

AI IN CRIMINAL INVESTIGATIONS AND PROSECUTIONS

HEARING BEFORE THE SUBCOMMITTEE ON CRIMINAL JUSTICE AND COUNTERTERRORISM OF THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

JANUARY 24, 2024

Serial No. J-118-52

Printed for the use of the Committee on the Judiciary



www.judiciary.senate.gov
www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2025

COMMITTEE ON THE JUDICIARY

RICHARD J. DURBIN, Illinois, *Chair*

SHELDON WHITEHOUSE, Rhode Island	LINDSEY O. GRAHAM, South Carolina,
AMY KLOBUCHAR, Minnesota	<i>Ranking Member</i>
CHRISTOPHER A. COONS, Delaware	CHARLES E. GRASSLEY, Iowa
RICHARD BLUMENTHAL, Connecticut	JOHN CORNYN, Texas
MAZIE K. HIRONO, Hawaii	MICHAEL S. LEE, Utah
CORY A. BOOKER, New Jersey	TED CRUZ, Texas
ALEX PADILLA, California	JOSH HAWLEY, Missouri
JON OSSOFF, Georgia	TOM COTTON, Arkansas
PETER WELCH, Vermont	JOHN KENNEDY, Louisiana
LAPHONZA BUTLER, California	THOM TILLIS, North Carolina
	MARSHA BLACKBURN, Tennessee

JOSEPH ZOGBY, *Majority Staff Director*
KATHERINE NIKAS, *Minority Staff Director*

SUBCOMMITTEE ON CRIMINAL JUSTICE AND COUNTERTERRORISM

CORY A. BOOKER, New Jersey, *Chair*

SHELDON WHITEHOUSE, Rhode Island	TOM COTTON, Arkansas, <i>Ranking Member</i>
AMY KLOBUCHAR, Minnesota	CHARLES E. GRASSLEY, Iowa
CHRISTOPHER A. COONS, Delaware	JOHN CORNYN, Texas
PADILLA, ALEX, California	MICHAEL S. LEE, Utah
OSSOFF, JON, Georgia	TED CRUZ, Texas
LAPHONZA BUTLER, California	JOHN KENNEDY, Louisiana

LYNDA GARCIA, *Democratic Chief Counsel*
DREW HUDSON, *Republican Chief Counsel*

CONTENTS

OPENING STATEMENTS

	Page
Booker, Hon. Cory A.	1
Prepared statement	32
Cotton, Hon. Tom	2

WITNESSES

Aguilar, Armando	5
Prepared statement	35
Responses to written questions	61
Howard, Karen L.	7
Prepared statement	38
Responses to written questions	63
Wexler, Rebecca	9
Prepared statement	54
Questions submitted with no response returned	64

APPENDIX

Items submitted for the record	31
--------------------------------------	----

AI IN CRIMINAL INVESTIGATIONS AND PROSECUTIONS

WEDNESDAY, JANUARY 24, 2024

UNITED STATES SENATE,
SUBCOMMITTEE ON CRIMINAL JUSTICE AND
COUNTERTERRORISM,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:32 p.m., in Room 226, Dirksen Senate Office Building, Hon. Cory A. Booker, Chair of the Subcommittee, presiding.

Present: Senators Booker [presiding], Whitehouse, Padilla, Ossoff, Butler, Cotton, and Kennedy.

OPENING STATEMENT OF HON. CORY A. BOOKER, A U.S. SENATOR FROM THE STATE OF NEW JERSEY

Chair BOOKER. Hello, everybody. I'm excited to see such a crowd, almost standing room only. There's a whole bunch of people waiting outside. I'm not sure if it was because of the rumors that broke out on Twitter that you and I were going to have a cage match.

But in all seriousness, I can't tell you how excited I am being next to Tom Cotton for this hearing because I think as much as Tom Cotton and I have that differs us, we actually both have a lot of the same commitment to community safety. And I think this is a hearing that strikes right to the heart of keeping communities safe and strong. And I'm excited that the two of us are here for this inquiry, really to hear from folks about an issue that is really exciting.

There is much made of technology and its influence on our society. When I was mayor of the city of Newark, the number one issue of my constituents, the pollster that I had and never seen anything like it, was the safety and the security of our neighborhoods and communities. And what was exciting for me is that we introduced a lot of technology as a mechanism with which to keep people safe, technology now that some of our witnesses actually can talk to, like ShotSpotter, and cameras, license plate readers, and more.

And what excites me now is I was a mayor about 11 years ago, which is a long time when it comes to the advancements of technology and innovation. We know that technology in America has so much promise, and in this sphere, it could do a lot. Many people will be stunned to know that our murder clearance rates in the United States is—something where, Chief Aguilar, you can help me out—but somewhere around 50 percent.

Mr. AGUILAR. Correct.

Chair BOOKER. Yeah. It's astonishingly—I think that was a hallelujah that he said there. Amen, Senator Booker—is astonishingly low. And so, one of the things that a lot of people don't realize is that technology could help us on clearance rates. It could help us to create more community trust. It could help us on investigations. It could help us in so many positive ways.

But we also know that technology presents a lot of possibilities to undermine our core values and our ideals as well when it comes to certain constitutional protections, when it comes to privacy, when it comes to some of the most sacrosanct elements of our democracy. And so we know that AI is consequential in our society as a whole in ways that many of us can't fully imagine, both in the possibility in the promise, as well as the potential problems.

When it comes to our criminal justice system, where often a person's liberty and a person's life are at stake, when the safety of their neighborhoods are at stake, where their constitutional protections are at stake is particularly consequential. Law enforcement's use of artificial intelligence technology is not a recent development, again, as all of our experts can attest to.

Its recent expansion raises a lot of questions, as well as raises a lot of excitement for me about the possibilities. And so, I'm going to submit the rest of my opening testimony for the record.

[The prepared statement of Chair Booker appears as a submission for the record.]

Chair BOOKER. But I do want to say to the witnesses that are here, how excited I am. I know you all made sacrifices and took time out. I'm going to introduce you in a moment after my Ranking Member, Senator Cotton, does this opening statement.

But we really are at a point in humanity where every generation has breakthrough technologies that shape and alter the course of humanity. AI is most certainly one of those things, and I know that Senator Cotton and I both are committed to trying to find a way to capture the possibility as well as protect against the risks.

And with that I'm very excited and very grateful to Senator Cotton and his entire team for helping to make this hearing possible. And I will turn the microphone over to him for his opening remarks.

**OPENING STATEMENT OF HON. TOM COTTON,
A U.S. SENATOR FROM THE STATE OF ARKANSAS**

Senator COTTON. Thank you, Senator Booker. I would say that artificial intelligence has gained a lot of attention lately, over the last year and a half or so in particular, but the core technology has been around for some time because of how it's depicted.

Maybe we start with what it's not. Many people, fortunately, most people, don't have much personal interaction with law enforcement or with the criminal justice system. What is AI in law enforcement? It's not RoboCop, it's not the Terminator, it's not the Matrix, not Ultron, it's not even WALL-E. It is never used independent of human decisionmaking in our criminal justice system. That's why it's a tool in the law enforcement toolbox, and it can provide impressive time-saving, and crime-solving, and justice-serving tools.

Just one example. Facial recognition software, for instance, could take a crime scene sketch or a security camera image, and go through thousands and thousands of pictures in a public data base, say a driver's license data base. It can eliminate obvious non-matches. It might be even narrow it down, but then that is a tool that independent human judgment can use to pursue leads. If the early stages of a criminal investigation are like looking for a needle in a haystack, then artificial intelligence, if you will, can provide a magnet for some of our criminal investigators in the police forces around the country.

That's why I want to enter into the record with consent here, a statement from the National Sheriff's Association, Major County Sheriffs of America, and the Major Cities Chief Association. They represent State and local law enforcement all across the country. I want to highlight one particular line from their statement. "It is essential to recognize that AI-powered technology serves as an investigative assistant to law enforcement rather than a replacement for the human element." Mr. Chairman, I ask consent to enter that statement into the record.

Chair BOOKER. Without objection.

Senator COTTON. I also want to give one concrete real-world example of how this can work. Last summer, British authorities contacted the Department of Homeland Security about a video, child sexual exploitation. They had reason to believe it was made in the United States. DHS ran the faces against a mass data base of photos, and they found a match. A college sports administrator in Missouri.

Investigators then found the suspect's Facebook profile and were able to confirm not only that it was the same person, but even that the child victim was on his Facebook page. They eventually got a search warrant from a judge, and in July, they were able to arrest and charge this predator. Without that facial recognition technology, he might be free today, and that child might still be subjected to abuse today as well.

AI-powered law enforcement tools also improve efficiency and save lives in other ways. For instance, by modeling where and when crimes happen, law enforcement agencies can better position limited patrol units to prevent crimes or to respond quickly. They can coordinate with other emergency services like ambulances for better staffing at times and places where there would be needed.

And yet other cases, AI-powered products like those made by Motorola Solutions are used by 911 call centers to clean up, transcribe, and even translate 911 calls in real time, or an AI product made by the company, Axon, is used by law enforcement to quickly blur faces and body cam footage, so police departments can share the footage with the public faster. Other AI-powered tools can analyze financial records to help identify financial crime, and AI-powered cameras can recognize license plates of wanted individuals and alert law enforcement to investigate.

Now, I understand there are some who have concerns about the use of artificial intelligence technology in law enforcement, and those concerns are in some cases valid and should be aired, which I think we'll do today. But I do want to point out that probably the most uncomfortable people with the use of artificial intelligence are

criminals who would like to avoid being caught because, again, artificial intelligence is simply a tool that human investigators, police officers, prosecutors, can use to help solve cases, convict criminals, and put them behind bars.

We need to remember that artificial intelligence-powered law enforcement tools are assistive technologies helping law enforcement officers be better at their jobs, and responsibly used, these technologies can help create a faster, cheaper, more accurate criminal justice system where the criminals are being caught, prosecuted, and victims are being provided justice, and the innocent are not being punished.

I know our witnesses have thoughts and expertise to share on these questions, and I look forward to today's conversation. I do want to say and apologize in advance that since this hearing was scheduled, the Republican Conference has scheduled an all-Republican meeting about the National Security Supplemental Bill that is currently under debate. So, I may not make it to the end, but I assure you it has nothing to do with your testimony. Thank you—all.

Chair BOOKER. Senator Cotton, thank you for those excellent remarks. You went through an array of movies there from WALL-E to Terminator. Were those recommendations, or did your staff sort of put them in?

[Laughter.]

Chair BOOKER. All right. I am excited that what I'm going to do now is introduce all the witnesses, and then I'm going to ask you to stand up, and raise your right hand, and swear an oath. We prefer you not to swear at us, but just swear the oath, and then we'll go and open it up for your testimony in alphabetical order.

So, I'm going to introduce really quickly the Assistant Chief of Police, Armando Aguilar, from the city of Miami Department and Law Enforcement Subcommittee Member of the National Artificial Intelligence Advisory Committee. Assistant Chief Aguilar is assistant chief of police for the city of Miami Police Department, which is having some extraordinary success in protecting citizens and keeping their community safe.

In 2022, you began serving as a member of the Law Enforcement Subcommittee of the National Artificial Intelligence Advisory Committee, which advises the President of the United States on matters related to the use of AI in law enforcement. As assistant chief of police, you oversee hundreds of sworn and civilian employees, and you've held many senior management positions in all divisions of the Miami Police Department.

During your time with MPD, you have implemented offender-focused strategies that have contributed to significant reductions in violent crime and significant increases in clearance rates. You hold a master in public administration from Barry University, and a bachelor's of criminal justice from Saint Leo University. It's really an honor to have you here, and we're very, very grateful.

I want to next introduce Dr. Karen Howard, Ph.D. Dr. Howard works with the U.S. Government Accountability Office, or GAO, as acting chief scientist, a role that she held from Jan.–Oct. 2023, and a director of the GAO Science, Technology Assessment, and Analytics Team, STAA. You manage a broad portfolio of topics, frankly,

an impressive portfolio of topics, including forensic algorithms, biological threats, chemical weapons, national security implications of emerging technologies, and other issues. It's pretty extraordinary the work you do.

You've produced key GAO reports that you're going to testify about, including forensic technology algorithms used in Federal law enforcement, and Forensic Technology: Algorithms Strengthen Forensic Analysis, but Several Factors Can Affect Outcomes. You've earned your Ph.D. in environmental chemistry and your master's degree in analytical chemistry. You are, as my dad would say, you have more degrees than the month of July, and it's great to have you here. And thank you for, again, flying up from Alabama as well.

It's difficult for me, Professor Wexler, you have so much Berkeley on your resume. As a Stanford man, I'm going to try to muscle my way through this. Okay. You are assistant professor of law at the University of Berkeley School of Law and faculty co-director. You're the co-director for the Berkeley Center of Law and Technology.

Professor Wexler is a faculty co-director of the Berkeley Center for Law and Technology, and assistant professor of law at UC, Berkeley. Your teaching and research focus on data technology and secrecy in the criminal legal system. Your scholarship has appeared in so many places; the Harvard Law Review, Stanford Law Review, Yale Law Journal Forum, NYU Law Review, UCLA Law Review, Texas Law Review, Vanderbilt Law Review, Berkeley Technology Law Review. I would criticize you because nothing in Arkansas. You need to correct for that.

Professor Wexler served as Senior Policy Advisor for Science and Justice at the White House Office of Science and Technology during the spring of 2023, and as the James C. Carpenter visiting professor at Columbia Law School. You've got your JD from Yale, MPhil from Cambridge as a Gates Scholar, and you are summa cum laude at Harvard. And again, we thank you for flying in all the way from California. Would the three witnesses please stand up and raise your right hand?

[Witnesses are sworn in.]

Chair BOOKER. Let the record show that each witness has answered in the affirmative. You may sit down, unless you want to stand for the hearing, which of course we have no preference. You each will now have 5 minutes for your opening statement. And again, we're going to start with an alphabetical order with Chief Aguilar.

STATEMENT OF MR. ARMANDO AGUILAR, ASSISTANT CHIEF OF POLICE, MIAMI POLICE DEPARTMENT, MIAMI, FLORIDA

Mr. AGUILAR. Good afternoon, Subcommittee Chair Booker, Ranking Member Cotton, and Subcommittee Members. I'm Armando Aguilar, assistant chief of police at the Miami Police Department, also currently serving a 3-year term as a member of the Law Enforcement Subcommittee of the National Artificial Intelligence Advisor Committee, or NAIAC-LE. I would, however, like to point out that I'm speaking here today on behalf of the Miami Police Department and not on my position on NAIAC-LE.

I'm proud to say that the Miami Police Department story is among the greatest turnaround stories in law enforcement. In 1980, Miami with a murder rate comparable to that of Honduras, was America's murder capital. I became a Miami police officer in 2001, and a homicide detective in late 2004; a year when 69 people would be murdered in Miami and another 6,400 would fall victim to violent crime.

By this time, we had the audacity to high-five each other because we were no longer in the top five most violent cities in America. We were, however, perennially on the top 25 list. Fast-forward to 2023, Miami ended the year with 31 murders and 2,600 violent crimes. Thirty one and 2,600 too many still.

Our murder clearance rate, the rate at which cases are solved, was 68 percent, or 97 percent under the FBI's Legacy Reporting System, which counts prior year cases closed during 2023. Our violent crime clearance rate was 58 percent. Now, for most of my career, our murder clearance rate hovered below 45 percent, and our violent crime clearance rate below 38 percent. So, what changed? A great deal.

I'll begin by stating that I've had the pleasure of leading the best generation of officers, detectives, and professional staff to serve the people of Miami, and our success begins with community trust. Violent crime, especially unsolved violent crime, is among the greatest threats which serve to undermine that trust. A shooting takes place, a community member calls in an anonymous tip. The police without any other leads to corroborate the tip, will eventually result in the case going cold. People stop reporting gunfire, the police in turn do not respond to gunfire that we don't know about.

The perception quickly becomes that the police are, at best, unable to keep them safe, or at worst, unwilling to. The Miami Police Department has successfully leveraged artificial intelligence over the past few years to great effect. We use gunshot detection systems, public safety cameras, facial recognition, or FR, video analytics, license plate readers, social media threat monitoring, and mobile data forensics. We use ballistic evidence to connect the dots between shootings and the violent actors that are victimizing our communities.

A recent BJA-funded study by Florida International University, found that violent crimes are one such resource was used by our detectives, had a 66 percent greater likelihood of being solved when compared to similar cases where no such resource was used.

I'm happy to discuss any of the technologies that we employ, but I'm going to take this time to discuss how we came to develop our policy governing the use of FR in criminal investigations. It started in January 2020, when The New York Times ran an article by Kashmir Hill. The article was critical of the use of law enforcement facial recognition, and of one vendor in particular.

Ms. Hill posed several questions which resonated with me as I do spend my time out of uniform as a private citizen. Without proper safeguards, Ms. Hill asked, what would stop police from using FR to identify peaceful protest organizers, or cyberstalking an attractive stranger at a cafe? What about the public whose biometric data that is our faces would be analyzed by police?

So my team and I set out to establish a facial recognition policy that would address these and other concerns. We're not the first law enforcement agency to use facial recognition or to develop FR policy, but we were the first to be this transparent about it. We did not seek to impose our policy on the public, we asked them to help us write it.

We started out by meeting with local privacy advocates. They absolutely hated it, but we wanted to know why they hated it. So they told us. We found that many of their critiques were thoughtful and reasonable. So we heard their objections, took it upon ourselves to treat them as recommendations, and incorporated several of them into our policy.

We highlighted successful arrests aided by FR through local media coverage, and that March, we held two virtual town hall style meetings virtually because in-person meetings were not an option due to the pandemic. One session was conducted in English, the other in Spanish. Each session included public questions and comments, and each session had about 1,300 live views in 3,600 total views.

The policy that resulted from our effort created a narrow framework within which we would use FR. Most importantly, our policy emphasizes that FR matches do not constitute probable cause to arrest. Matches are treated like an anonymous tip, which must be corroborated by physical testimony or circumstantial evidence. We laid out five allowable uses; criminal investigations, internal affairs investigations, identifying cognitively impaired persons, deceased persons, and lawfully detained persons.

We use FR retrospectively, that is, we don't use it in a live or real-time basis to identify persons going about their business in public spaces. And we do not use it to identify persons who are carrying out constitutionally protected activities.

We establish a policy limiting who has access to our FR platforms, and we disclose our FR use to defense counsel in criminal cases. We do not substantively manipulate or alter probe photographs, use composite sketches as probe photographs, or use any other technique which has not been scientifically validated.

These efforts, along with many others, resulted in a Miami that is safer today than in any other time in our history. I thank you for inviting me to speak before the Subcommittee, and I'm happy to answer any questions that you may have.

[The prepared statement of Mr. Aguilar appears as a submission for the record.]

Chair BOOKER. Thank you. That's extraordinary testimony.

I remind the witnesses that Senator Whitehouse and Senator Kennedy are here, so you should be on your best behavior. Dr. Howard.

**STATEMENT OF MS. KAREN L. HOWARD, DIRECTOR;
SCIENCE, TECHNOLOGY ASSESSMENT, AND ANALYTICS,
U.S. GOVERNMENT ACCOUNTABILITY OFFICE,
HUNTSVILLE, ALABAMA**

Dr. HOWARD. Chair Booker, Ranking Member Cotton, and Members of the Subcommittee, I am pleased to be here today to discuss technologies that can assist in criminal investigations.

Criminal justice is an important governmental responsibility with a significant impact on the public. Such investigations should be conducted as quickly and accurately as possible. A number of algorithms can aid investigators in the search for links between individuals and evidence collected at a crime. Some of these tools are enabled by artificial intelligence, while others rely on statistical or automated methods rather than AI.

My testimony today is based on two reports we issued, describing the strengths and limitations of the most common algorithms used for criminal investigations. In our work, we found that Federal law enforcement agencies primarily use three types of algorithms in their investigations; probabilistic genotyping, latent print analysis, and facial recognition.

These algorithms offer some common advantages over human analysts. For example, they dramatically increase the speed of comparisons, allowing larger data bases to be searched in significantly less time. In addition, they generally produce more consistent results because they don't get tired or have an off day as human analysts can. The best of these tools are highly accurate and effective, often more so than a human analyst alone.

However, this is not to say that such algorithms are perfectly accurate or objective. There are hundreds of algorithms in development and on the market, and performance can vary significantly among them as shown in independent testing by the National Institute of Standards and Technology, NIST. Studies have shown that the best results may be obtained from the combination of a highly accurate algorithm and a well-trained analyst.

Despite the advantages offered by high quality algorithms, there are also several challenges to their use. For example, poor quality crime scene evidence can significantly increase the effectiveness of the tools, and experts told us there is considerable variability in the standards for what constitutes suitable evidence quality, especially across the many State and local law enforcement agencies.

Other challenges include errors or improper use by human analysts, unknown and potentially biased training data for AI-based algorithms. The possibility that the correct person isn't in the data base used for comparison. Difficulties with interpreting and explaining the output. Lack of the necessary information for law enforcement agencies to identify the best performing algorithms, and sometimes a lack of resources to purchase those. And a lack of public trust in the results for some algorithms.

We proposed three policy options that may help address these challenges. First, increased training for analysts and investigators, which could improve their understanding of the importance of crime scene evidence quality. Increased training could also reduce errors and inconsistency by human analysts and increase proper interpretation of algorithm results.

Second, policymakers could facilitate the development and adoption of standards for appropriate use, which could set standards for algorithm performance that is acceptable, reduce the use of low-quality evidence, and increase public confidence in the results.

And third, increase transparency regarding the testing, performance, and use of algorithms, which could make it easier for law enforcement entities to identify the best performing technologies, and

improve understanding of the training data for AI-enabled tools, perhaps leading to the development of more robust and representative training data.

Finally, I note that there are many other types of algorithms in development or use beyond the three we examined. Some of these depend on AI to power their comparisons and decisionmaking. In our judgment, the challenges we identified are likely to also be relevant to these other types of algorithms.

In conclusion, we found that probabilistic genotyping, latent print analysis, and facial recognition can be very useful to help investigate crimes, but several challenges may limit their effectiveness. By addressing these challenges, we can improve the accuracy and effectiveness of criminal investigations and enhance public trust.

This concludes my prepared statement, and I would be happy to respond to any questions.

[The prepared statement of Dr. Howard appears as a submission for the record.]

Chair BOOKER. Dr. Howard, I'm really grateful. Professor Wexler.

**STATEMENT OF MS. REBECCA WEXLER,
ASSISTANT PROFESSOR OF LAW,
UC BERKELEY SCHOOL OF LAW,
BERKELEY, CALIFORNIA**

Professor WEXLER. Mr. Chairman, and Members of the Subcommittee, my name is Rebecca Wexler, and I am a co-director of the Berkeley Center for Law and Technology, and an assistant professor of law at Berkeley Law School. I'm honored to testify here today about the need for fair and open proceedings to scrutinize AI tools used in the criminal legal system.

Although AI tools present exciting opportunities to render the legal system more accurate and equitable in some respects, they also present troubling obstacles to fair and open proceedings. To help fix this problem, Congress should do two things. First, require that AI tools used in the criminal legal system be made available for auditing by independent researchers with no stake in the outcome. Second, prohibit either party in a criminal case from invoking the so-called trade secret privilege to block access to relevant evidence, and instead require that such evidence be disclosed under a reasonable protective order.

Zooming out, the U.S. criminal legal system is a model to the world in its commitment to fair and open proceedings to protect against wrongful convictions. That reputation rests on the safeguards we offer those accused of crime, including a fair opportunity to uncover weaknesses in the government's evidence of guilt, and to expose unlawful and unconstitutional police conduct.

This is why the Sixth Amendment guarantees the accused the right to confront witnesses against them, and to compel witnesses in their favor. It's why due process and statutory discovery laws require prosecutors to disclose evidence to the defense. It's why the Supreme Court has directed judges deciding whether to admit scientific and technical evidence, to consider whether the evidence has been subject to peer review. Fair and open proceedings in which evidence is subject to robust and independent adversarial scrutiny

are necessary for accurate, accountable, and legitimate criminal investigations and prosecutions.

These transparency commitments are all the more important in the emerging age of AI because we are together facing a new form of evidence that by its nature, cannot be scrutinized with the tools that parties have traditionally used, such as cross-examination and classic detective work. In turn, allowing AI to enter criminal courtrooms without sufficient scrutiny is dangerous.

While AI has the potential to improve law enforcement efficacy, it can also cause harmful errors with high-stakes consequences for life and liberty. For instance, erroneous AI face recognition hits and gunshot alerts have led to multiple alleged wrongful arrests and imprisonment. A recent study found that state-of-the-art AI photo forensic program, performed worse than regular people with no special training, and two DNA analysis forensic software programs came to divergent results about whether a defendant's DNA was included in a crime scene sample in a homicide case.

We need fair and open proceedings to expose these kinds of costly mistakes and discrepancies. Unfortunately, some vendors block independent review that might expose flaws in their AI products. For instance, consider probabilistic genotyping software, the GAO Office, the PCAST report, and NIST all expressed concern about the lack of independent review of these tools. Yet, when fellow academic researchers and I sought to purchase a research license to study one of them, the vendor, a company called Cybergenetics, told us, "Cybergenetics does not provide research licenses."

Representatives of this company have testified under oath in courts across the country that their product is subject to a peer review process and hence its output should be admissible in criminal cases. But when we actually tried to perform independent research into quality assurance and validation, the company stopped us from doing it.

Congress should require vendors to allow independent audits by clarifying that AI tools used in the criminal legal system must be subject to independent review. There's an important role for Congress here to authorize Federal grants for law enforcement agencies to purchase AI systems only if the vendors make them available for auditing by research groups with no stake in the outcome.

In another obstacle to fair and open proceedings, some vendors have also relied on a so-called trade secret privilege, to refuse to disclose details about how their technologies work to criminal defendants and expert witnesses, even under a protective order, and even in capital cases where the risk of error is wrongful death.

This should not be happening. We need criminal defense counsel and experts, as well as judges and prosecutors, to scrutinize AI systems to ensure accuracy and fairness. There's no good reason for trade secret law to block this crucial process. Once again, there's an important role for Congress to clarify that no trade secret privilege exists in federal criminal cases, and relevant evidence must be disclosed under a protective order.

Thank you for the opportunity to testify here today.

[The prepared statement of Professor Wexler appears as a submission for the record.]

Chair BOOKER. Thank you for the strong testimony. I'm here for the duration, so I'm going to go to Senator Butler. Then we're going to come back and go to the Ranking Member, Cotton. Then we're going to go to Whitehouse, and unless some nobody else comes, I will followup in the end. But we'll go to Senator Butler representing the great State of California.

Senator BUTLER. Thank you, Senator Butler—you can be Senator Butler, too.

Chair BOOKER. Hey, Butler's a kick up.

Senator BUTLER. Senator Booker, thank you so much, and to our Ranking Member for hosting such an important conversation. I will sort of skip the preface and really jump right into what I think is a very important topic to examine. Dr. Howard, if it's okay, I'll start with you, and I'll try to land in my constituents' basket there.

But Dr. Howard, you mentioned in the three recommendations that you would invite Congress to act in this space of increased transparency. I'd like to hear you talk a little bit about what kinds of transparency you think are needed. I'm going to direct this question to Professor Wexler as well, but I'd love to start with you and just sort of hear your thoughts there.

Dr. HOWARD. Certainly, and we, in making our policy options for policymakers, we try not to be too prescriptive—

Senator BUTLER. Sure.

Dr. HOWARD [continuing]. We want to leave room for the policymakers, but some of the things we heard about from experts we spoke with include being transparent about the training data bases. For example; how representative are they? Where are they drawn from? Are they representative of the kind of evidence that might be collected at a crime scene? The sort of print quality that might be expected, or photo quality that might be expected.

Also, increased transparency about whether they've been tested, and how, and what were the results of those tests so that everybody understands how does the algorithm perform under ideal conditions, under less-than-ideal conditions, which are often present in a criminal investigation? And can then make a determination about how much weight to give the evidence that is produced by the algorithm?

Senator BUTLER. And then, Professor Wexler, what would you add to it? I know there are a couple of specific areas that you also recommend increased transparency. You ended your testimony in the space of auditing. What other recommendations would you add there?

Professor WEXLER. Thank you for the question. I would add that the right test is the baseline relevance test. So by default, criminal defense counsel is entitled to discover relevant evidence on a case-by-case basis. That's the threshold that they should have to show in order to get access to any details about evidence used against their client.

What's the problem is when that threshold burden is raised to a necessity burden, for instance, based on some so-called secrecy interest. And the secrecy interest, if it's intellectual property, is not a legitimate one to do that.

Senator BUTLER. So stay, stay there for just 1 second because I did want to talk just a little bit about public defenders. And we all

know, have seen the data, particularly in metropolitan communities around the country, the overworked nature and caseload management of public defenders. You talk a lot about the potential challenges, the need for transparency. Share just a little bit about how the failure to disclose the usage of AI might enter the consideration or the management of the case workload for public defenders.

Professor WEXLER. Sure. So I have two thoughts on this. One is that because AI systems are used across many different cases, even if you have a public defender, or even private defense counsel who's particularly well-resourced, so say in a centralized office that has enough counsel to have specialized counsel focusing on DNA or other forensic technologies, even if disclosure goes just to—if it goes to everybody, but those well-resourced counsel are able to identify flaws or weaknesses in the technology, those identifications benefit everyone as a whole.

So even though not every counsel will have the bandwidth to address it, disclosure is still beneficial. And I can give a concrete example of where disclosure was beneficial in one case, if that would be helpful. The Office of the Chief Medical Examiner of New York City created a forensic software program called FST to analyze DNA evidence. And for years, they refused to disclose source code for that tool, claiming they had a trade secret interest in withholding it.

In one case, they finally were ordered to disclose by Judge Valerie Caponi, former general counsel of the FBI in the Southern District of New York. And the defense expert witness who reviewed it in that case uncovered a undisclosed function that discarded data in certain circumstances, and had been added after the New York State Forensic Science Commission's regulatory approval for the tool. So that discovery happened in an individual case and was beneficial, was useful information for many other defense counsel as well.

Senator BUTLER. Thank you so much, and thank you, Mr. Chair.

Chair BOOKER. Thank you very much, Senator. Ranking Member Tom Cotton.

Senator COTTON. Mr. Aguilar, you mentioned in your opening testimony that tip lines are like Crime Stoppers. You had also said last year in the interview that your department treats facial recognition technology, "like a tip that is called into Crime Stoppers." Is that correct? Do you recall that?

Mr. AGUILAR. Yes, Senator.

Senator COTTON. So in your career as a police officer, have you ever gotten erroneous tips from Crime Stopper hotlines?

Mr. AGUILAR. At least tips that we couldn't corroborate with other evidence. Absolutely, Senator.

Senator COTTON. Okay. Have you ever considered eliminating Crime Stopper hotlines because you get erroneous tips?

Mr. AGUILAR. Absolutely not.

Senator COTTON. Okay. You're not testifying that, say, facial recognition technology or ballistic technology is flawless. Are you?

Mr. AGUILAR. I'm not.

Senator COTTON. Okay. Let's say that you have facial recognition technology, and you run a security camera image through that

technology, and it gives you back seven potential positives. What's the next steps do you take? Do you go out and arrest all seven individuals?

Mr. AGUILAR. Absolutely not, Senator. We would treat the matches as if we had just received seven Crime Stoppers tips, and our detectives would do their due diligence, and either try to discount or corroborate it with other evidence that could tie that person to the crime scene.

Senator COTTON. Using other technology or even artificial intelligence technology or using traditional gumshoe investigative techniques?

Mr. AGUILAR. All of the above, Senator. This is absolutely not a substitute for traditional investigative methods. It compliments traditional investigative methods, but in no way can AI, at least in my view, substitute traditional methods.

Senator COTTON. Okay. What would be the consequence if you did not have this kind of technology in your department?

Mr. AGUILAR. I'm very certain that we would have many more crimes that would go not only unsolved, but there's an additional consequence to having unsolved crimes, and that is, that those criminal suspects are allowed to continue to victimize other people. And so it's not just a lower clearance rate, but it's also a higher victimization rate.

Senator COTTON. Okay. Ms. Wexler, one of your chief points seems to be that the vendors who provide such technology should be compelled to disclose their source code. Is that correct?

Professor WEXLER. If the source code is relevant evidence in a particular case, then that should be the baseline standard, and should be disclosed under a protective order that protects the intellectual property interest to a reasonable degree.

Senator COTTON. Could you give examples, again, of when that would be relevant evidence? Because as Mr. Aguilar said, if you get seven positives from facial recognition technology, that itself is not going to be what cinches is the case, or gets a conviction, or perhaps even admitted into court. It's going to be the follow-on investigative techniques that his detectives use.

Professor WEXLER. Sure. So relevance means any evidence that makes the fact at issue in a case more or less likely than it would be without the evidence. So it's actually a pretty low bar. I tell my students a brick is not a wall. So evidence doesn't have to disprove the whole case in order to be relevant. It just needs to weaken or strengthen one element of it. So any information about how a forensic technology works that could expose unreliability of a particular match would be relevant.

Senator COTTON. Let's use something a little more high tech than, say, facial recognition, which we all engage in every single day, let's say ballistic matching. If you have AI-assisted ballistic matching, is that the source code of that technology that's what's relevant, or is it going to be the human testimony that follows on that, presumably, from dueling witnesses the State uses and that the defense uses? Does the source code matter once you have those dueling witnesses in the follow-on question?

Professor WEXLER. So various aspects of the technology might be relevant in a particular case. A source code might not always be

relevant, but it could be in a particular case. Even if an AI technology is then being reviewed, the conclusions are reviewed by a human witness, the AI results may have bias to the human witness.

So it'd be important to understand if they were flawed. AI results may, in face recognition technology, produce alternate candidate lists that could be exculpatory evidence that would need to be disclosed to the defense. So those are examples.

Senator COTTON. Why do you think these vendors don't want to disclose your source code to you and your fellow law professors or to criminal defense attorneys?

Professor WEXLER. So to be clear, my fellow academic researchers—

Senator COTTON. And you-all wanted a license. Why do they not want to give you a license to use it, and why do they not want to disclose it to criminal defense attorneys?

Professor WEXLER. In my personal view, and of course I don't have insight into their own heads, is that they are concerned about subjecting their products to robust adversarial scrutiny because that scrutiny might expose weaknesses or flaws in their tools.

Senator COTTON. And these products have undergone testing by, say, our own Department of Justice. Haven't they?

Professor WEXLER. Some of the products have undergone testing and some of them less so. So in terms of probabilistic genotyping software programs, again, the GAO Office, NIST, the PCAST report have all identified concern that much of the testing was not performed by independent researchers. And most recently, NIST identified that some of the published validation studies don't have enough publicly available data to be independently verified.

Senator COTTON. Mr. Aguilar, do you have any thoughts on why these vendors might not want to disclose their source code to criminal defense attorneys, or provide research licenses to professors?

Mr. AGUILAR. Senator, I cannot speak for the vendors. I can only imagine that there's at least some concern over intellectual property, but I certainly cannot speak for the vendors.

Senator COTTON. Okay. And Professor Wexler, you keep saying protective order. There, you're talking about disclosure of source code in a criminal proceeding. Right?

Professor WEXLER. It could be disclosure of any aspect of the technology. So vendors, these companies, have actually alleged that trade secret privileges should apply to all sorts of aspects of these tools, including things like user manuals. So, it's not limited to source code.

But I will say that, you know, courts order disclosure of intellectual property under protective orders, reasonable protective orders all the time. It's a common solution in civil cases, and if it's effective there, it should also be deemed sufficient in criminal cases where the stakes are life and liberty.

And I'll add that protective orders give intellectual property holders more safeguards than the non-disclosure orders that companies usually—non-disclosure agreements, I'm sorry, that companies usually disclose the same information under for when they share it with their employees or with business negotiators.

So the protective order, if there were to be a leak, rare instance, there's not evidence that protective orders are generally violated or commonly violated. But in the rare circumstance where that might, happen trade secret holder would still be entitled to sue for misappropriation of their intellectual property.

And on top of that substantive trade secret guarantee, there would be the additional guarantee of criminal or civil contempt of court plus the possibility of disciplinary sanctions if it were an attorney who violated the protective order. So given those safeguards, trade secret law does not provide a good reason to withhold relevant evidence in a criminal case.

Senator COTTON. Mr. Aguilar, in your long history of criminal proceedings, has a protective order ever been violated?

Mr. AGUILAR. No instances come to mind, Senator.

Senator COTTON. Okay. Thank you.

Chair BOOKER. Thank you for that really thorough questioning. Senator Whitehouse.

Senator WHITEHOUSE. Could I ask each of you to consider in the law enforcement arena what you believe to be the most promising use of AI that we in Congress should consider encouraging, and what you consider to be the most dangerous use of AI that we should be more closely monitoring? Just go right across, if you don't mind, Aguilar, to Howard, to Wexler.

Mr. AGUILAR. Senator, it's very difficult to list any one that has the most promise, and I can cite several examples where we've successfully solved everything from violent crimes to property crimes using a number of AI tools. I think that the greatest threat comes in the absence of sound policy, and that applies to any tool that law enforcement uses.

So again, sometimes we may think of AI as something new and a challenge that we've never faced. But the reality is that law enforcement has, for many years, had access to sensitive information through driver's license data bases, criminal records, and it's the policy around those systems that really safeguards the public.

The same can be said for other tools that we use; our weapons, our vehicles. We don't rely on manufacturers to write our deadly force policies or our driving policies. So I think that the absence of policy would pose the greatest threat, and Congress should be looking at a number of AI tools that are right now making our community safer.

Senator WHITEHOUSE. Dr. Howard.

Dr. HOWARD. The only AI-enabled tool that we examined in any detail was facial recognition, but I would say broadly, the most promising AI tools are those that are trained on a reliable and representative data set that is well understood, and that is—

Senator WHITEHOUSE. Like ballistic information?

Dr. HOWARD. We have not studied that one. So I can't affirm that, I'm sorry.

Senator WHITEHOUSE. There's plenty of it though.

Dr. HOWARD. And that also I have a well-trained analyst and investigator using them, because remember, every AI tool is the middle piece of an evidence process. Somebody collects crime scene evidence, prepares it for use, determines whether it's a suitable quality to be inserted into the algorithm, and then assesses the output

that comes out of the other end and decides what to do about it. So that well-trained analyst is key.

The riskiest AI tool would be one where the training data set is not understood, not representative, and it's being handled by somebody who really doesn't understand what the technology is and isn't telling them in the output.

Senator WHITEHOUSE. Thank you. Professor Wexler.

Professor WEXLER. I think that it would be promising for Congress to support AI that is aimed at uncovering exculpatory evidence. One of the concerns that I have about the markets for AI tools is that most of the paying customers are law enforcement, and defense experts and defense investigators don't have the same money to throw at the problem. And this may bias the development of technologies in favor of identifying evidence of guilt rather than identifying evidence of innocence.

So any support Congress could give to AI technologies designed to identify evidence of innocence would be very promising, and my biggest concern are technologies that are kept secret and withheld from adversarial review by the vendors.

Senator WHITEHOUSE. And Mr. Aguilar, you might have mentioned this, but with your experience on law enforcement, have you had occasion to use any kind of AI technologies with ballistics information, with cartridges, spent bullets?

Mr. AGUILAR. Absolutely, Senator. So with our partnership with ATF, we do have an in-house ballistics program, a crime and gun intelligence center. And it's one of many tools that we employ to investigate and prevent violent crimes. It's certainly been helpful.

Senator WHITEHOUSE. Is there an AI component though? Because before there was AI, there were still computer programs that compared, for instance, the markings on an ejected cartridge or the markings on a spent bullet. Two other markings in the same way that fingerprint searches take place. Not so much with modern AI, it's just computer data bases.

Mr. AGUILAR. So our definition of AI sometimes changes. Right? As technology becomes more mainstream, we sometimes think of it as less AI than the newer technologies. But if we look at ballistic evidence where it's compared through an automated system in a data base, and then later it has to be verified by a human analyst, and it makes connections through the automated process that has to later be verified by a human analyst. So in that sense, I certainly consider it AI as it has to be human-verified.

Senator WHITEHOUSE. Thanks very much, Chairman.

Chair BOOKER. Thank you very much. I'm not sure who was here first. Padilla. California is well represented today. Senator Padilla.

Senator PADILLA. Thank you, Mr. Chair. Speaking of California, it was recently reported that a local police department in my State used AI to render a 3D image of a suspect from crime scene data DNA, and then attempted to run that image through facial recognition software in an effort to identify a suspect.

Now, this is the first reported case of law enforcement attempting to use facial recognition technology, which has questions in and of itself, on an AI-generated image. The incident first occurred, actually, in 2020. So it's been a couple of years, but the public did not become aware of it until it was reported this week. There ap-

pears to be a little transparency questions and concerns about how AI tools are being used by police and prosecutors during criminal investigations. And I cited just one example.

First question is for Dr. Howard. What steps should be taken to ensure that defendants and the public are aware of when AI is being used in criminal investigations?

Dr. HOWARD. Part of our policy option calling for transparency would envision a scenario where it is revealed when algorithms have been used in one form or another. And to speak to Mr. Aguilar's point, AI is often what we now think of as automated technologies, was originally considered AI, what most people call AI now is machine learning, which is trained on training data. We believe that transparency step should be known. People should be aware when an algorithm has been used in one form or another as part of the evidence collection and assessment process.

We do believe, however, it's very important to validate the results of those methods. And in this case, the articles that I've read have not indicated whether any validity testing has been conducted on the reconstruction process for the face, and then whether those faces can be reliably run through even the best algorithms. We've not seen any data indicating that those have been tested.

Senator PADILLA. Exactly. So it brings up a whole host of questions. Followup question for Professor Wexler. Welcome from California. How critical is transparency for fostering a positive relationship between citizens and law enforcement for ensuring just results in criminal proceedings?

Professor WEXLER. Transparency is crucial for a positive relationship between citizens, law enforcement, and just results in criminal proceedings. Transparency is one of the key functions of the adversary system. We have an adversary system to enable the criminally accused to scrutinize and contest the evidence against them so that we can ensure that law enforcement's use of that evidence is effective, accountable, and legitimate.

Senator PADILLA. Now, question on a separate topic. Last September, the GAO released a report showing that several Federal law enforcement agencies, including the FBI and DEA among others, did not require their agents to be trained on protecting civil liberties and rights when using facial recognition software.

As I mentioned earlier, facial recognition software begs a whole host of questions in and of itself. But this lack of training is troubling, given that the technology has been shown to produce biased results, particularly when it involves identifying black and brown persons. Back to Dr. Howard, since the release of this publication, have steps been taken to ensure that Federal agents are trained on how to responsibly use facial recognition technology?

Dr. HOWARD. We are not aware of any changes as a result of that report. That doesn't mean they haven't occurred. We just have not been able to followup with the agency to see whether—

Senator PADILLA. So then the bottom-line—

Dr. HOWARD [continuing]. They've been trained.

Senator PADILLA [continuing]. Question is; what recommendations do you have to this committee, to the Senate to Congress, to advance this?

Dr. HOWARD. One important feature of facial recognition is the need to test and verify the accuracy and the demographic bias. And this is one of the things that NIST does in its testing, but NIST does not exhaustively test every algorithm. It tests the algorithms that are submitted to it for testing.

So, one possibility would be to require algorithms to be tested through an independent third party, such as NIST, if they're going to be used for Federal law enforcement purposes, that would add that measure of third-party independent accountability. If you're using the best tools, can an error still occur? Of course. Human beings make lots of errors as well, and many of the most highly publicized errors with forensic algorithm tools have actually been traced back to errors the human analyst made, for instance, submitting evidence that was not of high-enough quality to the algorithm, and the algorithms then unable to give a reliable result.

Senator PADILLA. Right. And you have confidence that NIST or any, whichever Federal entity ends up with this responsibility, has a capacity for determining guidelines for testing and certification of algorithms?

Dr. HOWARD. We've not looked at that directly, but we do know that NIST is often tasked with the job of setting standards for such things and would seem to have the—

Senator PADILLA. That's the flip side. Right? You can do test all you want, but what are you testing for in determining what passes and what doesn't. Okay. Thank you. Thank you, Mr. Chair.

Chair BOOKER. I think when you get two parts, California, one part Georgia, that is New Jersey, but.

[Laughter.]

Chair BOOKER. So with that, Senator, you have to bake at 350 for about 45 minutes. But Senator Ossoff, thank you very much. Please proceed.

Senator OSSOFF. Thank you for convening us, Mr. Chairman, and thank you to our witnesses for your expertise.

Begin with you, please, Professor Wexler, what technologies or practices are being developed, or might need to be developed to make criminal investigations, law enforcement activity, civil litigation resilient against synthetic, fabricated evidence?

There's much discussion about voice cloning and the rapid advance in that technology. You can imagine that being provided by a malicious third party to law enforcement to prompt a criminal investigation of a targeted individual, or other cases where such technology could be used to frame or improperly implicate somebody. How do you protect against that risk, and do you think it's right to think of that as a risk?

Professor WEXLER. Oh, I think it's absolutely a legitimate concern. And it raises the question of whether our current legal system and current evidence rules are up to the task of maintaining accuracy and adversarial review with new technologies like deepfake technologies available.

So when AI-produced evidence or AI-analyzed evidence comes into court, risks of error are present just as they are with human witnesses. And yet, one of the new challenges is that some of the traditional safeguards we have for cross-examining human testimony don't apply to machine-generated outputs. So it's very dif-

ficult to put a AI output on the stand under oath and cross-examine them, and observe their demeanor. That's not going to work.

So the technology, I would say, as a lawyer, that we need to develop to ensure proper safeguards is the legal technology of ensuring we have robust discovery and transparency rules available, perhaps more pretrial testing, access to these technologies for validation and scrutiny rather than simply relying on the current evidence rules as they exist.

Senator OSSOFF. Where AI is used for purposes of investigative analysis, transparency and discovery through the adversarial process could be sufficient. But what about verification? The verification of the veracity or authenticity of evidence that's presented in court?

Professor WEXLER. So for evidence presented in court—

Senator OSSOFF. Or let me say, or if it's presented as a predicate to open a criminal investigation prior to even arriving or perhaps never arriving in court?

Professor WEXLER. Excellent. So, right, as an evidence professor, I always have to tell my students, the evidence rules don't even apply if you never get to court. So what are you going to do? And there I would say, we really need independent researchers with no stake in the outcome to be able to have access to these technologies to test, and scrutinize, and validate them.

And so one of the things that Congress could do here is require or incentivize through the Federal grants program for law enforcement assistance that AI technologies used in the criminal legal system are open to peer review or scrutiny by independent researchers with no stake in the outcome. And that will help with that verification piece, even before we get to trial.

Senator OSSOFF. And thinking about the rules of evidence and discovery, if synthetic and inauthentic evidence were used to open a criminal investigation, and the subsequent progress of the investigation yielded for criminal investigator sufficient evidence to prosecute, and the initial underlying inauthentic and synthetic evidence that was used to justify the progress of the investigation is never presented in court. Would a criminal defendant ever have means of knowing that at the very beginning of the process that led them to this position was something artificial or synthetic?

Professor WEXLER. Under current law, I don't believe there would be a requirement to disclose. There's not a clear path for that, and that's a concern. There's a process called parallel construction where law enforcement may undergo multiple investigations, and present one path toward finding evidence in court and not disclose the other paths. So there may be an opportunity and a role here for Congress to mandate affirmative disclosures of investigative strategies.

Senator OSSOFF. And that's a concern as well, isn't it, where foreign intelligence information may be the root of a criminal investigation, but through parallel construction, sufficient evidence is developed by investigators and prosecutors such that the origins of the investigation being rooted in foreign intelligence is never disclosed to the court or to the defendant.

Professor WEXLER. There certainly are concerns about that. Yes.

Senator OSSOFF. Dr. Howard, any thoughts on verification of evidence? Think about deepfakes voice cloning.

Dr. HOWARD. So we've done limited work on deepfakes. It was not a part of the work I'm testifying about today, but the fact that the current state technology is able to detect deepfakes, it sometimes takes time. It's not necessarily a quick process. And with deepfakes, that can be an issue if something is out in the public and causing harm, and we can't identify it quickly enough.

In the cases you're talking about, criminal investigations can take a long time, prosecution can add time to that as well. So one would hope the technologies would allow us to identify synthetic evidence before it were brought to court, for example, in the case that Professor Wexler might be hypothetically talking about.

But the tools in any kind of a fraud-type scenario, the tools are almost always a step behind the fraudsters. They're creating some new way to do something, and those who are trying to detect it are just a step behind them.

Senator OSSOFF. One more question.

Chair BOOKER. Of course. Go ahead.

Senator OSSOFF. So, or as Professor Wexler noted, the underlying synthetic evidence may never be brought into court, may never be scrutinized, may never be subject to verification. Dr. Howard, is your impression that the technology—have you done any study, do you have a sense of whether the technology for verification, for detection of synthetic evidence such as voice cloning is expected to stay ahead of the capacity for synthesis and production of deepfakes, or are we expecting instead that the apparent authenticity of deepfakes will become so sophisticated, so advanced that it defies verification?

Dr. HOWARD. We don't have any direct evidence either way, but historically speaking, the detection tools are normally just a step behind the new creations of ways to perpetuate fraud. One might assume the same would occur here, but we have no evidence of that in either direction. We don't see any evidence at the current time of something being created that's totally undetectable. It just may take time.

Senator OSSOFF. Thank you. Thank you, Dr. Howard. Thank you—all.

Chair BOOKER. Thank you very much. Professor Wexler, I really do question whether Senator Cotton has seen WALL-E. But otherwise, I actually think he's a really intellectually rigorous—and I don't always agree with his conclusions, but he's an intellectually honest person, and I think where he was going is really substantive, which is this idea of somehow the AI technology companies that we're talking about, that you rightfully asked for, you know, adversarial scrutiny, peer reviews, and how urgent it is for us to get over this trade secret privilege.

I guess the concern that, I think, that he was getting at was that those companies do have a legitimate—and again, might be cynical to say that they're just interested in being able to continue to sell their product. But you had some good retort for the idea, and I want to scratch it a little bit more, that those companies get more protection by opening themselves up to that scrutiny. Could you just explain that to me a little bit more?

Professor WEXLER. Sure. Absolutely. So substantive trade, secret law is a body of intellectual property that creates a negotiation between the public interest in accessing information and the goal of incentivizing innovation by providing property rights to the owner. And so there are limitations all the time to substantive property rights. Patent law has an expiration date, and trade secret law has some limitations as well that are part of that policy balance. The limitation of trade secret law is that you only get a right against misappropriators, which is wrongful acquisition, use, or disclosure.

And my position is that cross-examination in court is not misappropriation. So the only time the intellectual property interest would kick in is if somehow a protective order, if information's properly disclosed under the protective order subject to cross-examination for purposes of a criminal case, that limited case, could be attorney's eyes only, expertise only. The only reason that a company might have a legitimate concern is if that protective order might leak.

And what I was trying to explain, and I'm happy to have another opportunity to elaborate, thank you, is that in that unlikely event, and there's not evidence that this happens regularly, in the unlikely event that a trade secret were to leak when it was subject to a protective order, all of the substantive trade secret protections are still available to the intellectual property owner. They can sue for misappropriation, and yet, there's even more safeguards than normally occur outside of court because you have criminal contempt of court charges.

Chair BOOKER. Okay. So I understand that, and that's really, I think, a substantive point. And so to the extent you can, the only jeopardy there is you don't see any real business pecuniary jeopardy to that person exposing their algorithms or their processes to peer review. You really can't think of any other business threat to them because, clearly, they're getting some additional safeguards. Is that what you're saying?

Professor WEXLER. Correct. There's no legitimate business concern with disclosing the information for cross-examination under protective order for the limited purpose of ensuring accuracy in a criminal case.

Chair BOOKER. And then what about a prosecutorial concern? In all sincerity, could there be a concern amongst the prosecutors?

Professor WEXLER. I believe that the trade secret privilege should not be available to either party to claim in a criminal case, so that this would be a parallel and equal requirement of disclosure.

Chair BOOKER. Okay. Let me take off my Senator Cotton hat. He does a much better job at being Senator Cotton than I do. Although I can ask the staff, maybe, am I stepping up to the plate?

And now let me ask one of my concerns, which is 98 percent of criminal convictions is done during plea bargaining and has nothing to do with trial. And I'm wondering about this element that you said where—and Senator Cotton did a good job, I think, also of bringing out this fact that as Chief Aguilar said that, well, the AI gets me to a point, but my analysts, and my experts, and my good gumshoe police work—I need to know where that gumshoe, like, where does that come from? Is there really gums on their shoes. Explain this to me someday, please. But that it really is not—I'm

not relying solely on the technology. This has now been reviewed by expert human witnesses. So that renders your desire to break open my algorithm and all of that moot, because now it only led me to knowing it's one of seven people. Why should I be subject to that kind of scrutiny now?

Professor WEXLER. Great. So I have two responses. The first is to say defendants or prosecutors are only entitled to discover relevant evidence. So if information truly is moot, in other words, there's no possible way that disclosing the information could render a fact at issue, more or less likely than it would be without it, it's not discoverable. It's already protected. You don't get it. So we're only talking about relevant information.

Now, my second point is there may be all sorts of circumstances where it could be relevant to discover information about the algorithm, despite the fact that a human has reviewed it after the fact. And I certainly can't anticipate all those circumstances on a case-by-case basis, but I can think of a few.

An example would be if the algorithm, say a face recognition system, were known to the analyst who's reviewing it, and potentially biased to that analyst to have overconfidence in their conclusion, you'd want to know then whether it was overconfidence, how good was that algorithm? Were they right to trust it so much?

Another example might be that the algorithm could have produced alternate exculpatory information that wasn't disclosed by the human analyst because it didn't fit with the analyst's own conclusions. And that could help as well.

Chair BOOKER. A brilliant point. And so the last thing I would ask you is you said you give your law students this, "the brick is not the wall." Can you explain that to me again? Because I went to Yale Law School, as you know, that's an inferior law school compared to Boalt, but go ahead.

Professor WEXLER. Yes, thank you. You know, I don't even know where the phrase comes from, but a brick is not a wall means relevance is a relatively low bar. It doesn't mean nothing, but it's not an onerous threshold like showing that this piece of evidence is going to prove your whole case, no. It just means you get information, and you get to introduce it in court if it will make a fact, an issue ever so slightly more or less probable. And then with all those individual pieces of information, all those little bricks that are each relevant on their own, you build a case.

Chair BOOKER. Right. And then finally, there's this big—there's a great book "Why Innocent People Plead Guilty." Because they face such an enormous stacking of criminal charges and the enormity of it all. And I guess we could imagine a situation where a prosecutor is sitting there saying, "Take this deal. We'll give you 5 years, or else you're going to face 50, because we've got this evidence based upon AI." That's a very intimidating moment for an overworked—as one of my colleagues was saying—defense attorney. Is that a concern of yours?

Professor WEXLER. Absolutely a concern. I absolutely agree. And I'll just add to this concern that many indigent defense counsel may not have the resources to challenge the AI, but also individual defendants might—the cost of fighting the case, even when they maintain their innocence, could be so great; the risk of losing your

job, risk, of losing custody of your children, your home that it is perfectly rational to plead guilty even when you haven't committed the crime.

Chair BOOKER. All right. Chief Aguilar, it's interesting as an African American living in an African American community that's highly impacted by crime, that you have these two dueling reactions. One is you see how unfair the criminal justice system is. You know, I grew up in a predominantly white area, went to Stanford, Yale, saw lots of drug use, the enforcement of which was nil to nothing. But in communities of color like mine, you see a tremendous amount of drug use.

And then on the flip side, you see all these crimes, as you were eloquently putting, that are going on your neighborhood that aren't being solved. So you have this almost double down discontent with your public safety, and that's a problem. There's one great criminal justice writer that said that black communities have too much of the policing they don't want, and not enough of the policing that they need in terms of, as we said, the closeout rates of murders, and shootings, and the like.

But your story's extraordinary. So I'm so excited that you came as a witness today because you are working so hard to restore that trust within communities and that technology, and I saw this where the ACLU was dead set against me using a camera technology and ShotSpotters.

We invited them in to help us write the operating procedures, and then how much my community wanted this technology being used on their streets because, like, you don't live here. We want cameras on our streets and the like. So I guess this tension that I've lived my life is something you struggle with every day. And technology brings a whole new era of challenges to something that's so important for law enforcement, which is police community trust.

And so I'm hoping with that context, could you sort of tell me what your hope is amidst this for restoring the kind of trust needed for communities to be safe? And then, what is the excitement that you have as you see the future of this technology to even better help the most impacted communities have the kind of safety and security every community deserves?

Mr. AGUILAR. So, Senator, to your point. Absolutely. You know, we know that, at least through my experience, in the communities that are the most affected by gun violence, I have never heard anyone in those communities say we need less of this. They want everything that we can throw at the problem so that their children stop dying. Right. That's the overriding concern in the communities that are most affected by gun violence.

And so what I've found is that these tools have helped us hone in on those people that are the drivers of repeat gun violence. We know through numerous studies that it's usually about 5 percent of our gun offenders that are driving 50 percent of the shootings. So AI has given us the opportunity, along with traditional policing methods, where we employ micro hotspot policing, where we focus on repeat offenders.

We saw, for example, a disturbing trend in some domestic homicide cases where those incidents were preceded not by felony inci-

dents of domestic violence, but by misdemeanors that perhaps we couldn't get to quick enough. And so we found a way to identify those people that were repeat offenders for domestic violence, that we're also carrying out other crimes to where when we're talking about carrying out enforcement that's preventative in nature, we're not targeting and entire communities so much as we're targeting those 5 percent of the offenders and 5 percent of locations that drive 50 percent of our violent crime.

So I think that numerous studies have also shown that the more police officers we have out there, the more resources, human resources, the more positive our impact on crime rates. But it goes beyond that. Right. We have to just also embrace a lot of these technologies that help us focus on the right people that are driving violence in our communities.

Chair BOOKER. And technology's clearly a force multiplier. It allows one individual to do a lot more work a lot more quickly, and you've been a homicide investigator so you understand that. Yes?

Mr. AGUILAR. These technologies can cut out hours, even weeks' worth, of time in certain instances where we're talking video analytics, where we can get several weeks' worth of footage and be able to compress it to those points that are most relevant and of evidentiary value absolutely.

Chair BOOKER. And then, how do you see—is there anything on the frontiers that gets you really excited about where you think policing might be with these tools in 5 years, 10 years from now?

Mr. AGUILAR. I think that a lot of the technologies, just like I mentioned earlier with ballistic evidence to where we sometimes have a hard time considering that artificial intelligence, a lot of these technologies are going to become more mainstream. We use with facial recognition as an example. We use it in our daily lives just to get into our phone several times a day.

And so, I think that these technologies hold a great deal of promise. I think that they become smarter and more accurate with time. We just have to put behind it the responsible policy and the right amount of research. The NIST facial recognition vendor testing, for example, is an excellent resource. If we were to consider—if Congress were to consider Federal funding for some of these technologies, you know, comparing it to sources that are available like the NIST vendor testing, it would be greatly helpful.

Chair BOOKER. What about training and accountability of police officers? I mean, my police union resisted bodycams, and then it shifted really quickly. They appreciated them because for citizen complaints, it was a very good video to have. My former director now thinks bodycams is great for—all that footage is great for training because you can break down officer interactions.

I'm imagining that could be done with AI looking at the volumes and hours and hours looking for certain patterns that might help to create more accountable policing. Have you used it all to hold your police to higher levels of accountability and transparency?

Mr. AGUILAR. So, Senator, to your first point there, there's never enough training. And so, I am always a fan of more and better training. Right now, we are looking into a research partnership to where we will use artificial intelligence to go through those hours

and weeks' worth of bodycam footage to not only highlight problematic behavior, but also commendable behavior.

Chair BOOKER. Yes. You know, I just had a sheriff in New Jersey commit suicide. I have seen officer mental health challenges. I was just talking to a reporter about the Obama's 21st Century Task Force on Policing, and they saw a lot of predictive analytics for officer misconduct. One of them, which is actually doing suicide calls, seemed to be something that would pop up before an officer would have an interaction with a citizen that was negative. And I don't know if that's something you're thinking about how to see how AI might be able to help in that space to anticipate officer behavior who might need more training.

Mr. AGUILAR. Without a doubt, Senator. I think that any technology that'll help us flag problematic behavior—we've seen it. We've seen officers whose careers have come to a very ugly end, right, and they're often preceded by problematic behavior where that officer could have benefited by from early intervention. And so, we as a police department can't correct problematic behavior that we're not aware of. And so, if this technology helps us get there, I'm all for it absolutely.

Chair BOOKER. And so I would imagine—and I'm just on the last question then I'd like to move on to Dr. Howard. I do hear this though still in my community. My young kids are stopped and frisked more than any other community. This doesn't happen in wealthier, whiter communities. Now we're under video surveillance in ways that other communities are not. Now they have facial recognition that we're exposed to more than other communities. You can see how that list can go on, and on, and on, and on, which I wonder if people start to feel like they're under a surveillance state, or feel like they're having their just basic privacies. Could you empathize with that feeling, or is that just not your experience that you're seeing out there at all?

Mr. AGUILAR. So, Senator, I think that right now, video cameras are ubiquitous. I read in one place, I can't remember the exact source, but the United States is second only to China in terms of the number of video cameras that the average citizen encounters every day. The difference of course, being that most of the video cameras that we as Americans encounter are owned by individuals, are owned by the private sector.

And so I think that perhaps in some communities that are more prone to gun violence, where some of the cameras belong to law enforcement versus other communities where they're held by individuals in the private sector. But I do think that right now, being under some form of camera surveillance is just an accepted part of life for all communities throughout the United States.

Chair BOOKER. Thank you. Dr. Howard, I was really appreciative of your sort of best practices, and they resonated with Dr. Wexler in a significant way. And one of the things I think that resonates with Chief Aguilar is just this idea of training. Could you just go another level deeper on that? You said how important it's for analyst training. What does that mean?

Dr. HOWARD. So we know that in order for these tools to be used properly, the analyst decisions before the algorithm comes into play, are critical, and the analyst decisions afterwards. So if we

think about any one of these, if we think about a latent print analysis, for example, just to use a different one, the analyst, somebody in the human chain collects a fingerprint at a crime scene, or from a piece of evidence processes that fingerprint scans it.

It decides whether it's of sufficient quality to even be able to match it to something else, or to attempt to link it to somebody else, marks it up, or has a computer program mark it up on where the key features of this fingerprint that might be worth comparing with a data base, puts it into the algorithm. All the algorithm is doing is comparing it to a data base of prints.

There's nothing magical about that. That's been done for decades on computers before that, on cards stored in files. They would pull out the cards and they would compare each fingerprint. So all the algorithm is doing is speeding up that comparison process. And then at the end, it puts out a candidate list, and that candidate list is nothing more than the top 10, 20, 50, however many the program is designed for, or however many the analyst has asked for of the best matching candidates from the, you know, the best match at the top to the lesser matches as you move down the list.

But that doesn't say anything about the strength of the actual evidence. The person at the top of the list might actually be a lousy match, but it's the best match in the data base, and that's all the algorithm is able to do. If you have a partial print, or a smeared print, or one that's distorted, they may not be able to get a very good match. And if you were putting a percent match on it, which is not what these algorithms do, but if you were doing that, it might say something like 35 percent match, and that's your number one candidate.

Analysts often do not understand that. They often think this is my number one candidate, or these are my top 10. It's got to be one of these people that came up at the top of the list, and in reality, it might be somebody completely different. All the algorithm can do is find the best matches to whatever quality fingerprint they're given, and it has to be somebody who's already in the data base. And obviously, not everybody has their fingerprints in every data base that could be used for comparison. So a lot of human understanding at the beginning about what quality of print is good enough, and human understanding at the end about what do these results really mean.

Chair BOOKER. Right. But variations in training for local police departments could vary widely and end up with widely different results.

Dr. HOWARD. That's absolutely true.

Chair BOOKER. And so that's why one of your recommendations is to have national standards. Right?

Dr. HOWARD. We think national standards would help to drive the conversation if there were standards at the Federal level, or if there were standards that applied to how much is good enough. Right? What quality of print is good enough to put into a latent print algorithm?

Some of those kinds of standards could start to bring more consistency to this and help reduce the potential for well-meaning human investigators who are doing their best to solve a crime, to

be able to use the tools more effectively and interpret the results more efficiently.

Chair BOOKER. Right. And how would you feel, is that overly prescriptive for the Federal Government? Because I'm a big believer having run a local police department, how cash strapped you are, how you're constantly battling for resources. And so things like cops grants and other grants for technology are really critical. But how would you feel if those grants came with a requirement for certain standards for your analysts and the like? Is that overly burdensome?

Mr. AGUILAR. Senator, I think that, you know, it's a bit of a broad question. But I think that just generally speaking, a grant that comes with a requirement that the agency receiving the grant properly train to a particular standard the people who are going to be carrying out the function, I don't think is overly burdensome.

Chair BOOKER. Great. And so Dr. Howard, last question. When you say increased transparency, are you getting at some of the things that Professor Wexler's talking about in terms of the need of opening up these algorithms to peer review and to sort of a more adversarial analysis?

Dr. HOWARD. So we looked at the criminal investigation portion, which I realize feeds into the courtroom, but we did not look at the courtroom processes that might occur. So I want to set the stage with that. But the experts we spoke with indicated that transparency is critical, both in terms of how the algorithm was built, what if it's an AI-enabled algorithm, what training data were used, but also then transparency about has it been tested. What is the accuracy of this through something like the NIST facial recognition vendor testing? What accuracy was determined through that kind of testing? What demographic bias did this algorithm exhibit through that kind of testing? That can be very useful information, and our experts were very much in favor of that.

Opening the source code, though our experts told us it is not necessary. It is a path to figuring out how the algorithm works. It is not the only path in the view of the experts we spoke with. Independent third-party testing can accomplish many of the same things.

Chair BOOKER. And you guys noted in your report that there was a lack of sufficient independent validation.

Dr. HOWARD. That is often true. Yes. The NIST tests which are top of the line, gold standard testing, they are done only if a vendor chooses to submit its algorithm for testing. There's no requirement for a vendor to do that.

Chair BOOKER. And you're saying right now the DOJ, there's a lack—in the DOJ's engagement of this technology right now, there's a lack of sufficient independent sort of oversight.

Dr. HOWARD. So we didn't look at the DOJ in depth in terms of how they validate their algorithms. We did talk to a number of officials at FBI, and they told us—and I believe this is in our report—that they worked with NIST to develop a validation protocol that they then run in-house.

Chair BOOKER. But you haven't evaluated that.

Dr. HOWARD. We have not evaluated it, no. That was not part of the scope of our work. It's work we could do if there was interest.

Chair BOOKER. Well, I have interest, but I can't speak for the DOJ. But if you were to be called upon to do that analysis, one of the things you would be looking at is sort of an independent objective review, a sufficient review of algorithms of the technology itself. Correct?

Dr. HOWARD. Of the algorithm accuracy, demographic bias, features like that.

Chair BOOKER. And what's the danger of perhaps them not having done that right now?

Dr. HOWARD. Then they may not know how effectively their algorithm works, and they may not know that the candidate list they get out could be skewed by, for example, bias-training data that the algorithm was trained on. They just may not be aware of that if they haven't run that test.

Chair BOOKER. Doesn't that set alarms? Should I be writing to the DOJ and saying, "Look, I have legitimate concerns that you have not tested this in a sufficient way."

Dr. HOWARD. I would say any law enforcement entity that's using an algorithm that has not been validated in a form that would be considered defensible should set off alarms. Absolutely.

Chair BOOKER. Okay. And then finally, Ms. Wexler, again, you traveled the farthest and I'm grateful. But I do wonder, you obviously have a lot of concerns in your testimony, but there are also protections that AI tools could use. I always think of these waves of technology as potentially democratizing because you talked about the possible expense of a defense attorney in a situation, but AI might be a tool that defense attorneys could use to help out.

You've done a lot of writing and obviously sit with the technology group at Boalt. Are there some things that give you hope when you look at this technology that you might want to put into the record?

Professor WEXLER. Oh, yes, absolutely. To be clear, my concerns are neutral about the technology itself. I think AI technology is have potential to increase accuracy and efficacy of law enforcement investigations and prosecutions, and also have the potential to help criminal defense investigators identify evidence of innocence.

So the technologies themselves are not the issue. It's the legal rules that we set up around them to help us ensure that they are the best, most accurate, and effective tools, and not flawed or fraudulent in some way.

Chair BOOKER. I just want to say before I give my sort of closing remarks. Number one, I'm just so grateful to Senator Cotton with a lot of demands given some of the international issues that are going on for him to be here and give such, I thought, a really important line of questioning. His partnership is extraordinary.

But I want to thank the three witnesses. It is a frontier that we have that I think it's difficult to anticipate where we will be in 5 years from now, and this technology is really accelerating.

The challenge for government, and I've seen this in waves of innovation, is that we have not moved as fast as the innovations around us. I've seen this in nuclear energy. I've seen this in drone technology. The government has not been able to keep up. Maybe a platform of the substantive accord that we have in a bipartisan way on some of the challenges with social media, for example, is another great example.

You-all are on the cutting edge of looking at this. And it's exciting to me not only to hear your testimony, but to hear what some common-sense precautions could be on a federal level, as well as ways to try to figure out how to advance the technology to the greatest aims of humanity, which is a democratic system that protects the rights of all individuals, including rights to privacy, as well as what I think is a fundamental human right or a freedom that we should have; which is a freedom from fear, a freedom from the kind of depraved criminality that we often see manifesting in communities as well.

This testimony's been rich, both your written testimony and your verbal testimony. It gives me a lot of gratitude. I know that Congress as a whole is looking at AI from every different perspective. This is, from what I know of, the first hearing in the Senate that really is focusing in on. It's affecting the criminal justice system.

My hope is that you-all will be available in the future to consulting with us. There may be some potential for some great bipartisan ideas to come out of this, or at the very least, opening up conversations with some of the key actors in law enforcement on the federal level. I cannot tell you, Chief Aguilar, as a guy who lives in a community that has struggled with a lot of the issues that yours has, the heroic work that you're doing every single day. It's just something that means a lot to me, and I look forward to visiting it hopefully. And the truth of the matter is I'm a little concerned that we'll be confused for each other because we're both—you know, have similar haircuts. But I'm hoping that that won't be the case.

But I want to remind everyone that the Subcommittee questions for the record are due a week from today, Wednesday, January 31 at 5:30 p.m., and I hope that, should there be questions, because again, the Senators have been pulled in so many different directions. My Ranking Member's team might have some questions for the record as well. I hope that you-all after all the sacrifice you made, getting here, preparing written testimony, and testifying, that you will still be able to respond in a timely fashion to any questions that are sent to you.

When you testify before the U.S. Senate, I know how important that is. It may seem like a small Subcommittee hearing, but it is a service to your country, and the work that you-all are doing to me stands in that stead of patriotism, of giving to a nation, helping us to be better. Today was very, very helpful, and I'm grateful to each of you individually for participating and being a part. With that, the Subcommittee is adjourned.

[Whereupon, at 4:02 p.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

A P P E N D I X

Submitted by Senator Booker:

CAIDP—AI and Criminal Prosecution Statement	65
---	----

**Prepared Opening Remarks by Senator Cory Booker of New Jersey
Chair, Subcommittee on Criminal Justice and Counterterrorism
Subcommittee Hearing on AI in Criminal Investigations and Prosecutions
January 24, 2024**

Good afternoon, everyone. Let me start by thanking everyone for joining us today, both in this room and virtually. I want to welcome our witnesses who have journeyed from near and far to be with us. I also want to thank each of my fellow subcommittee members for taking the time to join us today.

I am also particularly grateful to Ranking Member Cotton for working with me to make this hearing a reality.

Once or twice in a generation, a breakthrough technology emerges that fundamentally reshapes our world, redefining the way we live and transcending the boundaries of what we once thought possible.

In our time, artificial intelligence is such a technology.

Artificial intelligence now shapes almost every aspect of our lives: the way we work, the way we learn, and how we communicate. It has permeated nearly every sector of society – from healthcare and education to transportation and science.

Yet, perhaps nowhere is the use of AI more consequential than in the nation's criminal justice system, where a person's life and liberty, and the safety of our communities, are at stake. While law enforcement's use of artificial intelligence technologies is not a recent development, its recent expansion raises important questions about its promise and risk. AI has the potential to enhance community safety, strengthen our communities, and assist law enforcement in solving crime. But, without safeguards, it can also function as a tool of injustice, exacerbating bias and causing harm to our more marginalized communities.

How we—as policymakers and as a society—respond to the use of AI in our criminal justice system will determine the extent to which we fall prey to its risks or capitalize on its promise.

Today's hearing focuses on the use of AI in the initial stage of our legal process—investigations and prosecutions. Advancements in technology for law enforcement hold great promise for transforming the way law enforcement operates, investigates, and promotes public safety. But, without proper safeguards, these technologies pose significant risks and could lead to wrongful arrests and convictions. Our witnesses gathered here today will help us fully understand the full scope of law enforcement's use of AI technologies, the benefits and risks associated with such use, and ways Congress can establish critical safeguards and promote the responsible use of AI in criminal investigations.

While AI tools have the potential to provide significant benefits to our criminal justice system, recent developments highlight serious risks associated with their use.

Law enforcement's growing reliance on facial recognition and biometric technologies has sparked such concerns. A 2021 *New York Times* report highlighted the real-world consequences of the unreliability and inaccuracy of these technologies.

Nijeer Park, a resident of Woodbridge, NJ, was falsely accused of shoplifting and assaulting a police officer based on facial recognition software, despite being 30 miles away at the time. Mr. Park was detained for 10 days in jail before the case was eventually dismissed due to a lack of evidence. Studies, including one by the National Institute of Standards and Technology, show that facial recognition has heightened inaccuracy rates with dark-skinned and Native and Asian American faces.

Part of the problem is the fact that AI technologies do not have minds of their own; they ultimately rely on input data to make decisions. This opens up the inherent risk that the data fed into these systems may carry biases, inaccuracies, or reflect systemic inequalities. If the data used to train AI models is inherently flawed or skewed, it runs the risk of perpetuating and even exacerbating existing societal prejudices.

Additionally, most individuals facing charges in our criminal courts remain unaware that artificial intelligence and automated systems played a role in the investigation of their cases. Prosecutors are not legally obligated to disclose the use of AI algorithms in the investigation or prosecution of those charged with crimes. This raises the unsettling prospect of individuals being convicted based on potentially flawed and invasive technologies without ever knowing, and thus, without the opportunity to challenge them in court. This lack of transparency hinders individuals' ability to make informed decisions about their legal defense and raises serious constitutional and legal concerns.

Yet, the risks of AI in criminal investigations – as real and immediate as they are – should not blind us to some of AI's potential to address crime and enhance the safety of our communities.

This is personal for me. When I was elected Mayor of Newark, I entered office with a clear mandate to confront the escalating wave of violent crime. In 2006, as I stepped into the role of Mayor, our city found itself in the throes of an unprecedented surge in crime. Our officers worked tirelessly to keep our streets safe, but they often found themselves overwhelmed by the sheer volume of cases and evidence that demanded their attention. I learned early on that we needed to harness technology to augment our efforts in ensuring the safety of our residents.

And that's precisely what we did – we introduced cutting-edge technologies not only to enhance our crime prevention efforts but also to allow officers to better allocate resources. It produced results. When I concluded my time as Mayor, crime was at an all-time low.

However, solving crime is not simple. I know this firsthand. I am the only Senator who goes home to a low-income inner-city community grappling with the disproportionate impact of violent crime. What I hear when I'm back home is a collective demand for policing that is not just fair and accountable but also dedicated to actually solving crime.

Our police departments are facing unprecedented challenges in this area. According to the latest FBI data, our national clearance rate has hit an all-time low, hovering just above 50 percent. This means that approximately half of all murders in the United States today go unsolved. It's a tragic reality that disproportionately affects people of color. Both local and national reports reveal that cases involving Black and Hispanic victims remain unsolved at significantly higher rates than those involving white victims.

With the necessary safeguards, AI-driven technologies, including DNA analysis, cutting-edge forensic tools, and advanced data analytics, could potentially assist officers in addressing this crisis.

In closing, let me emphasize again that I do not see this issue as a binary choice. We can embrace the technological advancements of AI in criminal investigations while simultaneously implementing the necessary safeguards to mitigate and prevent harm. Achieving this requires all of us – Republicans and Democrats, law enforcement and civil rights organizations – working together. We must work to fully understand the full range of risks and potential and listen to experts, practitioners, and those directly impacted. Yet, listening alone is not enough. Congress – and this committee, in particular – must also act. Working together, I am confident we can chart a path forward that ensures both greater safety and justice for all.

I look forward to our productive conversation with this extraordinary panel this afternoon. And with that, I will turn to the Ranking Member of the Subcommittee, my colleague from Arkansas, Senator Cotton.

Armando R. Aguilar
Assistant Chief of Police
Miami Police Department
Prepared Remarks – January 24, 2024

Good afternoon, Subcommittee Chair Booker, Ranking Member Cotton, and Subcommittee Members. I am Armando Aguilar, Assistant Chief of Police at the Miami Police Department. I am also currently serving a 3-year term as a member of the Law Enforcement Subcommittee of the National Artificial Intelligence Advisory Committee (NAIAC-LE). I would, however, like to point out that I am speaking today on behalf of the Miami Police Department and not on behalf of NAIAC-LE.

I am proud to say that the Miami Police Department's story is among the greatest turnaround stories in law enforcement. In 1980, Miami was America's murder capital. That year, Miami – with a residential population of under 347,000 – logged 220 murders, a rate comparable to that of Honduras. I became a Miami Police officer in 2001 and a Homicide detective in late 2004, a year when 69 people would be murdered in Miami and another 6,392 would fall victim to violent crime. By this time, we had the audacity to “high five” each other, as we were no longer among the nation's top five most violent cities. We were, though, perennially listed among America's 25 most violent cities. You see, Jack Maple, former Deputy Commissioner at the NYPD once described the story of crime in America as the “story of the 600-pound man”: if he loses 200 pounds and you hadn't seen him in a few years, you would think he looks amazing, but if you hadn't seen him since you were children, you'd be terribly concerned over his wellbeing. There was certainly good reason to be concerned about Miami's wellbeing.

Fast forward to 2023, the City of Miami – with a residential population of over 450,000 – ended the year with 31 murders. Our murder clearance rate (the rate at which cases are solved) was 68 percent, not including an additional 9 prior year murders which were solved that year. Using the legacy summary crime reporting system, which was used by the FBI until very recently, the 9 prior year cases would have boosted our murder clearance rate to 97 percent. Our violent crime clearance rate last year was 58 percent. For most of my career, Miami's murder clearance rate hovered at just below 45 percent, and our violent crime clearance rate, below 38 percent. So what changed? A great deal.

I will begin by stating that I have the pleasure of leading the best generation of officers, detectives, and professional staff to serve people of Miami. Through the years, the members of MPD have built an exceptional degree of trust with the communities we serve. Violent crime – especially unsolved violent crime – is among the greatest threats which serves to undermine that trust. A shooting takes place. A community member calls our anonymous

tip line and gives us the shooter's name. Absent any other evidence to support the tip, the investigation goes cold. People stop reporting gunfire. The police, in turn, do not respond to gunfire we do not know about. The perception among the community is that the police are, at best, unable to keep them safe; or at worst, unwilling to. Artificial intelligence complements, but will never replace, the human interaction which is at the foundation of community-oriented policing.

The Miami Police Department has successfully leveraged artificial intelligence in the past few years, to great effect. We use gunshot detection systems, public safety cameras, facial recognition, video analytics, license plate readers, social media threat monitoring, and mobile data forensics. We use ballistic evidence to connect the dots between shootings and the violent actors victimizing our communities. A recent BJA-funded study by Florida International University found that violent crimes where one such resource was used by our detectives had a 66 percent greater likelihood of being solved when compared against similar cases where no such resource was used. I am happy to discuss any of the technologies we employ, but I am going to take this time to discuss how we came to develop our policy governing the use of FR in criminal investigations.

It started in January 2020, when *The New York Times* ran an article by Kashmir Hill. The article was critical of the use of law enforcement facial recognition and of one vendor, in particular. Ms. Hill posed several questions which resonated with me, as I do spend my time out of uniform as a private citizen. Without proper safeguards in place, Ms. Hill asked, what would stop police from using facial recognition to identify peaceful protest organizers or cyberstalking an attractive stranger at a café? And what about the public, whose biometric data (i.e., our faces), would be analyzed by police? My team and I set out to establish an FR policy that would address these and other concerns. We were not the first law enforcement agency to use facial recognition or to develop FR policy, but we were the first to be completely transparent about it. We did not seek to impose our policy on the public – we asked them to help us write it.

We started out by meeting with local privacy advocates. They hated it. But we wanted to know why they hated it, so they told us. We found many of their critiques to be thoughtful and reasonable, so we heard their objections, took it upon ourselves to treat them as *recommendations*, and incorporated several of them into our policy. We then engaged our local media to cover cases where FR had assisted in solving crimes and to help us spread the word about town hall-style meetings which would be held that March, where we would be soliciting feedback from our stakeholders in finalizing our FR policy. The pandemic would ultimately keep us from hosting in-person town hall meetings, so we instead held them via Facebook Live. We held one session in English; and another, in Spanish, taking public

questions and comment during both. Each session had roughly 1,300 live views and about 3,600 total views.

The policy which resulted from our efforts created a narrow framework within which we would come to use FR. Most importantly, our policy emphasizes that FR matches do not constitute probable cause to arrest. Matches are treated like anonymous tips, which must be corroborated by physical, testimonial, or circumstantial evidence. We laid out five allowable uses: identifying suspects, victims, and witnesses in criminal investigations; identifying principal officers or other persons involved in Internal Affairs investigations; and identifying cognitively impaired persons, deceased persons, persons who are lawfully detained and whose identities cannot be established. We use FR retrospectively, i.e., we do not use it on a "live" or "real time" basis to identify persons going about their business in public spaces, and we do not use it to identify persons who are carrying out constitutionally protected activities. We established a policy limiting who has access to our FR platforms, we disclose our use of FR to defense counsel in criminal cases, and we do not substantively manipulate or alter probe photographs, use composite sketches as probe photographs, or any other technique which has not been scientifically validated.

Our use of FR and artificial intelligence, coupled with our community-oriented policing efforts and our traditional investigative and preventive efforts, has resulted in a Miami that is safer today than in any other time in our history. I thank you for inviting me to speak before the Subcommittee, and I am happy to answer any questions you may have.



United States Government Accountability Office

Testimony
Before the Subcommittee on
Criminal Justice and Counterterrorism,
Committee on the Judiciary, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. ET
Wednesday, January 24, 2024

FORENSIC TECHNOLOGY

Algorithms Offer Benefits for Criminal Investigations, but a Range of Factors Can Affect Outcomes

Statement of Dr. Karen L. Howard,
Director,
Science, Technology Assessment, and Analytics

GAO Highlights

Highlights of [GAO-24-107206](#), a testimony before the Subcommittee on Criminal Justice and Counterterrorism, Committee on the Judiciary, U.S. Senate

Why GAO Did This Study

For more than a century, law enforcement agencies have examined physical evidence to help identify persons of interest, solve cold cases, and find missing or exploited people. Forensic experts are now also using algorithms to partially automate the assessment of evidence collected in a criminal investigation, potentially improving the speed and objectivity of their investigations.

GAO conducted technology assessments on the use of forensic algorithms in law enforcement (GAO-21-435SP and GAO-20-479SP). This statement addresses the benefits and challenges of three algorithm types—probabilistic genotyping, latent print analysis, and facial recognition—along with options policymakers could consider to help address these challenges.

In conducting the prior assessments, GAO interviewed federal officials, select non-federal law enforcement agencies and crime laboratories, algorithm vendors, academic researchers; convened an interdisciplinary meeting of 16 experts; and reviewed relevant agency documentation and literature.

GAO presented policy options in the 2021 report supporting this testimony.

View [GAO-24-107206](#). For more information, contact Karen L. Howard at 202-512-6888 or HowardK@gao.gov.

January 2024

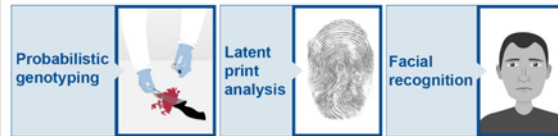
FORENSIC TECHNOLOGY

Algorithms Offer Benefits for Criminal Investigations, but a Range of Factors Can Affect Outcomes

What GAO Found

GAO's technology assessments in 2020 and 2021 found that federal law enforcement agencies primarily used three types of forensic algorithms to help assess whether evidence may have originated from an individual: probabilistic genotyping, latent print analysis, and facial recognition.

Figure. Federal law enforcement primarily uses three types of forensic algorithms.



Source: GAO (illustrations and information). | GAO-24-107206

Probabilistic genotyping algorithms compare collected DNA evidence (e.g., from blood, hair) to DNA samples from persons of interest. Such algorithms can assess a wider range of DNA samples than conventional methods but face some challenges. For example, it can be difficult to interpret or explain the results, and some experts told GAO that insufficient scientific studies have been conducted to fully validate their use for samples containing DNA from multiple people.

Latent print analysis can search larger databases of fingerprints and palm prints faster and more consistently than an analyst working alone. However, human involvement in using the outputs introduces opportunities for error and cognitive biases.

Facial recognition algorithms can also search large databases. They can be more accurate than a human analyst alone, but one study reported that the highest accuracy came from combining algorithms with trained analysts, as is common practice in federal law enforcement. However, human interpretation of algorithm outputs can introduce error or bias, and some law enforcement users may perceive the results as more certain than is warranted.

Furthermore, although some algorithms have high accuracy and very low bias, some law enforcement entities may not have enough information or resources to help them select such algorithms.

GAO's 2021 report described three options that policymakers could consider to help address key challenges to the use of forensic algorithms. Policymakers could support: increased training to improve consistent and objective use of forensic algorithms, standards and policies on appropriate use of forensic algorithms in investigations, and increased transparency related to algorithm testing.

Chairman Booker, Ranking Member Cotton, and Members of the Subcommittee:

Thank you for the opportunity to discuss our work on forensic algorithms. My testimony today summarizes our May 2020 and July 2021 technology assessments describing the uses, benefits, and challenges of forensic algorithms for criminal investigations, along with policy options that may help address the challenges.¹

For more than a century, law enforcement has used fingerprints and other physical evidence to help identify persons of interest, solve cold cases, and find missing or exploited people. Scientific advances are now allowing forensic experts to partially automate the examination of such evidence using algorithms.² In our prior reports, we found that federal law enforcement agencies primarily used three types of forensic algorithms to help assess whether evidence collected in a criminal investigation may have originated from an individual: probabilistic genotyping (an automated form of genetic analysis that is helpful for examining small or complex genetic samples), latent print (fingerprint and palm print) analysis, and facial recognition.³

My statement today addresses the benefits and challenges of those three algorithm types, along with options policymakers could consider to help address these challenges.

Forensic algorithms can be based on AI (e.g., facial recognition) or on mathematical models (e.g., probabilistic genotyping). With some forensic algorithms, like facial recognition and latent print analysis, numerous vendors offer forensic algorithms; previous testing by the National Institute of Standards and Technology (NIST) has shown that some of these algorithms are very accurate while others are less so. Experts told us that the best algorithms, when combined with human analysts, can offer significant benefits for law enforcement. However, forensic algorithm

¹GAO, *Forensic Technology: Algorithms Used in Federal Law Enforcement*, (Washington, D.C.: May 2020) GAO-21-435SP; and GAO, *Forensic Technology: Algorithms Strengthen Forensic Analysis, but Several Factors Can Affect Outcomes*, (Washington, D.C.: July 2021). GAO-20-479SP

²An algorithm is a set of rules that a computer follows to produce an outcome.

³Agencies also used algorithms to compare iris images, speech, and handwriting, to a lesser extent.

complexity and the variations between algorithms make it hard to understand and explain the results.

To examine these topics, we reviewed documents and interviewed officials from NIST and federal law enforcement agencies including the Department of Justice, the Department of Homeland Security, and the Department of Defense; conducted interviews with five non-federal law enforcement agencies or crime laboratories, four forensic algorithm vendors, and additional stakeholders; and reviewed relevant literature, including scientific articles and case law. We also convened a meeting of 16 experts including federal officials, researchers, legal scholars, defense advocates, and algorithm vendors. Additional information about our scope and methodology can be found in our May 2020 and July 2021 technology assessments. We performed the work on which this testimony is based in accordance with all sections of GAO's Quality Assurance Framework that are relevant to technology assessments.

Probabilistic Genotyping

Probabilistic genotyping algorithms compare collected DNA evidence (e.g., from blood, hair) to DNA samples taken from persons of interest. Probabilistic genotyping can assess a wider range of DNA samples than conventional methods, such as when a sample contains DNA from multiple people or when the sample is small or partially degraded. The output is a numerical measure of the probability that the person's DNA is part of the sample—a measure called the likelihood ratio. A high likelihood ratio indicates a higher probability that the person of interest contributed to the DNA sample.

Probabilistic genotyping does have some limitations; notably that the results still depend on the quality and quantity of the DNA. For example, a high-quality DNA sample will generally produce a higher likelihood ratio than a lower-quality sample from the same individuals. Similarly, a larger amount of material will generally yield a higher likelihood ratio than a smaller amount of material from the same source. Furthermore, the likelihood ratio typically decreases for evidence that contains DNA from more individuals.

We also identified two key challenges with the use of probabilistic genotyping algorithms: (1) difficulties with interpreting the meaning of a likelihood ratio and (2) lack of sufficient validation.

Experts told us that interpreting the meaning of a likelihood ratio is challenging for several reasons, including that some law enforcement professionals lack the necessary training about what these likelihood

ratios convey. They may view probabilistic genotyping algorithm results incorrectly as the likelihood that the suspect is guilty or not guilty. However, a probabilistic genotyping algorithm could return a low likelihood ratio if, for example, the sample is degraded or contains very little DNA, or there are multiple contributors. One agency official said that investigators who receive reports from probabilistic genotyping algorithms generally just look at the bottom line—whether an individual can be excluded or included in an investigation. Federal Bureau of Investigation (FBI) officials also explained that sharing technical information with others, including investigators, in an understandable way is the biggest challenge they face in working with probabilistic genotyping algorithms.

Validation, or the process of confirming these algorithms work as intended, is also challenging.

A key report by the 2016 President's Council of Advisors on Science and Technology (PCAST) stated that insufficient scientific studies have been conducted to fully validate the use of these algorithms for complex mixtures. The PCAST report also noted that establishing scientific validity requires independent evaluation, but there have been few such studies. Most of the studies evaluating probabilistic genotyping software have been done by software developers or law enforcement agencies. For example, the FBI has conducted its own studies to address these concerns for the algorithms it uses. Some policymakers have called for NIST to conduct additional studies, testing multiple algorithms across a broader range of variables than has been previously done. NIST is a non-regulatory agency in the Department of Commerce and independent of law enforcement and vendors.

Latent print analysis

Latent print analysis is an automated method to compare fingerprints and palm prints collected during a criminal investigation to a reference database of prints. A latent print can be an incomplete or distorted print left on a surface and then collected during a criminal investigation. The latent print is digitally scanned and its details (or minutiae) are marked by a human examiner. For federal criminal investigations, the marked scan is then uploaded into the Automated Fingerprint Identification System (AFIS), which uses multiple algorithms to analyze the print. These algorithms can improve image quality and read the many minutiae specific to a print, then compare those to a database of palm prints or tenprints—prints from all 10 of an individual's fingers—taken under controlled conditions. The output of this analysis is a candidate list of individuals who may be the source of the latent print found during an investigation, ranked in order by likelihood. An expert independently

compares the recovered print to the prints in this list of candidates and based on their own judgment, reaches an identification, exclusion, or inconclusive decision.

We found in our previous work that latent print algorithms are advantageous because they can search larger databases faster and more consistently than an analyst working alone. Law enforcement officials told us another advantage of these algorithms is that they can improve consistency. Human analysts may come to different conclusions when presented with the same latent print images, and latent print algorithms do not suffer fatigue.

We also identified several limitations and challenges to the use of these algorithms. For example, performance is poor when the quality of the evidentiary latent prints is poor. Furthermore, errors during collection can result in unusable data. Importantly, the candidate list of results will only include individuals whose prints are in the comparison database. This means that the actual person of interest may not appear in the candidate list produced by the algorithm.

In addition to these limitations, law enforcement agencies face three key challenges in their use of these algorithms: human involvement, communicating results, and testing. Human involvement is necessary to assess the results of latent print algorithms, but this also introduces opportunities for human error and cognitive biases. Because the algorithms return a candidate list, which is then reviewed by the analyst, human errors and bias can influence the end result. A 2011 study showed that false positives in latent print decisions are rare. But, as the PCAST report noted, false positive results can have negative consequences because they can result in false arrests, investigations, or convictions. A notable example is a 2004 case in which the FBI erroneously arrested and incarcerated a suspect for 2 weeks as a result of multiple analysts' errors and cognitive biases. One exploratory study showed that analysts' decisions when reviewing results could be influenced by knowledge of another analyst's prior judgement when considering the same prints.⁴ Law enforcement officials noted that other cases have led to improvements in latent print analysis practices, such as additional education for analysts to limit the challenge of human error and bias.

⁴I. E. Dror, D. Charlton, A. E. Peron, "Contextual information renders experts vulnerable to making erroneous identifications," *Forensic Science International*, Vol. 156 (2006).

A second key challenge is communicating the results to investigators and others. The results from a latent print algorithm do not include an assessment of the strength of evidence for or against a particular pair of prints being a match. Thus, when analysts communicate the results of their analysis, confidence in the results is generally based on factors such as the analyst's experience.

A third challenge is that the existing independent, comparative testing of the accuracy of these algorithms is out of date and does not always include key algorithms used by federal agencies. NIST last conducted comparative performance testing of latent print algorithms in 2012.⁵ NIST currently conducts a latent print algorithm test relaunched in 2020 and last updated their test plan on March 9th, 2022. In addition, vendors supply their algorithms to NIST without software names or versions, so law enforcement agencies cannot use the NIST results to gauge the accuracy of a specific algorithm. A 2018 internal validation study conducted by the FBI on its current algorithm showed a 63.3 to 69.6 percent accuracy rate.⁶ The accuracy rates from the NIST and FBI studies are not directly comparable because they involved different sets of latent prints.

Facial recognition

Facial recognition algorithms use AI to help analysts extract digital details from an image of a person's face collected as evidence (i.e., a 'probe photograph') and compare those details to images in a database. During federal criminal investigations that use facial recognition, the probe photograph is compared against the photos of known individuals in the FBI's Next Generation Identification System. Federal law enforcement may also use commercial facial recognition services with their own databases.⁷ The algorithm generates a candidate list of individuals from the database, with a ranking from most to least similar to the probe photograph.

⁵According to FBI officials, these 2012 accuracy data are out of date. In a 2018 internal validation study, FBI found higher accuracy rates for the algorithm currently used in the Next Generation Identification (NGI) System; however, we were unable to identify reports of comparative testing of latent print algorithms conducted in the intervening years. NIST relaunched its latent print technology research in May 2020.

⁶ Accuracy for latent print algorithms is measured as the percentage of attempts that returned the correct individual in the candidate list identified a possible source of the print.

⁷ GAO, Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties (Washington, D.C.: September 5, 2023), GAO-23-105607.

These algorithms are advantageous because they can search large databases faster and can be more accurate than analysts. For example, one vendor told us for our July, 2021 report that one of their algorithms returned a candidate list in 5 seconds from a test database of 363 people.

One study reported that an algorithm was more accurate than 73 percent of trained human analysts, and also reported that the highest accuracy came from combining the most accurate algorithm with a trained human analyst.⁸

One key limitation of facial recognition algorithms, as with latent print algorithms, is that the candidate list of results will only include individuals whose images are in the comparison database. This means that the actual perpetrator may not appear in the candidate list produced by the algorithm. As with other algorithms, the quality of the evidence (i.e., the probe image) will also affect the accuracy of the results. Our July, 2021 report also identified four challenges to law enforcement use of facial recognition algorithms: human involvement, testing and procurement, demographic effects, and public confidence.

Human involvement is an important aspect in the process of using these algorithms, according to stakeholders representing both law enforcement users and defense advocates. However, even with a highly accurate algorithm, human involvement can introduce errors. For example, a legal expert told us that analysts sometimes alter a low-quality probe image to increase the chances of getting a result, which can affect the candidate list produced by the algorithm. Such alterations can consist of adjustments of color contrast, rotating the face to the front, or more drastic edits such as adding open eyes over closed eyes.⁹ Humans can also introduce bias or errors when interpreting the list. For example, a 2020 study showed that seeing the algorithm outputs can influence how analysts interpret other evidence.¹⁰ The study found that prior identity

⁸See of P. J. Phillips et. Al, "Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms." *Proceedings of the National Academy of Sciences* vol 115, no 24 (2018).

⁹Rotating the face so that it aligns to the front, known as frontalization, uses facial landmarks to model a frontal image of the face. Frontal-facing images may improve accuracy of facial recognition algorithms.

¹⁰J. J. Howard, L. R. Rabbitt, and Y. B. Sirotin, "Human-algorithm Teaming in Face Recognition: How Algorithm Outcomes Cognitively Bias Human Decision-making," *PLOS ONE*, vol. 15, no. 8, (2020).

decisions, by either a computer or another human, influenced human decisions on whether a face pair was matching or non-matching.

Related to this, some law enforcement users may perceive the results of facial recognition algorithms as more certain than is warranted. For example, some users may not understand the extent to which the accuracy of the results depend on high-quality probe images. Additionally, they may not understand how enhancements or modifications to the probe image might affect results. These algorithms can return a candidate list regardless of image quality or other factors that may affect accuracy. For example, if a user assumes the candidate list is automatically reliable, the user risks identifying the wrong individual as a person of interest.

A second challenge is that law enforcement agencies may face difficulty procuring the most accurate, least biased algorithms. NIST currently has an ongoing facial recognition test known as the Face Recognition Vendor Test (FRVT). Federal law enforcement agencies have generally procured algorithms found by NIST to have the highest accuracy and limited or undetectable demographic bias. However, some agencies, including those at the state and local level, may not have the information or budget needed to procure the most accurate algorithms. One local law enforcement agency told us they selected an algorithm because the cost was relatively low.

A third challenge is that some facial recognition algorithms perform less accurately on certain demographic groups. According to the NIST testing, these demographic effects are small in the highest-performing algorithms. As we reported on July, 2021, there is no consensus on the exact cause or interaction of multiple causes of performance differences between demographic groups; however, we identified three possible factors specific to law enforcement use. First, people of color are disproportionately enrolled in the source mugshot databases searched by these algorithms. Second, algorithm developers and vendors do not have access to representative databases to train facial recognition algorithms to accurately identify faces. Third, image quality can exacerbate these demographic effects. A 2019 study demonstrated that the magnitude of

demographic effects can depend on the system used for image capture, which can affect image quality.¹¹

The fourth challenge is lower public confidence in facial recognition algorithms. Public mistrust of facial recognition algorithms can pose a challenge to law enforcement users if it leads to policies that restrict the use of the technology. For example, several localities have passed laws limiting or banning the use of facial recognition technology, due to concerns with privacy and misuse. The combination of a human expert analyst and top-performing algorithm can be more accurate than humans alone, and thus algorithms can be a powerful tool for generating leads in criminal investigations.

According to federal law enforcement officials, in some cases, the general public may not fully understand the types of controls that certain agencies have in place to govern use of the technology or its capabilities. For example, a key misperception among the public is that the algorithms operate with little to no human oversight. In fact, as described above, current algorithms require human involvement. A law enforcement official said that their algorithms simply replaced the act of searching through a series of mugshot books and selecting mugshots that looked similar to the suspect. Factors related to privacy and the images used for running searches may also reduce public confidence. Stakeholders we spoke with and literature we reviewed identified several sources of privacy concerns.¹² Further, some are concerned that facial recognition use could lead to general law enforcement surveillance of the public. Another potential cause for lower public confidence is the wide variation in standards and policies related to law enforcement use of facial recognition algorithms. An FBI official told us that non-federal law

¹¹C. M. Cook, J. J. Howard, Y. B. Sirotnin, J. L. Tipton, A. R. Vemury, "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*, vol. 1 no. 1 (2019).

¹²We have also previously discussed facial recognition privacy concerns in several reports: GAO-20-522, *Facial Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains*, GAO-19-579T (Washington, D.C.: June 4, 2019); GAO-22-106100 *Facial Recognition Technology: Federal Agencies' Use and Related Privacy Protections* (Washington, D.C.: June 29, 2022); and GAO-23-105607 *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties* (Washington, D.C.: Sep. 5, 2023).

enforcement agencies may use probe images that the FBI would reject as not meeting its higher image quality standards.

Policy options

Our July, 2021 report described three policy options that may help address key challenges to the use of forensic algorithms.¹³ The relevant policymakers could include Congress, other elected officials, federal agencies, state and local governments, academic research institutions, and industry. Specifically, policymakers could:

- Support increased training for law enforcement analysts and investigators to improve consistent and objective use of forensic algorithms and understanding of results. This could help reduce errors and bias and address challenges with interpretation of results.
- Support the development and implementation of standards and policies related to law enforcement testing, procurement, and use of these algorithms. This could help reduce errors, bias, and public mistrust, and help address challenges with interpretation of results. Some standards related to forensic algorithms already exist and others are under development. One step that may facilitate the development of new standards and policies may be to create a new forensic oversight body at the federal level, as recommended by a 2009 National Research Council report. Another option could be to assign a greater role to NIST and other federal agencies, as recommended by the 2016 PCAST report.
- Support increased transparency related to testing, performance, and use of forensic algorithms by law enforcement agencies. Such transparency could improve stakeholder and public knowledge and provide more useful information to law enforcement agencies.

In conclusion, forensic algorithms have expanded the capabilities of law enforcement and can improve the speed and objectivity of evidence analysis in investigations. However, use of these algorithms also poses challenges, including difficulties with understanding and interpreting the results and shortcomings in testing and validation. Fortunately, policymakers do have options for addressing these challenges.

¹³GAO-21-435SP

Chairman Booker, Ranking Member Cotton, and Members of the Subcommittee, this concludes my statement. I would be pleased to respond to any questions you or other Members may have.

If you or your staff have any questions about this testimony, please contact Dr. Karen L. Howard at (202) 512-6888 or howardk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Key contributors to this testimony include Hayden Huang (Assistant Director), Eliot Fletcher, and Rebecca Parkhurst. Additional contributors to the prior work on which this testimony is based are listed in our May 2020 and July 2021 reports.

Appendix I: Expert Meeting Participation

With the assistance of the National Academies of Sciences, Engineering, and Medicine, we convened a 1½-day meeting of 16 experts on forensic algorithms used in federal law enforcement. The meeting was held on January 15-16, 2020, in Washington, D.C. Many of these experts provided us with additional assistance throughout our work, including sending additional information for our review or reviewing our draft report for technical accuracy. The experts who participated in this meeting are listed below.

Sarah Chu; Senior Advisor on Forensic Science Policy, Innocence Project

Michael Coble; Associate Director of the Center for Human Identification, University of North Texas Health Science Center

Robert English; Special Counsel, Science and Technology Branch, Federal Bureau of Investigation

Tamara Giwa; Attorney, Assistant Federal Defender, Federal Defenders of New York

Patrick Grother; Scientist, Information Technology Laboratory, Information Access Division, Image Group, National Institute of Standards and Technology

William Guthrie; Division Chief, Statistical Engineering Division, National Institute of Standards and Technology

Karen Kafadar; Commonwealth Professor and Chair of Statistics, University of Virginia

Dan E. Krane; Professor and Interim Dean, Wright State University

James Loudermilk; Senior Director, Innovation and Customer Solutions, IDEMIA National Security Solutions

Anne May; Biometric Support Center Program Manager, Office of Biometric Identity Management, Department of Homeland Security

Mark Perlin; Chief Scientific and Executive Officer, Cybergenetics

Peter M. Vallone; Scientist, Biomolecular Measurement Division, National Institute of Standards and Technology

Appendix I: Expert Meeting Participation

Kit Walsh; Senior Staff Attorney, Electronic Frontier Foundation

James L. Wayman; Editor-in-Chief, IET Biometrics Journal

Rebecca Wexler; Assistant Professor University of California, Berkeley
School of Law

Michael Yates; Senior Technical Advisor on Biometrics, Science and
Technology Branch, Federal Bureau of Investigation

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook , Flickr , Twitter , and YouTube . Subscribe to our RSS Feeds or Email Updates . Listen to our Podcasts . Visit GAO on the web at https://www.gao.gov .
To Report Fraud, Waste, and Abuse in Federal Programs	Contact FraudNet: Website: https://www.gao.gov/about/what-gao-does/fraudnet Automated answering system: (800) 424-5454 or (202) 512-7700
Congressional Relations	A. Nicole Clowers, Managing Director, ClowersA@gao.gov , (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov , (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548
Strategic Planning and External Liaison	Stephen J. Sanford, Managing Director, spel@gao.gov , (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.

Testimony of
Rebecca Wexler

January 24, 2024

Statement of Rebecca Wexler
Co-Director, Berkeley Center for Law and Technology
Before the Senate Judiciary Committee
Hearing on "AI in Criminal Investigations and Prosecutions"
January 24, 2024

Mr. Chairman and members of the Committee. My name is Rebecca Wexler and I am a Faculty Co-Director of the Berkeley Center for Law and Technology and an Assistant Professor of Law at the University of California, Berkeley, School of Law. I also recently served as Senior Policy Advisor for Science and Justice at the White House Office of Science and Technology Policy, where I helped to implement President Biden's Executive Order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety. I am honored to testify here today about the need for fair and open proceedings to scrutinize A.I. tools used in the criminal legal system.

Although A.I. tools present exciting opportunities to render the legal system more accurate and equitable in some respects, they also, in their current form and use, present troubling obstacles to fair and open proceedings. To help fix this problem, Congress should do two things. *First*, require that A.I. tools used in the criminal legal system be made available for auditing by independent researchers with no stake in the outcome. *Second*, prohibit either party in a criminal case from invoking the so-called "trade secret privilege" to block access to relevant evidence, and instead require such evidence to be disclosed under a reasonable protective order.¹

THE UNITED STATES COMMITMENT TO FAIR AND OPEN CRIMINAL PROCEEDINGS

Zooming out, the United States criminal legal system is a model to the world in its commitment to fair and open proceedings to protect against wrongful convictions. That reputation rests on the safeguards we offer those accused of crime, including a fair opportunity to uncover weaknesses in the government's evidence of guilt and to expose unlawful and unconstitutional police conduct. This is why the Sixth Amendment guarantees the accused the right to confront witnesses against them and to compel witnesses in their favor.² This is why due process and

¹ The Justice in Forensic Algorithms Act of 2021, H.R. 2438, 117th Cong. § 2(b) (2021) provides a model of a bill to accomplish this important reform. *See also* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018) (examining the trade secret evidentiary privilege and explaining why it should not apply in criminal cases).

² U.S. CONST. AMEND. XI.

statutory discovery laws require prosecutors to disclose evidence to the defense.³ This is why the Supreme Court has directed judges deciding whether to admit scientific and technical evidence to consider whether that evidence has been subject to peer review.⁴ Fair and open proceedings, in which evidence is subject to robust and independent adversarial scrutiny, are necessary for accurate, accountable, and legitimate criminal investigations and prosecutions.

These transparency commitments are even more important in the emerging age of A.I. because we are together facing a new form of evidence that, by its nature, cannot be scrutinized with the tools parties have traditionally used, such as cross-examination and gumshoe detective work.⁵

In turn, allowing A.I. to enter criminal courtrooms without sufficient scrutiny is dangerous. While A.I. has the potential to improve law enforcement efficacy, it can also cause harmful errors with high-risk high stakes consequences for life and liberty.

Here are some examples. At least six people have allegedly been wrongfully arrested or jailed due to mistaken hits from A.I. facial recognition software.⁶ Researchers recently found that “a state-of-the-art A.I. system for estimating a person’s height and weight from a photograph”⁷ performed worse than regular people with no special training.⁸ Ninety percent of police deployments initiated by an A.I. gunshot audio detection system turned up no corroborating evidence of gunfire,⁹ but did lead to police “use of physical force on at least 82 Chicagoans, nearly all unarmed Black or Latinx men,” and to the alleged wrongful arrest and false imprisonment of at least three people.¹⁰ Two DNA analysis software programs came to

³ *Brady v. Maryland*, 373 U.S. 83 (1963); *Fed. R. Crim. P.* 16.

⁴ *Fed. R. Evid.* 702 *Advis. Comm. Note*; *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579 (1993).

⁵ *See, e.g.*, Andrea Roth, *How Machines Reveal the Gaps in Evidence Law*, 76 *VAND. L. REV.* 1631 (2023); Andrea Roth, *Machine Testimony*, 126 *YALE L.J.* 1972 (2017).

⁶ These individuals are Alonzo Sawyer, *see Eyal Press, Does A.I. Lead Police to Ignore Contradictory Evidence?* *The New Yorker* (Nov. 13, 2023); Porcha Woodruff, *see Kashmir Hill, Eight Months Pregnant and Arrested After False Facial Recognition Match*, *N.Y. Times* (Aug. 6, 2023); Randall Reid, *see Kashmir Hill & Ryan Mac, 'Thousands of Dollars for Something I Didn't Do,' N.Y. Times* (April 6, 2023); Nijeer Parks, *see Kashmir Hill, Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, *N.Y. Times* (Jan. 6, 2021); Michael Oliver, *see Elisha Anderson, Controversial Detroit Facial Recognition Got Him Arrested for a Crime he Didn't Commit*, *Detroit Free Press* (July 10, 2020); and Robert Williams, *see Kashmir Hill, Wrongfully Accused by an Algorithm*, *N.Y. Times* (June 24, 2020). *See generally*, Garvie, Clare, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, *CENTER ON PRIVACY & TECHNOLOGY AT GEORGETOWN LAW* (2022).

⁷ HANY FARID, *AI: A PRIMER FOR LEGAL PRACTITIONERS* 19 (2023).

⁸ Sarah Barrington & Hany Farid, *A comparative analysis of human and AI performance in forensic estimation of physical attributes*, *SCIENTIFIC REPORTS*, 13(1):4784, 2023.

⁹ CITY OF CHICAGO OFFICE OF INSPECTOR GENERAL, *THE CHICAGO POLICE DEPARTMENT'S USE OF SHOTSPOTTER TECHNOLOGY* 3 (Aug. 2021).

¹⁰ *See, e.g.*, Jonathan Manes & Alexa Van Brunt, *Williams v. City of Chicago*, *MACARTHUR JUSTICE CENTER*, available at <https://www.macarthurjustice.org/case/williams-v-city-of-chicago/>.

divergent results on whether the defendant's DNA was included in a mixture of DNA found in a homicide investigation.¹¹

We need fair and open proceedings to expose these kinds of costly mistakes and discrepancies and to allow our adversarial system to work according to the ideals it has always had and always should.

THE NEED FOR PEER REVIEW OF A.I. TECHNOLOGIES USED IN CRIMINAL PROCEEDINGS

Unfortunately, some vendors of A.I. technologies used in criminal proceedings are blocking independent peer review that might expose flaws or biases in their products. For instance, consider probabilistic genotyping software. The United States Government Accountability Office identified a “lack of independent review” of these tools whereby “[m]ost of the studies evaluating probabilistic genotyping software have been undertaken by software developers themselves or by law enforcement agencies.”¹² The President’s Council of Advisors on Science and Technology (“PCAST”) similarly concluded that further “studies should be performed by or should include independent research groups not connected with the developers of the methods and with no stake in the outcome.”¹³ Most recently, the National Institute of Standards and Technology (“NIST”) observed that for “most peer-reviewed articles that describe validation experiments” for probabilistic genotyping software tools, “sufficient data are not publicly available for an independent assessment of reliability”¹⁴

Yet when my fellow academic researchers at the University of California, Berkeley, and I sought to purchase a research license to study one of these probabilistic genotyping software systems, the vendor—a company called Cybergenetics—told us that “Cybergenetics does not provide research licenses.”¹⁵ Notably, representatives of this company have for years testified under oath in courts across the country that their product is subject to “a peer review process,”¹⁶ and hence, its outputs should be admissible in criminal trials. Yet when academic researchers with no stake in the outcome attempted to actually perform independent research into quality assurance and validation of their product, the company used contract law to stop that from happening.

¹¹ See PRESIDENT’S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, FORENSIC SCIENCE IN CRIMINAL COURTS: ENSURING SCIENTIFIC VALIDITY OF FEATURE COMPARISON METHODS 79 n.212 (2016) (hereinafter “PCAST Report”).

¹² GOVERNMENT ACCOUNTABILITY OFFICE, FORENSIC TECHNOLOGY: ALGORITHMS USED IN FEDERAL LAW ENFORCEMENT 41 (2020).

¹³ PCAST Report at 81.

¹⁴ NIST, DNA MIXTURE INTERPRETATION: A NIST SCIENTIFIC FOUNDATION REVIEW 50 (2021).

¹⁵ See Appendix, Email from Ria David to Rediet Abebe, Re: Research License for TrueAllele, March 24, 2021.

¹⁶ *Com. v. Foley*, 38 A.3d 882, 889 (P.A. Sup. Ct. 2012). See also, *People v. Wakefield*, 38 N.Y. 3d 367, 376 (N.Y. 2022) (concluding that “independent validation of the reliability of the software is available in the form of a free trial that can be used to verify a known sample” and that “TrueAllele Casework has been the subject of numerous peer-reviewed published articles in scientific journals”); *Ohio v. Shaw*, CR-13-575691 at *8 (Oct. 10, 2014), <http://www.cyngen.com/information/press-release/2014/TrueAllele-Casework-Ruled-Admissible-in-Ohio-Daubert-Challenge/admissibility.pdf> (describing testimony from Dr. Perlin that “TrueAllele has been validated and there are five published peer-reviewed validation papers on the TrueAllele Casework System”); *Foley*, 38 A.3d at 889 (“TrueAllele has been tested and validated in peer-reviewed studies.”).

Senators Blumenthal and Hawley's bipartisan framework on A.I. legislation states that developers should be required "to provide independent researchers access to data necessary to evaluate A.I. model performance."¹⁷ This is precisely what is needed and what is not happening for A.I. tools in the criminal legal system.

Congress should require vendors to allow independent audits by clarifying that A.I. tools used in the criminal legal system must be subject to peer review, and that peer review includes making the tools available for auditing by research groups with no stake in the outcome. This is a far more modest and practical solution than requiring that all technologies used in the criminal legal system be open source or simply having judges render the tools inadmissible. There is an important role for Congress here to authorize federal grants for law enforcement agencies to purchase A.I. systems only if the vendors of those systems make them available for independent researchers to evaluate performance.

CLARIFYING THAT NO TRADE SECRET EVIDENTIARY PRIVILEGE EXISTS IN CRIMINAL CASES

Vendors of A.I. technologies have also relied on a supposed trade secret evidentiary privilege to refuse to disclose details about how their technologies work to criminal defendants and expert witnesses, even under 'attorneys eyes only' protective orders that would reasonably safeguard the vendor's intellectual property interests, and even when the outputs from the A.I. systems are introduced as evidence in capital cases where the risk of error is wrongful death.¹⁸

As I recounted in a recent law review article, "A death penalty defendant in Pennsylvania, a 'family guy' with no prior criminal record, was acquitted on all counts—but not before being forced to undergo trial without the opportunity to review or challenge the source code of the forensic software used to analyze the evidence against him."¹⁹ Another death-eligible defendant in California was not so lucky. "Martell Chubbs was denied access to the source code for a forensic software program used to convict him because the developer claimed that it was a trade secret."²⁰ And "[i]n a federal court in Texas, the federal government claimed that trade secret interests should shield details about how a cybercrime investigative software program operates, even though the information was necessary to determine whether warrantless use of the tool had violated the Fourth Amendment."²¹

This should not be happening.

Adversarial review by criminal defense counsel and expert witnesses is an important component of fair and open proceedings that has proven effective at rooting out problems with

¹⁷ Senator Richard Blumenthal & Senator Josh Hawley, *Bipartisan Framework for U.S. AI Act* (2023).

¹⁸ See generally, Rebecca Wexler, *Life Liberty and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018).

¹⁹ *Id.* at 1361.

²⁰ *Id.* at 1358.

²¹ *Id.* at 1346.

law enforcement technologies in the past. For instance, it took years for defense experts to be able to review the source code for the “FST” forensic DNA analysis software program because the developer of that program—the Office of the Chief Medical Examiner of New York City—repeatedly claimed a trade secret privilege to entirely withhold relevant evidence from the accused. When a court finally ordered disclosure to a defense expert witness despite this claim, the witness discovered an undisclosed function that discarded data from certain calculations without alerting the user and that had been added *after* the system received regulatory approval for use in criminal cases with no notice to the regulator.²² We need criminal defense counsel and expert witnesses—as well as judges and prosecutors—to be able to scrutinize A.I. systems used in the criminal legal system to ensure the accuracy and fairness of criminal investigations and prosecutions.

There is no good reason for trade secret law to block this crucial process. Trade secret law is supposed to protect against misappropriations by business competitors, not cross-examination in court. Courts can protect intellectual property rights to the full extent reasonable by ordering disclosure under a protective order. That solution is commonly used in civil litigation and it should work in criminal cases as well. Of course, in the unlikely event that an attorney were to violate the protective order, the trade secret owner could sue them for misappropriation and the attorney could be subject to professional disciplinary sanctions and criminal contempt of court. That is more protection than trade secret law generally affords for common business negotiations where information is shared under non-disclosure agreements. In short, there should be no trade secret evidentiary privilege to entirely withhold relevant evidence in a criminal case.

Once again, there is an important role for Congress to clarify that no trade secret privilege exists in federal criminal cases and that relevant trade secret evidence must be disclosed under a reasonable protective order. The power to enact federal privilege law by statute is within Congress's well-established authority and comports with the Rules Enabling Act, 28 U.S.C. § 2071-77. Under Federal Rule of Evidence 501, Congress retains full authority to enact “a federal statute” to govern claims of privilege in the United States courts. Fed. R. Evid. 501. Accordingly, Congress may enact a federal statute stating that there is no trade secret evidentiary privilege in criminal proceedings.

Properly balancing A.I.'s promises and perils for criminal prosecutions and investigations will require firm commitment to our fundamental principles of fair and open criminal proceedings. Congress's help is needed to reaffirm that commitment for the age of A.I.

Thank you for the opportunity to testify here today.

²² *Id.* at 1398. This function had been added after the system was approved for use by New York's Commission on Forensic Science, yet the system was not submitted for re-approval. *Id.*

APPENDIX

1/16/24, 5:03 PM

UC Berkeley Mail - Fwd: Research License for TrueAllele



Rebecca E Wexler <[REDACTED]@berkeley.edu>

Fwd: Research License for TrueAllele

11 messages

Rediet Abebe <[REDACTED]@berkeley.edu> Wed, Mar 24, 2021 at 7:45 AM
 To: Rebecca Wexler <[REDACTED]@berkeley.edu>, Andrea Roth <[REDACTED]@berkeley.edu>

----- Forwarded message -----

From: Ria David <[REDACTED]@cybgen.com>
 Date: Wed, Mar 24, 2021, 6:35 AM
 Subject: Re: Research License for TrueAllele
 To: Rediet Abebe <[REDACTED]@berkeley.edu>

Dear Prof. Abebe,

Thank you for your inquiry. Cybergenetics does not provide research licenses.

Kind regards. Ria

=====

Ria David, PhD
 President
 Cybergenetics

[REDACTED] (c)
[\[REDACTED\]@cybgen.com](mailto:[REDACTED]@cybgen.com)
www.cybgen.com

> On Mar 19, 2021, at 3:03 PM, Rediet Abebe <[REDACTED]@berkeley.edu> wrote:
 >
 > Hi there,
 >
 > My name is Rediet Abebe and I'm an assistant professor of computer science at UC Berkeley working in algorithms and AI.
 >
 > I'm interested in conducting independent research into quality assurance and validation of various forensic software systems. I would like to purchase a research license to study TrueAllele. Would you happen to have a process for this? And do you have a rough timeline?
 >
 > Please let me know and many thanks in advance for your time,
 > Rediet
 >
 > --
 > Rediet Abebe, Ph.D.
 > Assistant Professor, University of California Berkeley
 > Junior Fellow, Harvard Society of Fellows
 > <https://www.cs.cornell.edu/~red/>

Rebecca Wexler <[REDACTED]@berkeley.edu> Wed, Mar 24, 2021 at 8:39 AM
 To: Rediet Abebe <[REDACTED]@berkeley.edu>
 Cc: Andrea Roth <[REDACTED]@berkeley.edu>

**Senate Judiciary Committee
Hearing on
“AI in Criminal Investigations and Prosecutions”
January 24, 2024
Questions for the Record**

Armando Aguilar, Assistant Chief of Police, Miami Police Department

In your written testimony you discussed how your police department developed responsible technology policies which govern the use of facial recognition technologies. This includes procedures to ensure that facial recognition matches are not used as probable cause to arrest, ensuring that facial recognition matches are treated as “tips” and followed up the type of police-work that generates court-admissible evidence, and limiting access to who can use facial recognition technologies.

- Can you speak to the importance of implementing responsible technology policies? *In law enforcement, public trust is our capital. This is, by no means, a novel concept. Sir Robert Peel, who founded the London Metropolitan Police Service (the first “police department” in the modern sense) almost 200 years ago, developed nine principles for policing that are just as relevant today as they were when they were first penned. The first two of those principles most appropriately addresses this question: 1) the basic mission for which the police exist is to prevent crime and disorder, and 2) the ability of the police to perform their duties depends on public approval of police actions. Our authority to enforce the law in a democratic society is derived from the consent of the people we serve. Technology companies have their role in delivering public safety, but they do not carry the same sworn duty to balance the delivery of public safety with the safeguarding of civil liberties. It is, therefore, incumbent upon law enforcement agencies to harness the power of these technologies while ensuring that they are used within a framework rooted in constitutional principles.*
- How do these policies allow police departments to use facial recognition technology to aid their public safety mission while also respecting the rights of the public they serve? *We rely on sound policy and training to ensure that we use facial recognition technology in a manner that is limited to a handful of allowable use cases. In developing our policy, we went to great lengths to ensure that our desire that FR not be used arbitrarily or as a tool to suppress constitutional rights (including but not limited to free speech, freedom of*

religion, and freedom of the press) was codified into policy and that our personnel were adequately trained in the requirements and intent of that policy.

- Are your department's policies available to the public or can you discuss how your office treats requests for information about A-I usage, to enhance public trust of the system and ensure accountability? A copy of the Miami Police Departmental Orders is available online at https://www.miami-police.org/DeptOrders/MPD_Departmental_Orders.pdf. Our policies are made available to the public, including our facial recognition policy, which begins on page 908. Our use of facial recognition in criminal cases is not withheld from defendants, and our facial recognition searches are subject to Chapter 119 of the Florida Statutes, which governs public records. Florida has very broad public records laws, but certain records (including, but not limited to, information pertaining to open criminal investigations) are exempt from public disclosure.

Question 1: How can Congress work to ensure that state and local law enforcement agencies have access to the resources they need to train personnel and keep their proficiency up-to-date?

In our technology assessment on forensic algorithms (GAO-21-435SP), we proposed a policy option to support training, but such efforts may require additional resources.

Specifically, we reported that there is variability in training requirements across different law enforcement agencies. For example, state and local law enforcement agencies using non-FBI databases for facial recognition do not necessarily have a training requirement, and available training may not be standardized. To address this challenge, we proposed a policy option that, among other things, proposed the support of increased training of law enforcement analysts, as well as investigators. Actions to support this policy option could include supporting the development of standards for training and certification.

One consideration to taking this approach is identifying an entity or entities that would actually develop relevant standards and certifications. Additionally, smaller law enforcement agencies may not have the funding or personnel to develop training materials. Addressing these and other considerations as discussed in our report could facilitate greater and more uniform proficiency among users of these algorithms.

Question 2: Are you familiar with other jurisdictions that we could look to for examples of responsible use of training and policy around A-I technology?

We did not conduct audit work focusing on local, state, and tribal law enforcement responsible use of artificial intelligence technology. While we did talk with some local law enforcement agencies, we did not specifically examine their use of artificial intelligence technology.

While not jurisdictions, federal agencies have worked on approaches to responsible implementation of artificial intelligence. For example, GAO issued an artificial intelligence accountability framework ([GAO-23-106811](#)) that could be used to guide responsible artificial intelligence use. Additionally, the National Institute for Standards and Technology (NIST) has also done work on responsible use of artificial intelligence, namely their Trustworthy & Responsible Artificial Intelligence Resource Center.

**Senate Judiciary Committee
Hearing on
“AI in Criminal Investigations and Prosecutions”
January 24, 2024
Questions for the Record**

For Rebecca Wexler, Assistant Professor of Law, UC Berkeley School of Law & Faculty Co-Director, Berkeley Center for Law & Technology

You have previously spoken about how neural networks, which power most generative A-I systems, are easy to scale but “can’t handle the truth.” These systems are generating convincing misinformation even when the user doesn’t ask them to.

- Can you tell us more about this problem in the context of the criminal justice system?
- Do you think teaching digital literacy, so that individuals understand how to identify misinformation, perhaps at nonprofits or to police officers, is part of the solution here?
- When it comes to AI-related data protection and privacy specifically, what would you call for in privacy legislation? How would a comprehensive federal privacy law impact or change the development of large language models?



January 24, 2024

Chairman Cory Booker
 Ranking Member Tom Cotton
 U.S. Senate Committee on the Judiciary
 Subcommittee on Criminal Justice and Counterterrorism
 226 Dirksen Senate Office Building, Washington D.C. 20515

Re: CAIDP Statement for the Record: "AI in Criminal Investigations and Prosecutions"

Dear Chairman Booker, Ranking Member Cotton, and Members of the Subcommittee,

We write to you regarding the hearing on "AI in Criminal Investigations and Prosecutions."¹ The Center for AI and Digital Policy (CAIDP) appreciates your leadership on addressing the risks and benefits of AI systems, particularly noting the serious risks of using AI in criminal investigations and prosecutions, and your work towards establishing standards of AI governance.

The CAIDP is an independent research and education non-profit based in Washington, DC.² Our global network of AI policy experts and advocates advise national governments and international organizations on artificial intelligence and digital policy, including the OECD, European Union, the Council of Europe, G7, G20, UNESCO, and, indeed, various branches of the U.S. Government. We also publish the annual *Artificial Intelligence and Democratic Values Report*,³ providing a comprehensive review of AI policies and practices in 75 countries.

In brief, our recommendations to this Committee are:

- 1) to exercise oversight on federal government tasked with protecting civil liberties in the administration of criminal justice under the Biden AI Executive Order⁴
- 2) to move forward with legislation—
 - a. Mandating transparency and accountability obligations that furthers equity and democratic principles
 - b. Prohibiting the use of pseudo-scientific and human rights-violating technologies, including in administration of criminal justice

¹ U.S. Senate Committee on the Judiciary, Subcommittee on Criminal Justice and Counterterrorism, *AI in Criminal Investigations and Prosecutions* (January 24, 2024), <https://www.judiciary.senate.gov/committee-activity/hearings/ai-in-criminal-investigations-and-prosecutions>.

² CAIDP, *About*, <https://www.caidp.org/about-2/>.

³ CAIDP, *Artificial Intelligence and Democratic Values* (2023), <https://www.caidp.org/reports/aidv-2022/>.

⁴ Executive Order 14110 of October 30, 2023, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, Federal Register Vol. 88, No. 210, pg. 75191-75226, <https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf>



Recommendation 1: Exercise oversight on the federal government tasked with protecting civil liberties in the administration of criminal justice under the Biden Executive Order

President Biden’s Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence⁵ (“AI EO”) is a sweeping document on AI guardrails and seeks to position the federal government as a model of accountable AI development and use.

The principles and policies section of the AI EO states, “*Artificial Intelligence policies must be consistent with my Administration’s dedication to advancing equity and civil rights. My Administration cannot—and will not—tolerate the use of AI to disadvantage those who are already too often denied equal opportunity and justice...[I]t is necessary to hold those developing and deploying AI accountable to standards that protect against unlawful discrimination and abuse, including in the justice system and the Federal Government. Only then can Americans trust AI to advance civil rights, civil liberties, equity, and justice for all.*”⁶

Section 7.1 of the AI EO 7.1 addresses the obligations of the federal government for “*Strengthening AI and Civil Rights in the Criminal Justice System*”⁷ including the following:

- the need to improve external stakeholder engagement to promote public awareness of potential discriminatory uses and effects of AI, and develop additional training, technical assistance, guidance, or other resources as appropriate.
- providing guidance, technical assistance, and training to State, local, Tribal, and territorial investigators and prosecutors on best practices for investigating and prosecuting civil rights violations and discrimination related to automated systems, including AI.
- Direction to the Attorney General to address unlawful discrimination and other harms exacerbated by AI mainly by coordinating with and supporting agencies in implementing and enforcing existing Federal laws to address civil rights and civil liberties violations and discrimination related to AI.

Notably, the AI EO requires the Assistant Attorney General in charge of the civil rights division to convene a meeting of the heads of Federal civil rights offices “[T]o discuss comprehensive use of their respective authorities and offices to: prevent and address discrimination in the use of automated systems, including algorithmic discrimination; increase coordination between the Department of

⁵ Executive Order 14110 of October 30, 2023, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, Federal Register Vol. 88, No. 210, pg. 75191-75226, <https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf>

⁶ *Id.* Section 2(d), pg. 75192

⁷ AI EO, pg. 75211



Justice's Civil Rights Division and Federal civil rights offices concerning issues related to AI and algorithmic discrimination".⁸ The EO mandates this action be completed within 90 days.

The National Institute of Justice in its report on *Using Criminal Justice To Address Criminal Justice Needs*⁹ states,

"Video analytics for integrated facial recognition, the detection of individuals in multiple locations via closed-circuit television or across multiple cameras, and object and activity detection could prevent crimes through movement and pattern analysis, recognize crimes in progress, and help investigators identify suspects. With technology such as cameras, video, and social media generating massive volumes of data, AI could detect crimes that would otherwise go undetected and help ensure greater public safety by investigating potential criminal activity, thus increasing community confidence in law enforcement and the criminal justice system. AI also has the potential to assist the nation's crime laboratories in areas such as complex DNA mixture analysis."

The Department of Justice and Office of Justice Programs has been deploying pseudo-scientific and potentially rights-impacting AI systems at all levels of criminal prosecution. We urge this Committee to act on its jurisdiction¹⁰ to exercise oversight on the mandates set out in Section 7.1 the AI EO and move forward with legislation protecting civil liberties.

Recommendation 2: Move forward with comprehensive AI legislation

We commend the recent actions to guide the appropriate use of AI— including the AI EO, the draft guidance of the OMB on federal agencies' use of AI,¹¹ the April 2023 joint statement by the FTC, DOJ, EEOC, and CFPB on bias in automated systems,¹² and the Blueprint for an AI Bill of Rights.¹³

⁸ *Id.*

⁹ Christopher Rigano, "Using Artificial Intelligence to Address Criminal Justice Needs," *NIJ Journal* 280, January 2019, <https://www.nij.gov/journals/280/Pages/using-artificial-intelligence-to-address-criminal-justice-needs.aspx>

¹⁰ U.S. Senate Committee on the Judiciary, *About the Committee*, <https://www.judiciary.senate.gov/about/committee>.

¹¹ OMB, *OMB Releases Implementation Guidance Following President Biden's Executive Order on Artificial Intelligence* (November 01, 2023), <https://www.whitehouse.gov/omb/briefing-room/2023/11/01/omb-releases-implementation-guidance-following-president-bidens-executive-order-on-artificial-intelligence/>.

¹² Rohit Chopra, et al., *Joint Statement On Enforcement Efforts Against Discrimination And Bias In Automated Systems*, EEOC, CRT, FTC, and CFPB (April 25, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.

¹³ *Blueprint for an AI Bill of Rights*, White House Office of Science and Technology Policy (October 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>.



However, these measures do not address the full spectrum of governance required for the development, deployment, and use of AI systems. We support and endorse the Blumenthal-Hawley Bi-Partisan Framework for U.S. AI Act¹⁴ and the Algorithmic Accountability Act¹⁵. We believe the implementation of either of these initiatives would go a long way in filling the legislative vacuum in which high-risk AI systems operate.

a. Congress should enact legislation that furthers equity and civil rights, in criminal justice and beyond

A recent report from the National Institute of Justice examined AI applications in the criminal justice system, focusing on AI's role in addressing prosecutorial needs.¹⁶ The report identified several uses of AI that pose significant risks and challenges. The following are examples worth highlighting:

- Law Enforcement: AI applications such as E-Discovery Technologies,¹⁷ Predictive Policing Technology,¹⁸ search engines to find relevant case law, predictive analytics to assist with litigation strategies, and algorithms to help detect evidence tampering, are relevant in the context of law enforcement activities.
- Automated Decision-Making (Pretrial, Prosecution, Parole): AI is being purported to have "predictive" uses across the criminal justice pipeline: determining bail/detention decisions in identifying suspects (e.g., facial recognition and fingerprinting), pretrial processing, determining whether or how to prosecute suspects, managing parole, and much more.
- Corrections: The San Francisco District Attorney is using AI redaction software in an attempt to eliminate bias in decisions about who to prosecute. Prosecutors use an AI-enabled "bias mitigation" tool developed at Stanford to automatically redact information from police reports that could identify a suspect's race.

¹⁴ Senator Richard Blumenthal & Senator Josh Hawley, *Bipartisan Framework for U.S. AI Act*, <https://www.blumenthal.senate.gov/imo/media/doc/09072023bipartisanaiframework.pdf>

¹⁵ Office of Senator Cory Booker, *Booker, Wyden, Clarke Introduce Bicameral Bill to Regulate Use of Artificial Intelligence to Make Critical Decisions like Housing, Employment and Education*, Press Release, (September 21, 2023), <https://www.booker.senate.gov/news/press/booker-wyden-clarke-introduce-bicameral-bill-to-regulate-use-of-artificial-intelligence-to-make-critical-decisions-like-housing-employment-and-education>

¹⁶ James Redden & Duren Banks, *Artificial Intelligence Applications for Criminal Courts: An Overview of Artificial Intelligence Applications for Prosecutors and Associated Considerations for the Criminal Court System*, National Institute of Justice (August 1, 2020), <https://nij.ojp.gov/library/publications/artificial-intelligence-applications-criminal-courts-overview-artificial>.

¹⁷ This includes video redaction and audio transcription.

¹⁸ Margo McGehee, *Predictive Policing Technology: Fourth Amendment and Public Policy Concerns*, University of Cincinnati Law Review Blog (February 17, 2021), <https://uclawreview.org/2021/02/17/predictive-policing-technology-fourth-amendment-and-public-policy-concerns/>.



When AI systems are deployed for any of those uses, there is always a high risk of error. The Supreme Court has laid down that “procedural due process rules are shaped by the risk of error inherent in the truth-finding process....”¹⁹ Hence, to ensure that the use of AI does not violate procedural due process under Fifth and Fourteenth Amendments,²⁰ it is incumbent upon the adjudicating body to ensure that notice is being provided as to the specific AI being used and its potential effects to ensure that individuals who are impacted by the technology are well-informed and afforded “meaningful opportunity to be heard in his own defense within a reasonable time.”²¹

In addition to the problem with procedural due process, the use of AI in prosecutorial decision-making raises the problem of “automation bias.”²² When humans use automation as a shortcut or a “recommendation,” they effectively treat the computer suggestions as final decisions, replicating the bias and inaccuracies of the system.²³

“Automation bias” also has an impact on the interpretation of the Fourth Amendment, particularly its requirement for reasonableness, which is used to determine the legality of a “terry stop.” Predictive policing tools could potentially facilitate law enforcement in identifying individuals who meet the reasonable suspicion standard, leading to an increase in “Terry stops”, because the use of technology leads to the often-misleading perception of objectiveness and accuracy. Therefore, this Committee should enact legislation that encompasses the Supreme Court’s clearly established standards of due process in the context of AI systems.²⁴ To address automation bias, the Committee should consider the following recommendations in developing legislation:

- i. Agencies should provide education to hearing officers about the fallibility of automated systems and offer explicit training on automation bias. Studies have shown that such training encourages individuals to critically evaluate automated system suggestions.²⁵

¹⁹ *Mathews v. Eldridge*, 424 U.S. 319 (1976), at para 344.

²⁰ *Mathews v. Eldridge*, at para 5-6; *Houston Fed’n of Tchrs., Loc. 2415 v. Houston Indep. Sch. Dist.*, 251 F. Supp. 3d 1168 (S.D. Tex. 2017); *T. v. Bowling*, No. 2:15-CV-09655, 2016 WL 4870284 (S.D.W. Va. Sept. 13, 2016), modified sub nom. *Michael T. v. Crouch*, No. 2:15-CV-09655, 2018 WL 1513295 (S.D.W. Va. Mar. 26, 2018).

²¹ *Houston Fed’n of Tchrs. v. HISD*, at para 1176.

²² When using AI systems, judges may have the tendency to rely on computer systems in mixed decision-making scenarios, which diminishes the value of human involvement. This trust in automated systems results in judges depending on computer-generated solutions and not actively seeking out information that may contradict these recommendations, even when they suspect a system malfunction.

²³ Hannah Bloch-Wehba, *Access to Algorithms*, 88 Fordham L. Rev. 1265 (2020), <https://ir.lawnet.fordham.edu/flr/vol88/iss4/2/>; Susanne Gaube, et al., *Do as AI say: susceptibility in deployment of clinical decision-aids*, 4 NPJ Digital Medicine 31 (2021), <https://doi.org/10.1038/s41746-021-00385-9>.

²⁴ *United States v. Curry*, 965 F.3d 313 (4th Cir. 2020), as amended (July 15, 2020), as amended (July 16, 2020).

²⁵ *Id.*



- ii. Agencies should mandate that hearing officers provide detailed explanations for their reliance on automated system decisions, including identifying the computer-generated facts or legal findings that influenced their decisions. This approach aligns with administrative law's emphasis on explicit statements of reasons and helps combat automation bias.²⁶

This Committee should move forward with comprehensive AI legislation. In furtherance of this, we reiterate recommendations made in previous communications to this committee.²⁷

- Implement ex-ante human rights impact assessments for any AI system that implicates civil rights or public safety
- Establish a licensing regime administered by an independent oversight body
- Create a liability regime that ensures not only legal accountability for harms, but takes a proactive approach to ensure compliance with established fairness and safety standards
- Emphasize data minimization, transparency, and the right to contest adverse decisions made by AI systems.
- Advance comprehensive, binding global cooperation to preserve human rights from both public and private uses of AI.

b. Prohibit the use of pseudo-scientific and human-rights violating technologies in the administration of criminal justice

Congress must establish guardrails that ensure that certain uses and/or AI systems is never appropriate. We call to the attention of the Committee to the following uses/systems which are pseudo-scientific and undermine the rule of law, due process, and human dignity, and as such, should be prohibited in any comprehensive legislation pursued by this Committee:

i. Predictive risk assessments in policing and immigration

Models that claim to predict future behavior,²⁸ such as criminal recidivism or even the identity and location of a crime, are pseudo-scientific technologies that draw spurious, often discriminatory,²⁹ correlations that are leveraged by authorities under claims of “objectivity” and “science.” In fact, a 2020

²⁶ *Id.*

²⁷ CAIDP, *Artificial Intelligence and Human Rights*, Statement for the Senate Judiciary Committee, Subcommittee on Human Rights and the Law (June 13, 2023), <https://www.caidp.org/app/download/8462575863/CAIDP-SJC-06132023.pdf?t=1705850993>; CAIDP, *Oversight of A.I.: Legislating on Artificial Intelligence*, Statement for the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law (May 11, 2023), <https://www.caidp.org/app/download/8457859963/CAIDP-Statement-SJC-AI-05112023.pdf?t=1705850993>.

²⁸ Will Douglas Heaven, *Predictive policing algorithms are racist. They need to be dismantled.*, MIT Technology Review (July 17, 2020), <https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/>.

²⁹ David Arnold, Will Dobbie, and Peter Hull, *Measuring Racial Discrimination in Algorithms*, Becker Friedman Institute for Economics at the University of Chicago (2020), https://bfi.uchicago.edu/wp-content/uploads/2020/12/BFI_WP_2020184.pdf.



letter by more than 1500 mathematicians called to end predictive policing work,³⁰ but such algorithms continue to be deployed and lead to unlawful and incorrect decisions.³¹ Congress must act against these fundamental attacks on the Constitutional presumption of innocence and right to human agency.

ii. Facial surveillance technology

The use of facial recognition technology for mass surveillance threatens the rights to privacy, consent, and transparency as we know it. Facial recognition technology is also known to be flawed due to racial and gender disparities in accuracy.³² The unfettered use of facial recognition technology in law enforcement, most notably through contracts with Clearview AI,³³ has resulted in incorrect and appalling incarcerations.³⁴

iii. Biometric categorization

Attempts to categorize people according to race, gender, nationality, religion, sexual orientation, political beliefs, etc. based on biometric data is fundamentally pseudo-scientific as they attempt to map biometrics onto subjective social constructs. These systems can also have particularly harmful effects on minority groups, such as transgender people.³⁵ Biometric categorization technologies

iv. Sentiment detection and analysis

Systems that claim to detect emotions, thoughts, or truthfulness from physical features and expressions are pseudo-scientific and discriminatory.³⁶ Research shows that the expression of emotions

³⁰ Lilah Burke, *Mathematicians Urge Ending Work With Police*, Inside Higher Ed (June 23, 2020), <https://www.insidehighered.com/news/2020/06/24/mathematicians-urge-cutting-ties-police>.

³¹ Matt Stroud, *Heat Listed*, The Verge (May 24, 2021), <https://www.theverge.com/c/22444020/chicago-pd-predictive-policing-heat-list>; Robert Koulisch & Kate Evans, *Punishing With Impunity: The Legacy of Risk Classification Assessment in Immigration Detention*, 36 Georgetown Immigration Law Journal pp. 1-72 (2021), https://scholarship.law.duke.edu/faculty_scholarship/4115/.

³² Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Conference on Fairness, Accountability, and Transparency, 81 Proceedings of Machine Learning Research pp. 1-15 (2018), <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.

³³ Nilay Patel, *Clearview AI and the end of privacy*, with author Kashmir Hill, The Verge (October 17, 2023), <https://www.theverge.com/23919134/kashmir-hill-your-face-belongs-to-us-clearview-ai-facial-recognition-privacy-decoder>.

³⁴ Kashmir Hill and Ryan Mac, *'Thousands of Dollars for Something I Didn't Do'*, The New York Times (updated April 6, 2023), <https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html>; Benj Edwards, *Innocent pregnant woman jailed amid faulty facial recognition trend*, ArsTechnica (August 7, 2023), <https://arstechnica.com/information-technology/2023/08/innocent-pregnant-woman-jailed-amid-faulty-facial-recognition-trend/>.

³⁵ Connor O'Sullivan, *Unmasking AI's Detrimental Effects on the Trans Community*, Medium: Towards Data Science (June 20, 2023), <https://towardsdatascience.com/unmasking-ais-detrimental-effects-on-the-trans-community-d8f870949d79>.

³⁶ Merve Hickock, *Comments of Merve Hickok to the Office of Management and Budget (OMB) regarding the Draft Memorandum published in Federal Register 88 FR 75625*, (November 4, 2023).



varies depending on the situation and cultural context.³⁷ These may also discriminate against people with disabilities, such as facial disorders, disfigurement, autism, or social anxiety.

Thank you for your consideration of our views. We ask that this statement be included in the hearing record. We would be pleased to provide you and your staff with additional information.

Sincerely yours,

A handwritten signature in blue ink, appearing to read "Marc Rotenberg".

Marc Rotenberg
CAIDP Executive Director

A handwritten signature in blue ink, appearing to read "Merve Hickok".

Merve Hickok
CAIDP President

A handwritten signature in black ink, appearing to read "Christabel Randolph".

Christabel Randolph
Law Fellow

A handwritten signature in black ink, appearing to read "Natalia Alarcón Rueda".

Natalia Alarcón Rueda
Research Assistant

A handwritten signature in black ink, appearing to read "Maanas Sharma".

Maanas Sharma
Research Assistant

³⁷ Tuan Le Mau, et al., *Professional actors demonstrate variability, not stereotypical expressions, when portraying emotional states in photographs*, 12 *Nature Communications* 5037 (August 19, 2021), <https://doi.org/10.1038/s41467-021-25352-6>.