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 Syste*m, 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 240, 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-revewed published articles in scientific journals"); Ohio v. Shaw, CR-13-575691 at *8 (Oct. 10, 2014), http://www.cybgen.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

bConnected
powered by Google

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
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>