STATE OF NEW JERSEY,

Plaintiff-Respondent,

v.

COREY PICKETT,

Defendant-Movant.

SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION

DOCKET NO. **A-4207-19T2**

CRIMINAL ACTION

ON LEAVE GRANTED TO APPEAL AN INTERLOCUTORY ORDER OF THE SUPERIOR COURT OF NEW JERSEY, LAW DIVISION, HUDSON COUNTY.

INDICTMENT NO. 17-07-470-I

Sat Below:
Hon. Patrick J. Arre,
J.S.C.

BRIEF OF AMICUS CURIAE UPTURN, INC. IN SUPPORT OF MOVANT-APPELLANT

William Singer, Esq.
Attorney ID No. 272741971
Singer & Fedun, LLC
2230 Route 206
P.O. Box 134
Belle Mead, NJ 08502
Tel: 908-359-7873
wsinger@singerfedun.com

Kendra K. Albert
Admitted pro hac vice
Cyberlaw Clinic
Harvard Law School
1585 Massachusetts Ave.
Cambridge, MA 02138
Tel: 617-998-1558
kalbert@law.harvard.edu

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

PRELIMINARY STATEMENT AND STATEMENT OF INTEREST

Independent and adversarial review of software used in the criminal legal system is necessary to protect the courts from unreliable evidence and to ensure that the introduction of new technology does not disadvantage the accused. Though such review has detected outcome-determinative errors in probabilistic genotyping software in the past, yet TrueAllele has never been subject to such review. Amicus Upturn respectfully requests that this Court grant the defense expert reviewer access to TrueAllele under the terms requested by the defendant. This access is necessary to determine whether TrueAllele is reliable enough to be used in this case and to ensure that the proprietary interests of software developers do not undermine the integrity of the criminal legal system.

Upturn is a nonprofit organization based in Washington, D.C. that seeks to advance equity and justice in the design, governance, and use of technology. Upturn frequently presents its work in the media, before Congress and regulatory agencies, and before the courts in briefs like this one. Upturn has an interest in seeing that forensic technology is not deployed in a way that promotes private interests at the expense of fairness and justice in the criminal legal system.

PROCEDURAL HISTORY AND STATEMENT OF FACTS

Amicus Upturn relies on the procedural history and statement of facts as presented by the defense.

ARGUMENT

I. TrueAllele combines forensic science and software engineering, each of which has its own risks and histories of failure.

Cybergenetics's DNA analysis software, TrueAllele, implements probabilistic genotyping in computer code to attempt forensic identification. One can think of TrueAllele as having three layers, each of which has its own points of failure. The first point of failure of TrueAllele is its complex and novel scientific method—probabilistic genotyping. The second point of failure is the statistical models, developed by Cybergenetics itself, through which TrueAllele carries out the probabilistic genotyping analysis. The third point of failure of TrueAllele is software code, authored by Cybergenetics itself, that implements the probabilistic genotyping algorithms. Failure at any of these points may have harmful, and even fatal, consequences.

A. Flawed forensic science has been used to convict and execute defendants before being subjected to appropriate scrutiny.

The first point of failure for software like TrueAllele is the scientific basis it uses to draw evidentiary conclusions. Here, there are many reasons to be cautious. Numerous evidentiary techniques, initially hailed as groundbreaking and relied on in criminal convictions, have been either found to have significant errors or completely debunked. Arson science used to secure the death sentence of Cameron Todd Willingham was "scientifically proven to be invalid" by both a government commission and an independent review by a panel of fire experts, but only after he had been executed. David Grann, Trial by Fire, The New Yorker

(Aug. 31, 2009).[1] The resulting national uproar and fundamental reexamination of arson science led to the exoneration of Texas inmate Ed Graf, but only after Graf had already served 26 years in prison. Jeremy Stahl, The Trials of Ed Graf, Slate (Aug. 16, 2015).[2] And in 2015, the FBI formally acknowledged flaws in its forensic hair analysis used in thousands of trials spanning a period of over two decades. Spencer S. Hsu, FBI Admits Flaws in Hair Analysis over Decades, Wash. Post (Apr. 18, 2015).[3] This flawed analysis was used against thirty-two people who were sentenced to death, fourteen of whom had already been executed or died in prison. Ibid. This history of flawed forensic science underscores that new forensic methods, such as probabilistic genotyping, must be subject to rigorous review to prevent wrongful convictions and executions.

B. Software engineering can independently introduce fatal flaws even when the underlying scientific methods are sound.

Software can allow more efficient and comprehensive data analysis—but it can also be biased, faulty, or completely ineffective. At the design stage, the process of creating software necessarily includes decisions and assumptions.

---

[1] https://www.newyorker.com/magazine/2009/09/07/trial-by-fire.
[2] http://www.slate.com/articles/news_and_politics/jurisprudence/2015/08/ed_graf_arson_trial_texas_granted_him_a_new_trial_would_modern_forensic.html.
[3] https://www.washingtonpost.com/local/crime/fbi-overstated-forensic-hair-matches-in-nearly-all-criminal-trials-for-decades/2015/04/18/39c8d8c6-e515-11e4-b510-962fcfabc310_story.html.

TrueAllele is no exception. It is these differing design decisions that have resulted in variability in conclusions across probabilistic genotyping software. For example, in a New York case TrueAllele and another probabilistic genotyping software produced different conclusions on the defendant's guilt for the same mixed DNA sample. 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 78 n.212 (2016) [hereinafter PCAST Report].[4] This is not a flaw by itself; Cybergenetics should design their own models and write their own code to implement probabilistic genotyping. In fact, these design and programming choices are the precise reason why TrueAllele's developers want to safeguard their code. However, the defense must have access to information about these design choices because they can influence ostensibly objective results. For example, the Forensic Statistical Tool, a peer to TrueAllele, was found in a 2016 source code review to have a hidden function that tended to overestimate the likelihood of guilt. See Stephanie J. Lacambra et al., Opening the Black Box: Defendants' Rights to Confront Forensic Software, NACDL: The Champion (May 2018). Without independent review of TrueAllele's source code, there is no guarantee that TrueAllele does not have

[4] https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

similar outcome-determinative functions that may also lead to wrongful convictions and potentially fatal consequences.

Even when software is not designed with faulty assumptions, unintentional errors can significantly impact the software's performance. Just this year, the UK's Most Serious Violence tool, a flagship artificial intelligence system designed to predict future gun and knife violence, was found to have coding flaws that experts concluded made it unusable. Matt Burgess, Police Built an AI to Predict Violent Crime. It Was Seriously Flawed, Wired (Aug. 6, 2020).[5] After discovery of a coding error that caused training data to be improperly ingested, the system, originally claimed by its developer to be up to seventy-five percent accurate, was demonstrated to be less than twenty percent accurate. Ibid. And in 2015, investigators in Australia encountered an error in their use of STRmix, a probabilistic genotyping software program intended to resolve mixed DNA profiles similar to TrueAllele. David Murray, Queensland Authorities Confirm 'Miscode' Affects DNA Evidence in Criminal Cases, The Courier Mail (Mar. 20, 2015).[6] The error produced incorrect results in at least sixty criminal cases, including a high-profile murder case. Ibid. This is especially concerning given STRmix's striking similarities to TrueAllele—both are

[5] https://www.wired.co.uk/article/police-violence-prediction-ndas.

[6] https://www.couriermail.com.au/news/queensland/queensland-authorities-confirm-miscode-affects-dna-evidence-in-criminal-cases/news-story/833c580d3f1c59039efd1a2ef55af92b.

forensic identification software systems that use probabilistic genotyping.

C. Allowing companies to shield their software from review increases the risk of undetected failures.

As New Jersey courts have recognized across other contexts, there is no substitute for independent and searching review to find flaws in software that puts people's lives at stake. When such testing is not permitted, the consequences are disastrous.

Perhaps the most striking recent example is the failure of the Boeing 737 Max 8 airplanes in 2018 and 2019, which killed 346 people and led to the grounding of over 300 737 Max passenger jets worldwide. Boeing was able to evade independent review—a cautionary tale that shows the consequences of letting financial concerns take priority over human life. The Federal Aviation Administration (FAA) did not thoroughly test Boeing's new Maneuvering Characteristics Augmentation System (MCAS) software because Boeing stated the software was not "safety critical." This software, designed to counteract the weight of new, larger engines, ultimately malfunctioned and led to two crashes. The FAA should have served as an independent inspector, but delegated too much of its responsibility to Boeing itself. See Committee on Transportation and Infrastructure, Final Committee Report: The Design, Development, and Certification of the Boeing 737 Max 57 (Sep. 15, 2020). Boeing was thus able to conceal internal flight simulation testing data that showed pilots took more than twice the time to mitigate an MCAS activation than

federal guidelines allow for. Ibid. at 13 & n.66. A technical review found that the FAA was "unable to independently assess the adequacy . . . of MCAS, which was a new and novel feature that should have been closely scrutinized. Had FAA technical staff been fully aware of the details of MCAS, they would have likely identified the potential for the system to overpower other flight controls, which was a major contributing factor leading to the two MAX crashes." Id. at 66–67. Like Boeing, TrueAllele has relied upon self-validation: the main developer of TrueAllele, Mark Perlin, has co-authored the majority of the validation studies done on TrueAllele. In fact, there has never been a complete external review of TrueAllele's source code, nor has there ever been independent and adversarial testing of TrueAllele's software to see how it performs under different conditions. Whether Cybergenetics is aware of flaws in TrueAllele or not, without independent review, defects in TrueAllele may go unidentified just in Boeing's MCAS.

The lack of independent external review in both cases is enabled by the failure of safeguards meant to prevent such cases. Regulatory capture in the aerospace industry led to Boeing's dedicated FAA reviewers failing to scrutinize the 737 Max thoroughly, in some instances bringing up concerns with Boeing but failing to include those concerns in their report to the FAA itself. Id. at 69–70. In the criminal legal system, rather than a regulatory body, courts and the adversarial process are the safeguards meant to ensure that evidence

generated by new technologies is reliable and appropriately used. To uphold its role as a safeguard against wrongful convictions based on questionable evidence, this Court must ensure TrueAllele is thoroughly tested and scrutinized.

This Court should also consider the incentives that Cybergenetics has to shield its technology from review. Perlin has testified that Cybergenetics has invested millions in TrueAllele, and that allowing independent review would pose an unacceptable financial risk. See Decl. of Mark W. Perlin, at ¶ 68, Washington v. Fair, No. 10-1-09274-5 SEA (Sup. Ct. King Cnty. Wash.). Cybergenetics has placed untenable limitations on defense access to TrueAllele's source code, even under a protective order, because its code constitutes trade secrets. But the Boeing example has shown that, when a company is acting based on monetary interests, harmful trade-offs may be made between profit and safety or reliability. In the criminal legal system in particular, TrueAllele's monetary and proprietary interests to shield its technology from review should not outweigh the liberty interests at stake for defendants convicted based on TrueAllele-produced evidence.

II. Each aspect of TrueAllele must be subject to independent and adversarial review to ensure its reliability.

In New Jersey, the standard for admitting new scientific evidence in criminal cases centers around the question of "reliability.". See State v. Chun, 194 N.J. 54 (2008). For TrueAllele, this question cannot be properly addressed without

independent and adversarial review. TrueAllele's first and second layers—the underlying method and statistical models—must be subject to independent validation studies to determine the reliability of the underlying method as well as TrueAllele's specific approach and its limitations. For the third layer—TrueAllele's implementation in software—in addition to testing, direct source code review is necessary to trace how design specifications were implemented and to identify errors.

A. The reliability of TrueAllele's approach to probabilistic genotyping has only been partially addressed through existing validation studies.

Even aside from issues of self-validation, software validation and developmental validation of forensic methods are different. Although validation studies may be able to determine the validity of a scientific method, and perhaps even prevent against failures in translating assumptions to software code, they cannot fully guard against either coding or user error. For example, validation studies are performed on specific versions of the software. It is common for errors in coding to be introduced when new versions are released.

The version of the TrueAllele software used in Mr. Pickett's case postdates every one of the validation studies cited in the report prepared by Cybergenetics, as well as those cited in the initial state's brief in favor of the admission of TrueAllele. Da19-21. None of the peer-reviewed studies listed as part of the state's appendix appear to be performed on the version of the

VUIer client (which is responsible for the match statistic) used in this case. Ra454-55. Prior validation studies cannot replace source code review because subsequent source code versions may introduce new errors not present when validation was completed.

B. TrueAllele's source code has not been independently reviewed.

Independent review of TrueAllele's source code is a basic, necessary step to ensuring that TrueAllele is reliable. See Darrel C. Ince et al., The Case for Open Computer Programs, Nature (Feb. 22, 2012) (explaining that "anything less than the release of source programs is intolerable for results that depend on computation"). Specifically, this level of review is a necessary condition of ensuring the software is properly implementing a program's design specifications and that the code is devoid of bugs that could affect the software's output. See Lacambra et al., at 32 (stating "programmed assumptions . . . must be reviewed at the source code level for reliability and accuracy"). The code in TrueAllele has never been scrutinized by any party outside of Cybergenetics. See Natalie Ram, Innovating Criminal Justice, 112 Nw. U. L. Rev. 659, 661 (2018) (noting that "no one outside of Cybergenetics—Perlin's company—has seen or examined that source code"). However, adversarial and independent source code review—particularly when performed by a defense expert—is a necessary safeguard that prevents probabilistic genotyping programs from doing serious harm.

Despite its limitations, source code review was able to catch

errors in the Forensic Statistical Tool (FST), the aforementioned probabilistic genotyping program formerly used in New York. In the course of a murder trial, the court granted a defense expert full access to the program's source code. See Lauren Kirchner, Where Traditional DNA Testing Fails, Algorithms Take Over, ProPublica (Nov. 4, 2016).[7] This analysis produced two alarming observations. First, the code did not seem to be implementing the methods and models that were used in FST's validation studies. See Jessica Goldthwaite et al., Mixing It Up: Legal Challenges to Probabilistic Genotyping Programs for DNA Mixture Analysis, Champion (May 2018) at 12, 15 (noting "disturbing differences between what FST was initially advertised to be and what is actually being used in criminal casework"). Second, there seemed to be coding errors that caused results to favor the prosecution's theory of the case. See id.

This is why it is so important that New Jersey, as it has in the past, compel the release of proprietary source code to defense experts to prevent the potential damage new, unchecked technologies can cause. In a move aimed to protect the integrity of evidence obtained through the Alcotest 7110 breathalyzer, the Supreme Court of New Jersey compelled the breathalyzer's maker, Draeger Safety Diagnostics, to release its source code to defense experts. See Chun, 194 N.J. 54 (2008). In 2018, New

[7] https://www.propublica.org/article/where-traditional-dna-testing-fails-algorithms-take-over.

Jersey courts again took action to preserve the integrity of trial evidence, addressing calibration issues in Draeger technology used to obtain DWI convictions. See State v. Cassidy, 235 N.J. 482 (2018). Unlike Alcotest, TrueAllele has been subject to peer-reviewed studies and Cybergenetics allows for some inspection and review. But the proposed review conditions are inconsistent with determining reliability. In light of the gravity of these possible errors, this Court should move similarly to act as a steward of emerging forensic technologies and to subject TrueAllele to independent and adversarial review.

III. Admitting TrueAllele as scientific evidence into the New Jersey criminal court system without independent and adversarial review will harm the administration of justice.

In the criminal court system, the "gatekeeping" function of judges works in tandem with later procedural safeguards such as cross-examination and discovery rights to ensure that the accused is adequately protected from questionable evidentiary technology. Thus, requiring independent and adversarial review in the Frye hearing stage is not simply an option, but rather a necessity to preserve the integrity of the court system and the rights of defendants. Frye v. United States, 293 F. 1013 (D.C. Cir. 1923). New Jersey's emphasis on reliability as the standard for admitting new scientific evidence in criminal cases creates the obligation for judges to act as gatekeepers by excluding unreliable scientific evidence from criminal proceedings. New Jersey courts have historically embraced this role, even going

so far as to vacate prior convictions based on questionable scientific evidence en masse to preserve the interest of justice. See, e.g., Cassidy, 235 N.J. at 497 (holding that over 20,000 cases relying on potentially unreliable breathalyzer testing needed to be re-opened). The current question before the Court is not whether TrueAllele is scientifically valid, but rather whether, given the evidence in Parts I and II of this brief and the court's considerations of the administration of justice, TrueAllele can be adequately determined to be reliable without independent and adversarial review including full source code access. Upon consideration of the balance between private parties' interests and defendants' rights, it becomes clear that TrueAllele must be thoroughly reviewed, not just rubber stamped.

A. Admitting scientific evidence without independent and adversarial testing incentivizes secrecy and gives undue influence to private, corporate actors.

Although independent and adversarial review is functionally necessary to assess the reliability of new scientific evidence, trade secrets are often invoked to combat attempts at independent and adversarial review. Although often portrayed as protective measures, trade secrets should not be prioritized over considerations of justice. See Rebecca Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, 70 Stan. L. Rev. 1343, 1358–71 (2018) (noting how trade secret protections have led to increased secrecy and difficulty for defendants throughout the criminal

legal system). Corporations, which prioritize profits and competitive advantage, often argue that trade secrets are necessary for business interests. However, the idea that courts cannot protect both criminal defendants and corporate actors is a false dichotomy in light of existing procedural safeguards that can appropriately protect both private interests and the administration of justice. To faithfully conduct a Frye reliability analysis, independent and adversarial review and testing should not be impeded by trade secret protections. Rather, all relevant materials should be available to reviewing experts, with appropriate procedural safeguards in place.

While the doctrine of trade secrecy has sometimes been used reasonably in cases of extreme business need, the tendency of companies today is to "change the traditional function of trade secrecy from protecting against a competitor's misappropriation to a function that impedes public investigation." See Sonia K. Katyal, The Paradox of Source Code Secrecy, 104 Cornell L. Rev. 1183, 1246 (2019). This is particularly inappropriate in a Frye hearing analysis since it creates a "contradictory paradox of source code secrecy: on one hand, companies argue that their methods are sufficiently known and proven to be broadly accepted by the scientific community and yet, on the other hand, companies will go to enormous lengths to keep their source code confidential so as to preclude further investigation." Id. at 1242–43. This tendency of trade secret protections towards advancing secrecy at the expense of crucial analysis like

independent and adversarial testing is at odds with the aims of the criminal legal system—a system built upon revelation and truth seeking for the advancement of justice.

The emphasis on business prospects also leads companies to protect their interests through extreme penalties, further discouraging independent review and distorting the end goal of justice. In this case, the prosecution suggested a $1,000,000 liability if any "proprietary materials are improperly handled, negligently or otherwise." Da235. The State's concern for Cybergenetics's business prospects and the large monetary penalty warp the incentives of parties and detract from the central issue of finding and administering justice. Additionally, the State's attempt at imposing financial risk through a large monetary penalty without a clear definition of a breach highlights the undue influence that a corporation like Cybergenetics can have on criminal proceedings.

Asserting a trade secret privilege in order to avoid independent and adversarial review produces the precise injustice that the New Jersey criminal court system seeks to avoid. New Jersey's law on trade secret privilege in the criminal court system rejects any trade secret privilege that will "tend to conceal fraud or otherwise work injustice." N.J.S.A. 2A:84A-26. From a procedural standpoint, concealing information in a criminal case produces fundamental injustice because it stifles a defendant's rights and inhibits the adversarial methodology of the court system. Recognizing this

tendency, the United States Supreme Court has said "evidentiary privileges must be construed narrowly because privileges impede the search for the truth." Pierce County v. Guillen ex rel. Guillen, 537 U.S. 129, 144 (2003). Courts have recognized that trade secrets are not wholly independent concerns, prioritized above all other legal analysis, but rather, considerations that must not take precedence over substantial justice and an overall search for the truth. Therefore, trade secrets should only be invoked when they are absolutely necessary and do not impede the overall goals of the judicial system.

Traditionally, trade secret protections were intended to prevent malicious or accidental disclosures of vital information that could hurt a business prospect. These considerations have little relevance in the context of good-faith independent and adversarial review, aimed at investigating the reliability of the technology itself. Even if a court finds that disclosure is a valid concern, there are better ways to protect proprietary information than blocking source code review. Since source code is routinely produced during discovery in civil cases, "litigators have ready-made tools at their disposal to address the merit of software related disputes while ensuring that source code remains protected and yet disclosed in a litigation dispute." Katyal, at 1275–76. For example, New Jersey courts can issue protective orders to protect source code from disclosure. Thus, blocking production of key information needed to verify scientific evidence in a criminal court case on the basis of

trade secrets is not only a questionable prioritization of property over liberty, but also an unnecessary choice.

B. Allowing trade secrecy to prevent review violates the procedural rights of this defendant and future defendants.

Admitting scientific evidence without independent and adversarial review at the Frye hearing stage can hinder a defendant's ability to mount a defense and confront the basis of the prosecution's evidence in the subsequent criminal proceedings. Historically, New Jersey has prioritized defendants' rights in the context of considering new scientific evidence at every stage of criminal proceedings beginning with the Frye hearing. Although a defendant's rights are balanced against other interests, New Jersey law has consistently recognized the centrality of a defendant's potential loss of liberty in this analysis. Since reliability is the underlying evaluation in a New Jersey Frye hearing, access to every piece of information that may inform such a reliability assessment about the new scientific evidence should be considered.

Admitting scientific evidence without independent and adversarial review at the Frye hearing stage may not only allow unreliable evidence but also directly undermine other safeguards in the criminal legal system. Procedural safeguards in later parts of the criminal process afford defendants the opportunity to challenge admitted evidence. See Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 596 (1993) ("Vigorous cross-examination, presentation of contrary evidence, and

careful instruction on the burden of proof are the traditional appropriate means of attacking shaky but admissible evidence."). However, these subsequent safeguards are not always adequate. Defendants can experience substantial difficulty challenging "shaky evidence" when the inner workings of the tools that produced such evidence are not fully known. See State in Interest of A.B., 219 N.J. 542 (2014) (noting that "[a] criminal trial where the defendant does not have access to the raw materials integral to the building of an effective defense is fundamentally unfair" (internal quotations omitted)). For one thing, once evidence has been admitted, the onus is flipped to the defendant to compel discovery with a subpoena and argue the defense's necessity for this particular portion of information—the exact opposite of what the Daubert court had envisioned. See Katyal, at 1245. Moreover, the same trade secret protections that create opacity during a Frye hearing can continue to prohibit analysis at later stages of the criminal process. Thus, subsequent opportunities to address and attack the unreliability or secrecy of new scientific technology are never guaranteed to a defendant after the Frye hearing stage. Since a lack of independent and adversarial review at the Frye hearing stage cannot be replaced by subsequent procedural safeguards, the gatekeeping function of judges at the Frye hearing stage is fundamental to procuring justice.

The benefits of independent and adversarial review of forensic technologies extend beyond the life of a criminal case as well.

Rigorous scrutiny during a Frye hearing can help prevent future litigation if a technology is later proven to have been inaccurate. Not only is this desirable from a judicial economy perspective, vetting for inaccuracies at an early stage in litigation can also preventively protect against wrongful convictions, preserving both the court's integrity and future defendants' rights. In Cassidy, rigorous scrutiny of breathalyzer technology proved the test to be unreliable, causing the re-opening of 20,000 cases. See Cassidy, 235 N.J. at 482. While the Supreme Court of New Jersey's decision to remedy this injustice regardless of the administrative burden on the system is admirable, adequate scrutiny during earlier stages of the court proceedings could have prevented the need for re-litigation altogether. Catching errors at the first possible opportunity is particularly crucial within the criminal legal system, since re-litigation cannot always remedy the damages caused by admitting inaccurate scientific evidence. For example, in a 2018 study, the National Registry of Exonerations determined that the known false convictions in the United States since 1989 totaled 20,080 years behind bars. See Radley Balko, Report: Wrongful Convictions Have Stolen at Least 20,000 Years from Innocent Defendants, Wash. Post (Sept. 10, 2018).[8] Furthermore, in a legal system that has already been scrutinized

[8] https://www.washingtonpost.com/news/opinions/wp/2018/09/10/report-wrongful-convictions-have-stolen-at-least-20000-years-from-innocent-defendants/.

for its wide racial and economic disparities, issues of fairness are inherently issues of equity as well. See, e.g., Radley Balko, 21 More Studies Showing Racial Disparities in the Criminal Justice System, Wash. Post (Apr. 9, 2019).[9] Therefore, early application of independent and adversarial testing in the Frye hearing stage can be beneficial in terms of judicial economy and prevents perpetuation of future injustice.

CONCLUSION

Novel forensic methods and software used in the criminal legal system and other high-stakes contexts that have not been subject to sufficient review have historically had incredibly harmful consequences. For probabilistic genotyping in particular, STRmix and FST have both been revealed to have outcome-determinative errors. In the case of FST these errors were identified through independent source code review by the defense. While there is also a larger question of whether probabilistic technology should be used in the criminal legal system at all, cf. Emily Berman, Individualized Suspicion in the Age of Data, 105 Iowa L. Rev. 263 (2020), at minimum, the court should utilize its gatekeeping role in the Frye hearing stage to require independent and adversarial review of TrueAllele, including its source code, in the interest of preserving the integrity of the New Jersey criminal legal system.

[9] https://www.washingtonpost.com/opinions/2019/04/09/more-studies-showing-racial-disparities-criminal-justice-system/.

Dated: October 15, 2020

Respectfully Submitted,

/s Kendra K. Albert

Kendra K. Albert
Admitted pro hac vice
Cyberlaw Clinic
Harvard Law School
1585 Massachusetts Ave.
Cambridge, MA 02138

William Singer, Esq.
Attorney ID No. 272741971
Singer & Fedun, LLC
2230 Route 206
P.O. Box 134
Belle Mead, NJ 08502