Appellate Case No. C089567

IN THE COURT OF APPEAL FOR THE STATE OF CALIFORNIA
THIRD APPELLATE DISTRICT

THE PEOPLE OF THE STATE OF CALIFORNIA,

Petitioner and Appellant,
v.

ALVIN LARRY DAVIS,

Defendant and Respondent.

Appeal from the Superior Court for the County of San Joaquin
The Honorable George Abdallah, Jr., Judge
Case No. STKCRFE20160004780

APPLICATION OF ELECTRONIC FRONTIER FOUNDATION FOR LEAVE TO FILE BRIEF AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT AND RESPONDENT

Kit Walsh (SBN 303598)
kit@eff.org
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: 415.436.9333
Fax: 415.436.9993

Counsel for Amicus Curiae
Electronic Frontier Foundation

APPLICATION FOR LEAVE TO FILE BRIEF AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT AND RESPONDENT[1]

Pursuant to California Rule of Court 8.200(c), the Electronic Frontier Foundation respectfully requests permission to file the attached brief as *amicus curiae* in support of Petitioner and Appellant.

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for 30 years. With over 30,000 active donors, EFF represents the interests of people impacted by new technologies in court cases and broader policy debates surrounding the application of law in the digital age. EFF has special familiarity with and interest in constitutional issues that arise with new forensic technologies and has served as amicus in cases regarding a defendant's right to confront forensic DNA software. E.g., *United States v. Lafon Ellis*, No. 19-369, 2021 WL 1600711 (W.D. Pa. Apr. 23, 2021); *State v. Pickett*, 466 N.J. Super. 270, 246 A.3d 279 (App. Div. 2021); *People v. Johnson*, No. F071640, 2019 WL 3025299 (Cal. Ct. App. July 11, 2019). EFF has also participated in the U.S. Government Accountability Office's recent inquiry

[1] Pursuant to California Rule of Court 8.200(c)(3), undersigned counsel certifies that this brief was not authored in whole or in party by any party of any counsel for a party in the pending appeal and that no person or entity other than *amicus* made any monetary contribution intended to fund the preparation or submission of this brief.

regarding forensic technology, including probabilistic genotyping, which was prompted by concerns from elected officials about the use of these technologies in criminal proceedings. *See Forensic Technology: Algorithms Used in Federal Law Enforcement,* U.S. GOVERNMENT ACCOUNTABILITY OFFICE (May 12, 2020), https://www.gao.gov/products/gao-20-479sp.[2]

For the foregoing reasons, *amicus curiae* respectfully requests that the Court accept the accompanying brief on the merits for filing in this case.

Dated: May 7, 2021

Respectfully submitted,

/s/ Kit Walsh
Kit Walsh (SBN 303598)
kit@eff.org
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: 415.436.9333
Fax: 415.436.9993

Counsel for Amicus Curiae
Electronic Frontier Foundation

[2] All Internet citations last visited April 27, 2021.

Appellate Case No. C089567

IN THE COURT OF APPEAL FOR THE STATE OF CALIFORNIA
THIRD APPELLATE DISTRICT

THE PEOPLE OF THE STATE OF CALIFORNIA,

Petitioner and Appellant,
v.

ALVIN LARRY DAVIS,

Defendant and Respondent.

Appeal from the Superior Court for the County of San Joaquin
The Honorable George Abdallah, Jr., Judge
Case No. STKCRFE20160004780

AMICUS BRIEF OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT AND RESPONDENT

Kit Walsh (SBN 303598)
kit@eff.org
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: 415.436.9333
Fax: 415.436.9993

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF INTERESTED ENTITIES OR PERSONS

Amicus curiae Electronic Frontier Foundation ("EFF") is a non-profit organization and is not a party to this action. Pursuant to California Rule of Court 8.208, EFF hereby states that no entity or person has an ownership interest of 10% or more in EFF, and EFF knows of no person or entity that has a financial or other interest in the outcome of the proceeding under Rule 8.208.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Constitutional Provisions

ISSUE PRESENTED

Whether a defendant's rights of due process and confrontation include the ability to examine the source code of forensic software used by the prosecution to establish guilt.

INTEREST OF THE AMICUS CURIAE

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for 30 years. With over 30,000 active donors, EFF represents the interests of people impacted by new technologies in court cases and broader policy debates surrounding the application of law in the digital age. EFF has special familiarity with and interest in constitutional issues that arise with new forensic technologies and has served as amicus in cases regarding a defendant's right to confront forensic DNA software. *E.g.*, *United States v. Lafon Ellis*, No. 19-369, 2021 WL 1600711 (W.D. Pa. Apr. 23, 2021); *State v. Pickett*, 466 N.J. Super. 270, 246 A.3d 279 (App. Div. 2021); *People v. Johnson*, No. F071640, 2019 WL 3025299 (Cal. Ct. App. July 11, 2019) (unpublished). EFF has also participated in the GAO's recent inquiry regarding forensic technology, including probabilistic genotyping, which was prompted by concerns from elected officials about the use of these technologies in criminal proceedings. *See Forensic Technology: Algorithms Used in Federal Law Enforcement,* U.S. GOVERNMENT ACCOUNTABILITY OFFICE

(May 12, 2020), https://www.gao.gov/products/gao-20-479sp.[3]

[3] All Internet citations last visited April 27, 2021.

POINTS AND AUTHORITIES

Is STRmix a widely-understood and vetted technology? Or does it function according to trade secrets in the source code that are, by definition, secret? Plainly the answer cannot be both. What we do know for sure is this: STRmix has been neither subjected to rigorous independent testing nor shown to contain any information technologies that qualify for trade secret protections at all.

Independent review of the source code of probabilistic genotyping technology, including STRmix, is an essential step in evaluating and unearthing errors in these forensic tools, errors that could cause the conviction of innocent people. The financial interests of a private party cannot override the fundamental rights of due process and confrontation enshrined in the United States and California Constitutions; to the contrary, a criminal defendant is entitled to analyze and respond to the prosecution's evidence and cannot be required to blindly accept the claims of a forensic technology vendor. No questioning of the designer or vetting of an abstract algorithm can substitute for independent analysis of the code itself or satisfy the constitutional protections that prevent injustice in criminal prosecutions.

Where both the defendant and the public have compelling interests in the guarantees of a fair and public trial, public disclosure should be the rule. Denying the defense access to the code deprives the accused of the ability to challenge the evidence's admissibility or to meaningfully confront the evidence against them.

For these reasons, this Court should rule that Mr. Davis is entitled to the source code so that the defense may mount a challenge to STRmix's admissibility during a *Kelly/Frye* hearing, and, if the STRmix results are admitted, may properly confront the evidence against him.

I. The Confrontation Clause and Due Process requires disclosure of the source code of forensic software used to inculpate the defendant.

The United States Constitution and Califonia Constitution guarantee an accused the right to review and meaningfully confront the prosecution's evidence. U.S. Const. amend. VI; Cal. Const. Art.1, § 15. In order to adequately protect a defendant's constitutional rights, evidence relied upon by the prosecution—including privately owned forensic software source code—must be disclosed.

Failure to disclose STRmix's source code violates Mr. Davis's right to confront the evidence against him. Source code dictates the operation of an electronic program and is comprised of letters, numbers, symbols, and punctuation marks that often contain material errors. The code can also reveal which operations and assumptions are incorporated into a program and their effect on the outputted forensic evidence. These assumptions are central to establishing the reliability of the program and the evidence offered as proof of guilt; the defense must be allowed to review the source code in order to understand, meaningfully challenge, and confront the State's evidence of identity—the essential element in this case where Mr. Davis has maintained his innocence.

Moreover, the California Penal Code section 1054.1 specifically provides for the production of "(c) All relevant real evidence seized or obtained as a part of the investigation of the offenses charged"; and "(f) Relevant written or recorded statements of witnesses or reports of the statements of witnesses…, including any reports or statements of experts made in conjunction with the case, including the results of physical or mental examinations, scientific tests, experiments, or comparisons."

The prosecution relied heavily on the STRmix analysis in its case against Mr. Davis. Thus, Mr. Davis had statutory and Constitutional rights to review STRmix's source code.

A. It is a routine occurrence to discover software errors via adversarial and independent analysis.

Software errors are extremely common. As software becomes ever more complex and regularly interacts with increasingly complicated systems, these bugs become harder to prevent. Some, like those that may cause a program to crash, are fairly easy to discover. Others are not; while the software may appear to function properly, it may in truth output incorrect results, often going undiscovered for years. And each new version of a software introduces new code and the possibility of additional errors.

These errors can be caused by anything from creator bias coded into the program to misplaced punctuation. By way of example, the hole in the ozone layer went undiscovered for years because NASA's software was programmed to ignore outlier data the original programmers assumed was unrealistic.[4] A misplaced less-than (<) symbol in Ireland's National Integrated Medical Imaging System may potentially have led to thousands of incorrectly recorded MRIs, X-rays, and CT scans that, in turn, may have led to unnecessary medical procedures.[5] In rare cases, the errors may even have been intentional, as was the case with Volkswagen software designed to make its vehicles produce inaccurate emissions readings during testing.[6]

As with all complex software, modern forensic technology poses similar risk of error. Most of these errors are not discoverable by merely questioning the program's creators or users; rather, independent public scrutiny and testing is the best—and often only—way to unearth them. To

[4] *Research Satellites for Atmospheric Sciences, 1978-Present, Serendipity and Stratospheric Ozone*, NASA'S EARTH OBSERVATORY, , https://earthobservatory.nasa.gov/Features/RemoteSensingAtmosphere/remote_sensing5.php (last visited Apr. 27, 2021).

[5] Jack Power, *Software company behind HSE scan glitch begins investigation*, THE IRISH TIMES (Aug. 5, 2017), https://www.irishtimes.com/news/ireland/irish-news/software-company-behind-hse-scan-glitch-begins-investigation-1.3178349.

[6] Sonari Glinton, *How A Little Lab In West Virginia Caught Volkswagen's Big Cheat*, NPR MORNING EDITION (Sept. 24, 2015), http://www.npr.org/2015/09/24/443053672/how-a-little-lab-in-west-virginia-caught-volkswagens-big-cheat.

this end, the President's Council of Advisors on Science and Technology ("PCAST") issued a report in 2017 emphasizing the need for independent review of probabilistic DNA programs to determine, in part, "whether the software correctly implements the methods" on which the analysis is based.[7]

B. Analyzing the source code is critical to determining the reliability—and therefore admissibility—of probabilistic DNA tools like STRmix.

The necessity of independent source code review for probabilistic DNA programs was starkly demonstrated when FST (a counterpart to STRmix that was used in New York crime labs) was finally provided to a defense team for analysis. According to a defense expert, the undisclosed portion of the code could incorrectly tip the scales in favor of the prosecution's hypothesis that a defendant's DNA was present in a mixture. Reply Mem. of Law in Supp. as to Kevin Johnson at 19-21, *United States v. Kevin Johnson*, (S.D.N.Y. Feb. 27, 2017) (No. 15-CR-565 (VEC), D.I. 110). In fact, STRmix[8] has suffered from programming errors that created

[7] The President's Council of Advisors on Science and Technology (PCAST), Report to the President: Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods 79 (Sept. 2016),, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

[8] It is unclear whether that version of STRmix is the same as the one used in this case.

false results in 60 cases in Queensland, Australia.[9]

The problems caused by nondisclosure are especially acute in the context of the latest generation of probabilistic DNA analysis because there is no objective baseline truth against which the output from the program may be evaluated—and thus it is impossible to gauge the accuracy of these programs by examining their results. The importance of such a baseline is demonstrated in the breathalyzer context. It is possible to determine, as an objective fact, the parts per million of alcohol in the air using existing non-portable technology. Thus, emerging portable devices can be evaluated by comparing their results with the factual measurement.[10]

Unlike breathalyzers, the latest generation of complex DNA analysis tools cannot be measured against an objective truth. Instead, these DNA

[9] David Murray, *Queensland authorities confirm 'miscode' affects DNA evidence in criminal cases*, COURIER MAIL (Mar. 20, 2015), http://www.couriermail.com.au/news/queensland/queensland-authorities-confirm-miscode-affects-dna-evidence-in-criminal-cases/news-story/833c580d3f1c59039efd1a2ef55af92b.

[10] Nonetheless, numerous states require disclosure of the source code for breath-testing machines. *See e.g., State v. Underdahl*, 767 N.W.2d 677 (Minn. 2009) (potential defects that could be detected in breathalyzer source code warranted order to disclose complete source code); *State v. Chun*, 194 N.J. 54, 123 (2008) (noting that the court had previously remanded to allow defense examination of breathalyzer source code); *People v. Robinson*, 860 N.Y.S.2d 159 (2d Dept. 2008); *see also Davenport v. State*, 289 Ga. 399, 404 (2011) (Nahmias, J., concurring) (noting potential due process concerns if source code for forensic machines could not be discovered, lauding majority decision for rejecting such a conclusion and remanding).

programs are more akin to probabilistic election forecasting models, such as those designed by FiveThirtyEight and The Economist. The outputted results are based on the calculation of the probability of events—that the defendant, rather than a random person, contributed to the DNA mixture or that person X will win an election—a value that is not an objectively measurable fact. This is why different DNA programs, and even different laboratories using the same program, will generate substantially different results for the same sample. Each DNA analysis is specific to the sample that was tested, the program and version that was used, the conditions in the lab, and any additional input used in the analysis.

Furthermore, the sample analysis is dictated by the assumptions programmed into the software. This creates the worrisome reality that softwares like STRMix and its alternatives provide divergent probability calculations from one another—a discrepancy that can mean the difference between exculpation and inculpation. In one case, TrueAllele, an alternative to STRmix, calculated a match statistic of 189 billion, while another competitor's match statistic was 13,000—a more than 14-million-fold difference. *See Commonwealth v. Foley*, 38 A.3d 882, 887, 890 (Pa. Super. Ct. 2012).

One of the reasons for such drastic differences between the results of DNA analysis tools is that they take different approaches to the random effects that can alter results, from trying to conteract them to ignoring them altogether. *See People v. Collins*, 49 Misc.3d 595, 600, 604-06 (N.Y. Kings Co. Sup. Ct. 2015) (discussing stochastic effects in context of analyzing admissibility of probabilistic genotyping program). For example, DNA software are all subject to the random phenomena "allelic drop-out" rate and "allelic drop-in" rate. *Id.* at 605-06. The former refers to the rate at which the software ignores alleles (DNA patterns) and the latter is the rate of falsely reporting their presence. *Id*. at 605-06. Other common but more complicated phenomena, such as "exaggerated stutter" and "peak height imbalance," may also create the appearance of DNA patterns that are in fact absent, or incorrectly indicate the prevalence of certain patterns. *Id.* at 606-610.

A higher statistical number does *not* mean that the software outputting it is more accurate, and may purely result from how the various assumptions were programmed or ignored in the software's design. But the higher numbers sound compelling and owners of these probabilistic programs may have an incentive to structure their product to output larger numbers in an effort to give the impression of higher precision.

The programmed assumptions, and the exact way they are coded into the software, are critical to the defense's ability to identify areas for challenges to its reliability and accuracy. Information regarding how STRmix is *supposed* to work is simply insufficient for the defense's arguments opposing STRmix's admissibility at a *Kelly/Frye* hearing. The *only* method of ascertaining precisely how these myriad effects are accounted for, if at all, is to examine the source code.

C. The Confrontation Clause entitles the defense to review the prosecution's evidence to allow for meaningful examination during a *Kelly/Frye* hearing and at trial.

Meaningful confrontation of the STRmix analysis on the shoelace and other items from the crime scene necessarily depends on Mr. Davis's access to and opportunity to review the source code and the assumptions embedded within it.

Recently, federal and state courts have recognized that disclosure of the source code of probabilistic DNA programs is necessary for conducting a *Daubert* or *Frye* hearing. *See, e.g.*, *United States v. Ellis,* No. 19-369, 2021 WL 1600711 (W.D. Pa. Apr. 23, 2021); *State v. Pickett*, 466 N.J. Super. 270 (App. Div. 2021). Failure to disclose the source code not only prevents the defense from being able to cross-examine the evidence at trial but also "substantially hinders defendant's opportunity to meaningfully challenge reliability at a *Frye* hearing." *Pickett*, 466 N.J.Super. at 306.

A fair trial necessitates that the accused "be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; [and] to have compulsory process for obtaining witnesses in his favor." U.S. Const. amend. VI; see also Cal. Const. Art. 1, §15. This is a procedural right and cannot be disposed of simply because the evidence *appears* reliable. *See Crawford v. Washington*, 541 U.S. 36, 62 (2004)

(“Dispensing with confrontation because testimony is obviously reliable is akin to dispensing with jury trial because a defendant is obviously guilty.”). The Confrontation Clause’s animating concern is “to ensure the reliability of the evidence . . . by subjecting it to rigorous testing.” *Maryland v. Craig*, 497 U.S. 836, 845 (1990). The Supreme Court has recognized that this concern applies with full force to forensic evidence. *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 310, 313 (2009) (holding that affidavits reporting the results of a forensic analysis of seized drugs are testimonial and subject to the Confrontation Clause); *Bullcoming v. New Mexico*, 564 U.S. 647, 663–64, 666 (2011) (holding that certification on a forensic laboratory report is testimonial and defendant has a right to confront the specific analyst who made the certification).

In the modern context, black-box technologies like STRmix squarely parallel the *ex parte* examinations that motivated the founders to adopt the Confrontation Clause in the first place. Performed at the government’s demand, intentionally opaque in its operation, and unduly impressive to the jury, STRmix renders the defendant powerless both to test the credibility of the source and to undermine the state’s case against him. One side (the prosecution) has the use of evidence denied to the opposing party and reasonably believed to be essential to a fair resolution of the lawsuit. Disclosure is thus necessary to ensure that Mr. Davis may examine the program methodology for accuracy, functionality and credibility in order to meaningfully confront the test results and receive a "fair trial, understood as a trial resulting in a verdict worthy of confidence." *Kyles v. Whitley*, 514 U.S. 419, 434 (1995).

CONCLUSION

For these reasons, STRmix's source code should be disclosed to enable Mr. Davis to meaningfully challenge the admissibility of STRmix's results and the evidence against him.

Dated: May 7, 2021

Respectfully submitted,

/s/ Kit Walsh
Kit Walsh (SBN 303598)
kit@eff.org
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: 415.436.9333
Fax: 415.436.9993

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF WORD COUNT

I certify pursuant to California Rules of Court 8.204 and 8.504(d) that this *Amicus Curiae* Brief of Electronic Frontier Foundation is proportionally spaced, has a typeface of 13 points or more, contains 2,590 words, excluding the cover, the tables, the signature block, and this certificate, which is less than the total number of words permitted by the Rules of Court. Counsel relies on the word count of the Microsoft Word word-processing program used to prepare this brief.

Dated: May 7, 2021

/s/ Kit Walsh
Kit Walsh

CERTIFICATE OF SERVICE

I, Victoria Python, declare:

I am a resident of the state of California and over the age of eighteen years and not a party to the within action. My business address is 815 Eddy Street, San Francisco, California 94109.

On May 7, 2021, I served the foregoing documents:

APPLICATION OF ELECTRONIC FRONTIER FOUNDATION FOR LEAVE TO FILE BRIEF AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT AND RESPONDENT

AND

***AMICUS* BRIEF OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT AND RESPONDENT**

X BY TRUEFILING: I caused the foregoing documents to be filed and served with the court using the court's e-filing system, TrueFiling. The parties and/or counsel of record are designated for electronic service in this matter on the TrueFiling website.

Kelly E. LeBel
Office of the State Attorney General
P.O. Box 944255
Sacramento, CA 94244-2550

Counsel for Plaintiff and Respondent

Byron Charles Lichstein
Attorney at Law
2852 Willamette Street., #164
Eugene, OR 97405

Counsel for Defendant and Appellant

X BY FIRST CLASS MAIL: I caused the foregoing documents to be placed in an envelope for collection and mailing following our ordinary business practices. On the same day that correspondence is placed for collection and mailing, it is deposited in the ordinary course of business with the United States Postal Service, in a sealed envelope with postage fully prepaid.

San Joaquin County D.A.'s Office
222 E. Weber Ave., #202
Stockton, CA 95202

Superior Court of California,
San Joaquin County Appeals Dept.
180 E. Weber Ave., Ste. 230
Stockton, CA 95202

Alvin Larry Davis, #BJ4527
CHCF
P.O. Box 31960
Stockton, CA 95213

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Victoria
Victoria Python