hill, *Wrongful Accused by an Algorithm*, NYTIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; *see* Eyal Press, *Does A.I. Lead Police to Ignore Contradictory Evidence,* New Yorker, https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence; *see* Thomas Germain, *Innocent Black Man Jailed After Facial Recognition Got It Wrong, His Lawyer Says*, GIZMODO (Jan. 3, 2023), https://gizmodo.com/facial-recognition-randall-reid-black-man-error-jail-1849944231; *see* Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, NYTIMES (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html; *see* Brian Fun, *Lawsuit: Facial recognition software leads to wrongful arrest of Texas man; he was in Sacramento at time of robbery*, CBS News (Jan. 23, 2024), https://www.cbsnews.com/sacramento/news/texas-macys-sunglass-hut-facial-recognition-software-wrongful-arrest-sacramento-alibi/.

[17] *Id.*

Some proponents of the continued and largely still unregulated police use of facial recognition technology may point out that seven errors in hundreds of thousands of investigations involving a facial recognition search sounds like a low number, an "acceptable" error rate amounting to less than one percent of total investigations. This is a fallacy. For one, the seven known misidentifications likely represent a small fraction of the actual error rates; we have no ground truth data for how often the police facial recognition searches get it right—or wrong. This is particularly true given the rates at which cases plead out and the known risk that people—particularly indigent defendants—plead guilty to crimes they didn't commit to avoid a "trial penalty," the risk of facing exponentially higher sentences should they invoke their right to trial and lose.[18] Perhaps more importantly, however, this is not a laboratory setting, where margins of error may be acceptable; this is our criminal legal system. These are real people whose lives are irreparably harmed by a wrongful arrest.

And while this pattern of misidentification alone should give rise to a civil rights inquiry into how this technology is used across the federal government and beyond, it is not the only risk that facial recognition poses to over-policed communities. Facial recognition affords the State powerful remote, biometric surveillance capabilities which carry significant risks to free speech, expression, association and movement through public spaces.[19] A Privacy Impact Assessment co-authored by representatives from several state and federal agencies including the FBI detailed this risk in report, cautioning:

> "The public could consider the use of facial recognition in the field as a form of surveillance. The potential harm of surveillance comes from its use as a tool of social control. The mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition. These potential consequences of routine surveillance are often referred to as 'chilling effects.'
>
> "The act of identifying individuals raises privacy concerns because it enables surveillance by facilitating the monitoring of a person. As an instrument of surveillance, identification increases the government's power to control individuals' behavior. It can further inhibit one's ability to be anonymous, which is an important right in a free society."[20]

Yet despite this warning, federal agencies have used facial recognition to surveil activities related to Black Lives Matter protests.[21] The City of Detroit briefly paired facial

[18] *See, generally, The Trial Penalty: The Sixth Amendment Right to Trial on the Verge of Extinction and How to Save It,* NACDL (2018), https://www.nacdl.org/getattachment/95b7f0f5-90df-4f9f-9115-520b3f58036a/the-trial-penalty-the-sixth-amendment-right-to-trial-on-the-verge-of-extinction-and-how-to-save-it.pdf.

[19] *See, supra* note 5.

[20] *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field*, Nlets (June 30, 2011), *available at* https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf.

[21] *See, supra* note 6.

surveillance capabilities with Project Green Light, a video monitoring program that included cameras mounted on churches, public housing complexes, women's health clinics, freestanding pharmacies, and more.[22] And while the facial surveillance programs in Detroit and elsewhere have been shuttered in response to public pressure, at the federal level and in most states these types of systems haven't been legislatively banned.

This type of surveillance, and over-policing more generally, negatively impacts affected communities in other ways beyond misidentifications and disproportionate arrest rates. Studies into the impacts of surveillance, stop-and-frisk, proactive policing, and other practices that target certain communities show a measurable, negative impact. Repeat police engagement may increase criminality and subsequent delinquent behavior by breaking trust in the legal system, causing psychological distress and the labeling of a person or a community as "criminal," which is then internalized. Studies on the impacts of enhanced policing of youth show declines in educational outcomes and negative changes in life course trajectories. Facial recognition may well contribute to these harms by exacerbating preexisting policing biases toward Black and Brown communities through disproportionate targeting, database enrollment, and differential error rates.[23]

2. Trust, but don't verify: A lack of scientific validity and transparency perpetrates due process violations.

Police have conducted facial recognition searches in hundreds of thousands of criminal investigations since 2001.[24] Underpinning these searches are two assumptions: a) they are a reliable means of identification; and b) because they generate investigative leads and not probable cause to arrest, there is no requirement to disclose information about the search to the defense. It is a "trust, but don't verify" approach to policing, one which has no place in our criminal legal system.

A. Lack of foundational validity

The way facial recognition searches are conducted in a given police investigation represents a forensic investigative technique whose foundational validity has never been established. In other words, we do not know how reliable—or unreliable—the results of a facial recognition search are.[25] To be sure, there have been numerous studies examining the accuracy

[22] *See, supra* note 5.

[23] This paragraph is taken from a report I authored in 2022 titled *A Forensic Without the Science: Face Recognition Use in U.S. Criminal Investigations*, Georgetown Law Center on Privacy & Technology, 49–50 (Dec. 6, 2022), https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf.

[24] *See id.* at 1.

[25] For a detailed analysis of this assertion, *see id.*

of facial recognition algorithms, most notably those conducted by the National Institute of Standards and Technology (NIST).[26] These and other studies have been used to support the assertion that facial recognition is highly accurate—more accurate even, perhaps, than human facial analysis.

These studies, however, do not reflect the real-world conditions under which police use the technology—conditions that in total have never been evaluated for reliability. In the context of a criminal investigation, a facial recognition search typically involves numerous human steps in addition to the algorithmic search, each of which alone carries risk of error, and may also impact the reliability of subsequent steps, including the algorithm's performance.[27] The quality of the image selected, for example, will directly impact how reliable the subsequent algorithmic search is. And yet the United States lacks any minimum photo quality standards governing what type of images are suitable for facial recognition comparison.[28] Many facial recognition programs allow the analyst running the search to edit the investigative photo prior to submitting it to the algorithm for comparison. This introduces a vast range of variation and the possibility of error that has never been studied.[29]

Systems produce a list of numerous possible "match" candidates for the analyst to review, meaning that a human is responsible for making a final determination about who is identified as the lead suspect in a given investigation. And yet there are no national proficiency tests, standardized training requirements, or certification programs to ensure that this vital aspect of a facial recognition search is reliable.[30] Moreover, these analysts are not shielded from task irrelevant information while conducting their comparisons.[31] As such, cognitive bias, where "humans (1) may tend naturally to focus on similarities between samples and discount differences and (2) may also be influenced by extraneous information and external pressures about the case"[32] should be assumed.[33] The cross-race effect, the documented human tendency to distinguish between faces of people belonging to the same racial group as themselves better than those belonging to different racial groups, may play a biasing role here as well.[34]

[26] *See* Facial Recognition Technology Evaluation (FRTE) 1:N Identification (formerly known as Face Recognition Vendor Test (FRVT)), https://pages.nist.gov/frvt/html/frvt1N.html (last visited Feb. 22, 2024).
[27] *See, supra* note 23 at 9–12.
[28] *See id.* at 34.
[29] *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Georgetown Law Center on Privacy & Technology (May 16, 2019), https://www.flawedfacedata.com/.
[30] *See, supra* note 23 at 22–35.
[31] *Id*.
[32] *Report to the President: Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods,* Executive Office of the President, President's Council of Advisors on Science and Technology, 49 (Sept. 2016), *available at* https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.
[33] *Strengthening Forensic Science in the United States: A Path Forward*, National Research Council, 122 (National Academies Press 2009), http://www.nap.edu/catalog/12589.
[34] *See, supra* note 23 at 36; *see, supra* note 3 at 4–5, 7.

B. Lack of transparency

A common response to concerns regarding the lack of scientific validity is that facial recognition searches produce investigative leads, not probable cause and not evidence to be introduced in court. In theory, police need to conduct further investigation and identify additional sources of evidence that corroborate the facial recognition search results, prior to taking adverse action against an individual.[35] Perhaps because of this posture, the facts of a facial recognition search are frequently *not* disclosed to the defense.[36] In one particularly stark example, in the first fifteen years the Pinellas County Sheriff's Office facial recognition system was in operation, during which the system was searched up to eight thousand times per month, the Public Defender's Office never received information about a facial recognition search as part of discovery or *Brady* disclosure in a criminal case.[37] This may be oversight, or it may be intentional: In a training slide about the Bureau of Detectives facial recognition system, the Chicago Police Department instructed trainees: "Do not let the software become exculpatory evidence."[38]

But being labeled an "investigative lead only" has not prevented officers from relying heavily—or exclusively—on facial recognition search in making an arrest or pairing the search results with additional evidence that is similarly not admissible in court.[39] In the wrongful arrest of Robert Williams in Michigan, for example, officers "corroborated" the facial recognition search results with a non-eyewitness identification. They showed the video of the crime, a robbery at a Shinola store in downtown Detroit, to the loss prevention officer who was not on duty at the time of the robbery and then had her perform a photo array-based identification.[40] In the wrongful arrest of Nijeer Parks in New Jersey, the investigating detective—again not an eyewitness—merely conducted his own visual comparison of the investigative photo, a fraudulent driver's license left at the scene of the crime, and Mr. Parks' booking photo, and determined "it is the same person."[41]

Moreover, the fact that facial recognition search results are labeled investigative leads does not create a de facto legal exemption from disclosure. Under *Brady v. Maryland*,

[35] *See, supra* note 23 at 4–6.

[36] *See, supra* note 3 at 2, describing this and other transparency problems surrounding police facial recognition use.

[37] *See, supra* note 9, https://www.perpetuallineup.org/findings/transparency-accountability.

[38] *Bureau of Detectives Presents Facial Recognition,* Chicago Police Department (date unknown), Document no. 023653 (Center on Privacy & Technology), *available at* https://drive.google.com/file/d/1H8CMe1LEVWyiK0jtdbTLu8A-YTfdUGFl/view?usp=sharing.

[39] *See, supra* note 23 at 68.

[40] *See* Kashmir Hill, *Wrongfully Accused by an Algorithm*, The New York Times (June 4, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[41] Affidavit of Probable Cause, State of New Jersey v. Nijeer Parks, Police Case No. 19010123 (Woodbridge Mun. Ct 2019); *see* Complaint and Demand for Trial by Jury, Nijeer Parks v. John E. McCormack et al, No. 2:21-CV-03021 (Sup. Ct. NJ 2020), *available at* https://int.nyt.com/data/documenttools/new-jersey-facial-recognition-lawsuitnijeer-parks-v/38ff3e74088a95a9/full.pdf.

information must be disclosed if it is material to a person's guilt or punishment. Information about an identification procedure that lacks scientific validity and is prone to cognitive bias would be material to a defendant's claim of innocence and to the defense's ability to impeach witnesses against them. Any failure of the State to disclose this information should be considered a due process violation.[42] As a harm borne principally by criminal defendants, this will disproportionally impact Black and Brown and low-income individuals—particularly indigent defendants.

C. Plea bargaining

This systematic lack of transparency is likely exacerbated by the plea bargaining system. Nearly 98% of criminal convictions come from a plea deal.[43] When a case involves advanced technology that gives rise to protracted conflicts over disclosure, trade secret exemptions, and may involve numerous reliability and other hearings—all while a defendant sits in jail—that defendant faces mounting pressure to plead guilty. In the words of one defense attorney:

> "A lot of individuals are being held in custody and even if they have an attorney who's knowledgeable and picks up on [the technology] right away, they're often sitting in jail when this is going on. There's enormous pressure on them to take a plea to get out of that jail that often trumps any interest in fighting any unfair technology or use.
>
> "These are people who have been taught they're subject to unfairness over and over again. They don't have the ability to walk away from cases when the prosecution doesn't want to disclose; the burden is on an indigent defendant to take a plea deal."[44]

This may happen despite claims of guilt or innocence, or of mitigating factors that would be litigated if a case went to trial. Indeed, at least two of the men wrongfully arrested because of a facial recognition error considered taking a plea deal to get out of jail and avoid the "trial penalty"—the risk of a higher sentence should they have taken their case to court.[45] A press interview with Nijeer Parks contained the following exchange:

> Nijeer Parks: "I knew I didn't do it, but it's like, I got a chance to be home, spending more time with my son, or I got a chance to come home, and he's a grown man and might have his own son."

[42] For more on this argument, *see, supra* note 23 at 41–43.

[43] *See 2023 Plea Bargain Task Force Report urges fairer, more transparent justice system*, *American Bar Association* (Feb. 22, 2023), https://www.americanbar.org/news/abanews/aba-news-archives/2023/02/plea-bargain-task-force/.

[44] This quote comes from an interview I conducted with a defense attorney, name withheld, on Jan. 4, 2024 for *NACDL's Comments to DOJ on Policing Technologies in Executive Order 14074* (Jan. 19, 2023), https://www.nacdl.org/Document/CommentsDOJPolicingTechnologiesEO14074-01192024. Notes on file with author.

[45] *See, supra* note 18.

> Anderson Cooper: "'Cause I think most people think, 'Well, if I didn't commit a crime, there's no way I would accept a plea deal.'"
>
> Nijeer Parks: "You would say that until you're sitting right there."[46]

To be sure, the primary burden of this process rests on the defendant, but the harms extend to the criminal justice system as a whole.[47] When a facial recognition case pleads out, a court never examines the burden of the State under *Brady* to disclose information about how a search is run, never assesses the reliability of evidence produced by a facial recognition system under the *Frye* or *Daubert* standards, never rules on important legal questions surrounding the use of new technologies in the criminal legal system. Instead, we remain stuck in a "trust, but don't verify" approach to new and advanced policing technologies, and due process violations are allowed to persist.

Conclusion

The purpose of this hearing is to examine how facial recognition technology is being used by federal agencies, emerging civil rights concerns, and any safeguards the federal government is implementing to mitigate those civil rights concerns.[48] In addition to being major law enforcement adopters of facial recognition technology, the Commission should consider the role that DOJ and DHS play in promoting state and local adoption and use of the technology, both through federal grant programs and through providing policy and acceptable use guidance that directly implicates civil rights concerns.

DOJ and DHS are currently conducting a study of facial recognition technology and other biometric-based and predictive algorithmic technologies in law enforcement, pursuant to Executive Order 14074 on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety.[49] This report will include "an assessment of how such technologies and algorithms are used, and any privacy, civil rights, civil liberties, accuracy, or disparate impact concerns raised by those technologies…"[50] and recommendations for appropriate use limitations to be adopted by "Federal, State, Tribal, local and territorial law

[46] Anderson Cooper, *Police departments adopting facial recognition tech amid allegations of wrongful arrests*, CBS 60 Minutes (May 16, 2021), https://www.cbsnews.com/news/facial-recognition-60-minutes-2021-05-16/.
[47] *See, generally, supra* note 18. *See, supra* note 43.
[48] *Public Briefing: Civil Rights Implications of the Federal Use of Facial Recognition Technology*, U.S. Commission on Civil Rights (Feb 1. 2024), https://www.usccr.gov/files/2024-02/frt-briefing-save-the-date.pdf.
[49] *Executive Order 14074: Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*, Executive Office of the President (May 25, 2022), *available at* https://www.federalregister.gov/documents/2022/05/31/2022-11810/advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and; Guidance for Written Comments, Department of Justice and Department of Homeland Security, *available at* https://drive.google.com/file/d/1ot3Qew8duPa9ymb8HPyaWKfuapKVZ7OQ/view (last viewed Feb. 22, 2024); *see, supra* note 3.
[50] Executive Order 14074 § 13(e)*, supra* note 49.

enforcement agencies."[51] To the extent that they are concurrent, Commission should be given access to this process to ensure that the policy guidance comports with the Commission's own findings and recommendations on facial recognition technology and civil rights. For any DOJ and DHS guidance published before the finalization of the Commission's report, the Commission should evaluate whether that guidance goes far enough, or allows for continued civil rights harms. Finally, the Commission should remain open to the possibility that the harms outweigh the benefits of continued police use of facial recognition technology, and that a ban may be appropriate.[52]

In addition, while the focus of this hearing is on facial recognition, this technology represents just one of the many automated and AI-based tools increasingly adopted into modern-day policing. Some are new; others, like facial recognition technology, have been in use in a largely unregulated manner for decades.[53] As the Commission investigates and makes recommendations on facial recognition use by DOJ, DHS, and HUD, it should consider the broader applicability of these findings and recommendations to other systems. Like with facial recognition technology, the Commission should consider whether regulation is sufficient, or whether certain tools have no place within our criminal legal system. If we are ever to realize the goals of the Civil Rights Act, we cannot keep waiting twenty years before examining the civil rights implications of advanced policing technologies.

I am grateful for the Committee's attention to these vital issues. Thank you for the opportunity to present this testimony.

[51] Guidance for Written Comments, Department of Justice and Department of Homeland Security, *supra* note 49.
[52] *See, supra* note 3 (recommending that in light of the risks posed by facial recognition and other technologies, "NACDL calls on DOJ and DJS to: 1) carefully consider whether federal law enforcement agencies should use these technologies at all; 2) condition federal funding on strict and expansive validation and disclosure requirements; and 3) increase requirements on companies providing the technology to open their systems to external validation and review by the criminal legal system."
[53] *See, generally,* supra note 9.