Case No. F071640

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA
FIFTH APPELLATE DISTRICT

The People of the State of California,

Plaintiff and Appellee,

v.

Billy Ray Johnson,

Defendant and Appellant.

On Appeal from Kern County Superior Court,
Case No. BF151825A
The Honorable Gary T. Friedman, Judge

Brief of *Amici Curiae* American Civil Liberties Union and American Civil Liberties Union of Southern California In Support of Defendant–Appellant Seeking Reversal

---

Brett Max Kaufman
Brandon Buskey
Rachel Goodman
Vera Eidelman
Andrea Woods
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, New York 10004
T: 212.549.2500
bkaufman@aclu.org

Peter Bibring (SBN 223981)
American Civil Liberties Union Foundation of Southern California, Inc.
1313 W 8th Street, Suite 200
Los Angeles, CA 90017
T: 213.977.9500
pbibring@aclusocal.org

Attorneys for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutional Provisions

Other Authorities

INTEREST OF AMICI CURIAE[1]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than one million members dedicated to defending the civil liberties guaranteed by the Constitution. The ACLU of Southern California is a regional affiliate of the ACLU which serves Kern County and seven other Southern California counties. Transparency concerning algorithms used in criminal prosecutions is important to the work of a number of projects and programs at the ACLU, including the Racial Justice Program, the Speech, Privacy, and Technology Project, and the Criminal Law Reform Project. The ACLU and the ACLU of Southern California have appeared in numerous cases, both as direct counsel and as *amici*, before courts in California and throughout the nation in cases involving the meaning and scope of the rights of criminal defendants and the legal limitations on the use of technology by police and prosecutors.

[1] Pursuant to California Rule of Court 8.360(f) and 8.200(c), counsel for *amici curiae* have submitted a motion for leave to file this brief. In addition, counsel for *amici curiae* certify that no party or counsel for a party authored this brief in whole or in part, and no person other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission.

1. INTRODUCTION AND SUMMARY OF ARGUMENT

This case is about errors, both human and constitutional. It is about the fallibility of a technology—an algorithmic DNA-matching technique called TrueAllele—designed by humans and therefore subject to human mistakes, biases, assumptions, and choices. And it is about the failure of the court below to recognize and enforce the constitutional guarantees of confrontation, due process, and fairness to protect the civil rights of an individual on trial.

TrueAllele is aimed at solving a complex problem—evaluating the likelihood that an individual's DNA is present in a sample comprised of scraps of multiple individuals' genetic material. To do what a traditional DNA test cannot do, TrueAllele relies on an intricate algorithm designed by scientists and computer scientists to produce a simple score, called a "likelihood ratio." But the supposed objectivity of the likelihood ratio is belied by the many choices, cognitive biases, and plain-old mistakes that TrueAllele's programmers almost certainly embedded within the 170,000 lines of computer "source code" that drive the program. Those choices and errors, both known and not, can cause—and in documented cases, have caused—TrueAllele to produce wildly different results, even based off the same genetic samples. And the choices do not stop with the code itself, as the company also chooses how to report its results, including to the court below.

Given this, and the centrality of the TrueAllele test results to the State's case against Mr. Johnson, the Sixth and Fourteenth Amendments required that Mr. Johnson be given access to the TrueAllele source code. The Sixth Amendment guarantees a criminal defendant the right to meaningfully confront the witnesses used against him. And the same amendment, in

tandem with the Fourteenth, guarantees him a fundamentally fair trial, including adversarial testing of the State's evidence. Access to the TrueAllele source code, which Mr. Johnson sought and the trial court denied him, would have permitted his experts to inspect the code to uncover its potential flaws and biases, and to meaningfully confront the human choices behind the algorithm. Such adversarial process is necessary to properly inform the jury of what weight to assign to the TrueAllele results. By denying him access to the source code, the trial court violated Mr. Johnson's constitutional rights.

Beyond violating Mr. Johnson's rights, the trial court's denial of access to the source code implicated the rights of the public as well. Though not at issue in this appeal, the First Amendment right of access guarantees public oversight of criminal trials to ensure that the State exercises its prosecutorial power fairly and with integrity, and that the public trusts the criminal justice system. The right of access plainly attaches to algorithmic source code that plays a critical role in establishing a defendant's guilt at trial. The trial court's violation of Mr. Johnson's rights, which kept the source code from becoming part of the record, meant that the public could not exercise its constitutionally guaranteed oversight function in this case.

For these reasons and those given below, this Court should reverse the court below and remand to the district court to remedy the violations of Mr. Johnson's constitutional rights.

2. BACKGROUND

TrueAllele, the technology at issue here, purports to identify the perpetrator of a crime from a tiny, degraded DNA sample swimming in a mixture of multiple individuals' DNA. The problem TrueAllele seeks to solve is difficult: while traditional DNA analysis only looks for a match to

a single person's known DNA profile, TrueAllele must first sketch that profile—based on assumptions about the sample, including things like how many individuals contributed to the mixture, how much of each person's DNA is present, and how old or degraded the DNA is—before looking for a match. *See* Andrea Roth, *Machine Testimony*, 126 Yale L.J. 1972, 2018–19 (2017). Essentially, traditional DNA analysis is like looking at a photograph, while TrueAllele's analysis is like relying on an investigator's composite sketch.

To accomplish this feat, TrueAllele implements an "algorithm" (using "source code") to produce a "likelihood ratio." Each of these quoted terms deserves unpacking.

At the most elementary level, an algorithm is a "computational procedure"—or series of steps—that transforms inputs into an output. *See* Thomas Cormen et al., *Introduction to Algorithms* 1 (1st ed. 1994). In essence, it is like a manual or a recipe: a set of instructions for how to build something from raw materials.

In TrueAllele's case, the output is a single number called a "likelihood ratio." The likelihood ratio is computed by dividing (1) the estimated probability that the contributor of the DNA in the tested sample has the defendant's DNA profile, by (2) the probability that a random person of a particular race or ethnicity has the defendant's DNA profile. *See* William C. Thompson et al., *Forensic DNA Statistics: Still Controversial in Some Cases*, Legal Studies Research Paper Series No. 2013-122, 23 n.17 (Dec. 2012), *available at* http://ssrn.com/abstract=2214459. In other words, the likelihood ratio sets forth "how much more . . . a suspect . . . match[es] the evidence than a random person" of a particular reference population. 23RT 4115–4116, 4118, 24RT 4167–4168.

Unlike its output, TrueAllele's inputs are not fully known—and this is one of the significant problems at the crux of this case. Based on the record, two known inputs include assumptions about the number of contributors to a particular DNA sample, 24RT 4244, and the race or ethnicity of the comparison population, 24RT 4167–4168. But the inputs may also include assumptions about the quantity of DNA from each contributor, the degree to which the DNA is degraded, and the probability that certain alleles[2] may not be picked up. Other inputs might be inaccurately amplified because of the low quality of the DNA sample.

The algorithm at issue here is the series of steps that TrueAllele uses to turn these and other inputs into the likelihood ratio. Also at issue is TrueAllele's source code. "Source code" refers to the human-written instructions that tell a computer how to execute the algorithm. It is the implementation of the algorithm.

3. ARGUMENT

3(A) Algorithms are human constructs that include numerous sources for bias and mistake.

Algorithms are not neutral, infallible truth tellers: rather, they are tools designed, built, and employed by humans. Accordingly, they are vulnerable to human bias and mistake—and should therefore be subject to careful adversarial and judicial scrutiny—at each stage.

At the design stage, people make foundational assumptions that undergird the algorithmic model. For probabilistic DNA analysis, these assumptions include the "thresholds for what to count as a true genetic

---

[2] An "allele" is a genetic marker. At each relevant location on his/her DNA sequence, and individual has two "alleles," one inherited from each parent. *See* Thompson et al. at 13.

marker versus 'noise,'" "the probability of unusual events—such as small amounts of contamination during testing—that directly affect interpretation," and "the appropriate reference population for generating estimates of the rarity of genetic markers." Roth at 1996–97. In this way, algorithmic analysis is like more traditional DNA testing: using either method, it is a human who decides whether something identified in the DNA sample is "stutter" (i.e., random noise that can be ignored) or an actual allele (i.e., a characteristic that the suspect must match). That assumption has proven dispositive for whether a defendant is found to be a match. *Roberts v. United States*, 916 A.2d 922, 933–34 (D.C. 2007); *see also* Roth at 1996. In other words, humans decide at the outset of designing an algorithm what data to ignore and what data matters.

At the building stage, people operationalize the algorithm—assumptions and all—through source code. Such code is built from numbers, letters, symbols, and punctuation marks, and it can be materially altered by errors or "bugs" as simple as a misplaced ampersand. *See* Christian Chessman, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 Cal. L. Rev. 179, 187 (2017); Roth at 1994 (quoting Sergey Bratus et al., *Software on the Witness Stand: What Should It Take for Us to Trust It?*, *in* Trust and Trustworthy Computing 396, 397 (Alessandro Acquisti et al., eds., 2010)). The risk of bugs only increases with the complexity of the code and the difficulty of the problem it is attempting to solve. Roth at 2024. TrueAllele's code is likely to be affected by both issues. As noted above, TrueAllele's selling point is the difficulty of the problem it attacks, and its code runs more than 170,000 lines. Roth at 2035.

At the employment stage, people make choices about input parameters

that can make the difference between a conclusive and inconclusive match. Based on the promotional video available on its website, TrueAllele allows its analysts to set the number of contributors to a DNA sample, as well as an undefined variable called a "coancestry coefficient," among other variables. *See* TrueAllele Overview Video at 2:30, *available at* https://www.cybgen.com/products/casework.shtml. Mark Perlin, the creator of TrueAllele, acknowledges that some probabilistic DNA algorithms "give different answers based on how an analyst sets their input parameters." Letter from Mark W. Perlin, Chief Sci. and Exec. Officer, Cybergenetics, to Jerry D. Varnell, U.S. Dep't of Justice, Procurement Section, at 3 (Apr. 1, 2015), *available at* https://www.cybgen.com/information/newsroom/2015/may/Letter_to_FBI.pdf.

Finally, at the output stage, people must interpret the algorithm's result and translate it into terms that others can understand. Crucially, people—and not a computer or other machine—decide which results are significant enough to communicate to the jury. In this case alone, the experts who used TrueAllele—Dr. Perlin and Garett Sugimoto, a criminalist at the Kern County Regional Lab who underwent a one-year training to operate TrueAllele and ran the program in-house for the government lab in this case, *see* Resp.'s Br. 31—disagreed on what likelihood ratio could be considered conclusive: Dr. Perlin's threshold of exclusion was 1,000, 23RT 4138; Mr. Sugimoto's was ten times that, 24RT 4276. And humans also decide which precise result to disclose to the jury. In a case in Northern Ireland, for example, TrueAllele generated four different likelihood ratios regarding a defendant—389 million, 1.9 billion, 6.03 billion, and 17.8 billion; Dr. Perlin chose to report the 6.03 billion statistic. *See* Thompson et al. at 20.

At each of these stages, people will almost certainly make mistakes.

For example, with regard to the coding stage, one study found that even highly experienced programmers make a mistake in "almost 1 % of all expressions contained in [their] source code." Chessman at 186–87. Assuming that one expression appears per one line of code, that error rate would translate to 1,700 mistakes in TrueAllele. If even only one percent of such errors is material, that would mean that the TrueAllele program has seventeen significant errors—not to mention any errors in other programs to which it connects or relies upon to run, including MATLAB, *see* 4CT 934.

Beyond random mistakes, people hold cognitive biases that can materially affect the variables they include in an algorithm, as well as how they interpret the results—including whether a DNA sample results in a match. *See* Itiel E. Dror & Greg Hampikian, *Subjectivity and Bias in Forensic DNA Mixture Interpretation*, 51 Sci. & Just. 204, 206–07 (2011) (finding that more DNA examiners determined that an individual matched a DNA mixture when they knew that he was a criminal defendant in a gang rape case than when they did not). And, when it comes to an issue as complex as probabilistic DNA typing embodied in 170,000 lines of code, people may simply have conceptual blind spots. The fact that TrueAllele combines two complex areas—forensic science and probabilistic programming—suggests that Cybergenetics employees, while expert in one, may make errors due to an incomplete grasp of the other. Chessman at 188.

Moreover, financial incentives may pervert the goals of companies that build such algorithms. These dynamics are particularly acute in the field of probabilistic DNA typing, where the prosecution, backed by the superior resources of the state, is the most likely customer. That customer is likely to be most satisfied with an algorithm that delivers a match, and is less likely

to question its results. Therefore, private companies may be incentivized to find a match, rather than the truth, in order to attract and retain these customers. *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 318 (2009) ("A forensic analyst responding to a request from a law enforcement official may feel pressure—or have an incentive—to alter the evidence in a manner favorable to the prosecution."). In TrueAllele's own words, its goal is to turn low-quantity or degraded DNA mixtures from many individuals into "a match statistic *strong enough for court*," see TrueAllele E-Brochure at 4, *available at* https://www.cybgen.com/products/casework/forensic_e-brochure.pdf (emphasis added).

Not surprisingly, given these potential sources for error, criminal justice algorithms often fail to meet the needs of a rigorous and fair judicial system. In this case, the prosecution tasked TrueAllele with identifying the perpetrator of a crime. Recent history has shown that similar probabilistic DNA typing algorithms have failed at precisely this job, with serious consequences. In just the last few years, researchers documented a coding error in a competing probabilistic DNA typing algorithm that had enormous consequences: it produced incorrect results in 60 criminal cases in Australia, altering likelihood ratios by a factor of 10 and forcing prosecutors to replace 24 expert statements in criminal cases. 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. In New York, after a trial court ordered one of TrueAllele's competitors to release its source code, an expert witness for the defense discovered that "the program dropped valuable data from its calculations, in

ways that users wouldn't necessarily be aware of, but that could unpredictably affect the likelihood assigned to the defendant's DNA being in the mixture." Lauren Kirchner, *Traces of Crime: How New York's DNA Techniques Became Tainted*, N.Y. Times, Sept. 4, 2017, http://nyti.ms/2vJwxze. In response, the prosecution withdrew the DNA evidence against the defendant. *Id*. Earlier this year, the New York State Commission on Forensic Science "shelved" two previously-approved probabilistic DNA algorithms for similar reasons. *Id.*

These experiences highlight not only the possibility of error, but also its significance in altering results. A wrong result is a serious problem—both for criminal defendants, whose lives are put into jeopardy by faulty coding, and for prosecutors, whose cases can be upended by their introduction of unreliable evidence.

Indeed, notwithstanding the fact that each probabilistic DNA algorithm claims to provide accurate results based on objective scientific principles, competing programs frequently reach different results for the same underlying data. For example, in one case, after prosecutors shopped around for the program that would generate the strongest match, the court denied the admissibility of any probabilistic DNA evidence because two programs, including TrueAllele, reached different results. See *New York v. Hillary*, No. 2015-15 (N.Y. Cnty. Court Aug. 26, 2016);[3] *see also Commonwealth v. Foley*, 38 A.3d 882, 887, 890 (Pa. Super. Ct. 2012) (noting that TrueAllele calculated a match statistic of 189 billion, compared

[3] *Available at* www.northcountrypublicradio.org/assets/files/08-26-16DecisionandOrder-DNAAnalysisAdmissibility.pdf.

to a competitor's estimate of 13,000—a more than 14-million–fold difference). Even in this case, Dr. Perlin and Mr. Sagimoto—who were using the same program to match the same DNA evidence to the same defendant—calculated wildly different results. *See* App.'s Br. 35–37 (summarizing results that differed by factors of up to 10.7).[4] Indeed, Dr. Perlin testified that he expected Kern Lab's results—again, generated by running the same data through the same program—to be "within two zeros," or a magnitude of 100, of his results. 24RT 4191–4193. Such a difference could shift a likelihood ratio of 100 to 10,000, pushing it over Dr. Perlin's stated significance threshold.

For the reasons described above, algorithms are fallible. While this may be a surprising concept to laypeople, computer scientists, their creators, have long been acutely aware of this fact. They caution that "the evidence produced by computer programs is no more inherently reliable or truthful than the evidence produced by human witnesses." Chessman at 185. Yet when these algorithms are introduced in the courtroom, legal experts and prosecutors suggest that they are infallible and that their results are foolproof, "overstat[ing] the probative value of their evidence, going far beyond what the relevant science can justify." President's Council of

---

[4] The likelihood ratios introduced into evidence in Mr. Johnson's case—ratios like 34,000; 1 million; 740 million; and 211 quintillion—inevitably sound impressive, but the magnitude is partially due to the simple fact that TrueAllele "considers more information when making calculations" than do conventional methods; while conventional methods "generally consider only whether an allele is present or absent in a sample[,] TrueAllele also considers the height of the underlying peak and the presence or absence of technical artifacts that often accompany actual alleles." Thompson et al. at 19. These larger numbers do not necessarily equate to greater accuracy or validity. *Id.* at 20.

Advisors on Science and Technology ("PCAST"), *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods* (Sept. 2016) at 29, *available at* https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf. And juries, when deprived of the source code or any countervailing testimony that could expose the algorithm's potential pitfalls, generally do not question the prosecution's results. "The potential prejudicial impact" of such evidence is therefore "unusually high." PCAST at 45 (describing finding that mock jurors heavily underestimated the error rates of qualified, experienced forensic scientists); *see also* Matthew Shaer, *The False Promise of DNA Testing*, Atlantic, June 2016, http://theatln.tc/2xs7XUL (describing finding that sexual-assault cases involving DNA evidence in Australia were twice as likely to reach trial and 33 times as likely to result in a guilty verdict; homicide cases were 14 times as likely to reach trial and 23 times as likely to end in a guilty verdict).

In other words, juries put too much trust in algorithms when a defendant, and the public more broadly, cannot subject the relevant source code to adversarial analysis. Source code reveals the programmers' intent, assumptions, biases, and mistakes in ways that no other form of the program can as easily reveal. Adversarial review of the source code would reveal the set of variables used and underlying assumptions made in the algorithm, as well as any errors or mistakes in the source code.

Like any other evidence, algorithms are neither inherently good nor inherently bad—they are merely tools to replace human analysis of data, with varying degrees of accuracy. That degree of accuracy must be explored in court if juries are to reach just results. The adversarial system exists to ensure that the potential for error is illuminated for the jury. In this

case, that process failed.

3(B) Reliance on a secret algorithm in a criminal trial violates the Confrontation Clause.

The trial court's refusal to allow the defense access to TrueAllele's source code violated Mr. Johnson's Sixth Amendment right to confront "the witnesses against him." U.S. Const. amend. VI. 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*, 557 U.S. at 313 (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). But that concern was not satisfied in this case.

Mr. Johnson's confrontation right hinges primarily on whether his lack of access to TrueAllele's source code unduly inhibited his ability to confront Dr. Perlin, TrueAllele's progenitor and the prosecution's main witness to introduce the software program's likelihood ratios against Mr. Johnson. Effectively confronting Dr. Perlin's testimony, in turn, necessarily required that the defense access and confront TrueAllele's source code. *See, e.g., People v. Hammon*, 15 Cal. 4th 1117, 1127 (1997) ("When a defendant proposes to impeach a critical prosecution witness with questions that call for privileged information, the trial court may be called upon, as in [*Davis v. Alaska*, 415 U.S. 308 (1974)], to balance the defendant's need for cross-examination and the state policies the privilege is intended to serve."). To be sure, the California Supreme Court held in *People v. Lopez* that

mechanical printouts of raw data are not statements, and that "a machine cannot be cross-examined." *People v. Lopez*, 55 Cal. 4th 569, 583 (2012). *Lopez* does not control this case, however. That case held that the results of a blood alcohol analysis performed by a gas chromatography machine were not testimonial under *Crawford v. Washington*, 541 U.S. 36 (2004). *Lopez*, 55 Cal. 4th at 584–85. It did not address the question presented here of whether a court violates a defendant's right to confront an expert by denying him access to the source code used to generate the data underlying an expert's testimony. With this distinction, *Lopez* actually supports the disclosure of source code. There, defense counsel had access to a printout of the calibrations of the gas chromatography machine taken on the same day as the relevant test—a close parallel to the source code sought by Mr. Johnson here. *See id.* at 582; *see also People v. Vangelder*, 58 Cal. 4th 1, 7 (2013).

Like most expert testimony, Dr. Perlin's testimony resulted from the "distributed cognition" among Dr. Perlin, TrueAllele's programmers, and the software itself. Itiel E. Dror & Jennifer L. Mnookin, *The Use of Technology in Human Expert Domains: Challenges and Risks Arising from the Use of Automated Fingerprint Identification Systems in Forensic Science*, 9 L. Probability & Risk 1, 2 (2010); *see also* Chessman at 220 ("When a forensic report is the output of a computer program, it is thus a joint statement—one composed of the interaction between the statements of the programmer and the input of the program user."). Just as Dr. Perlin did not gather the DNA samples at issue himself, he also did not manually calculate the likelihood ratio. *See United States v. Washington*, 498 F.3d 225, 230 (4th Cir. 2007) (noting that technicians who operated a gas chromatograph could not independently verify the results because they only

relied on the analysis performed by the machine). Indeed, the entire reason he developed TrueAllele was to replace and improve upon such manual calculations. Instead, Dr. Perlin and TrueAllele's programmers developed a set of assumptions about probabilistic genotyping and programmed those assumptions into TrueAllele. Even accepting that TrueAllele software cannot be a witness under current California law, that software, under Dr. Perlin's design and direction, performed the only probabilistic calculations of the DNA mixtures in this case. And its analysis produced the inculpatory estimates of the likelihood that Mr. Johnson was a contributor to the collected DNA samples.

In this light, True Allele's source code is a critical component of contesting Dr. Perlin's testimony. Confronting experts like Dr. Perlin may reveal some bias or mistakes in their assumptions in formulating an algorithm or performing analysis of its results, but examining the source code is the only way to uncover the software's bias or mistakes. The software's intricate relationship with and dependence upon its human creators means that its operation is not immune from fraud, bias or incompetence. *See supra* § 3(A). To the contrary, coding errors—both deliberate and benign—are an inherent and significant part of programming. Roth at 1994; *see generally* Chessman at 183–99 (discussing various forms and frequencies of programming errors). As discussed above, consequential coding errors have been discovered in probabilistic genotyping programs once they were subject to outside scrutiny. *See supra* § 3(A). These are the very sorts of evils confrontation is meant to deter. *Melendez-Diaz*, 557 U.S. at 318–19.

It is no answer, as the trial court implicitly offered, that the source code is unnecessary because TrueAllele's general methodology has been

validated. *See* 4RT 494–97. Indeed, defense access to the sort of source code at issue here has already proven its worth. In 2016, in a New York case, a defense expert's access to the source code underlying a probabilistic DNA algorithm revealed that the code "could unpredictably affect the likelihood assigned to the defendant's DNA being in the mixture" and led the prosecution to withdraw the DNA evidence against the defendant. Kirchner, *supra*.

Moreover, the Supreme Court has repeatedly admonished that the right to confrontation is procedural, and cannot be discarded simply because the evidence appears reliable. *Crawford*, 541 U.S. at 62 ("Dispensing with confrontation because testimony is obviously reliable is akin to dispensing with jury trial because a defendant is obviously guilty."); *Melendez-Diaz*, 557 U.S. at 318; *see also Bullcoming*, 564 U.S. at 663 ("If a particular guarantee of the Sixth Amendment is violated, no substitute procedure can cure the violation, and no additional showing of prejudice is required to make the violation complete." (quotation marks omitted)).

Regardless, validation is far from a panacea for guaranteeing the accuracy of probabilistic genotyping in particular cases. The validation studies themselves are often conducted under conditions far more ideal than the actual circumstances in the field where they are typically deployed, and likelihood ratios are by their very nature more difficult to falsify, since their predictions can rarely be compared to a known baseline. Roth at 1982. Thus, a validated program's likelihood ratio still "might be off by orders of magnitude because of a host of human or machine errors." *Id.* This phenomenon introduces the risk that the results of a validated program may still be highly misleading. Examining whether the source code is operating as designed is therefore critical to determining the likelihood ratio's true

accuracy.

The trial court also erroneously accepted the prosecution's and Dr. Perlin's representations about why disclosure of the source code was unnecessary. First, their suggestion that disclosure was unnecessary because the code was "too complicated" for the defense's expert to decipher is exactly backward, and should never justify denying a defendant access to material witnesses. The code's complexity can only increase the need for adversarial scrutiny. As discussed above, complex code is more likely to contain errors, yet jurors are also more likely to accept its results as gospel.

Second, the prosecution's argument that there were sufficient other ways to evaluate the program, such as contacting Cybergenetics, the company that makes TrueAllele, to ask questions about the program through an "Internet Skype-like meeting," is entirely unavailing. *See* 4RT 495. As an initial matter, such alternatives are likely far less effective than adversarial testing as a means to challenge TrueAllele's likelihood ratio. But even if the Internet hotline were superior, the existence of an alternative way to challenge TrueAllele's results does not change the fact that "the Constitution guarantees one way: confrontation." *Melendez-Diaz*, 557 U.S. at 318.

Here, meaningful confrontation required defense access to the source code, especially given Dr. Perlin's admission that there were potential errors in the code, 23RT 4064: 18–20, a prospect made all the more certain by the program's numerous alternations and updates over time. *See* 4CT 947 (noting that TrueAllele "underwent many rounds of testing and model refinement over 10 years"); *see also* Chessman at 189 ("As the number of programmers and the age of software increases, the number of errors,

mistakes, and broken segments of code increases."). These errors could explain the fact that the software produced different results when separately run by Dr. Perlin and Mr. Sugimoto at the Kern County lab, or call into question the accuracy of both analyses.

Ignoring the relevant precedent, the trial court effectively allowed Dr. Perlin to set the parameters of his own cross-examination: Dr. Perlin alone determined that TrueAllele's source code was too complicated for outside scrutiny, and he alone dictated the means by which the defense might attempt to undermine his life's work. Predicting the results of such a one-sided confrontation does not require an algorithm. The trial court's unreasonable prohibition on defense counsel's ability to probe for inevitable areas of bias and error hidden within the source code constitutes a fundamental violation of the confrontation right. *See Delaware v. Van Arsdall*, 475 U.S. 673, 680 (1986) ("[A] criminal defendant states a violation of the Confrontation Clause by showing that he was prohibited from engaging in otherwise appropriate cross-examination designed to show a prototypical form of bias on the part of the witness.").

At its root, this case reveals the strong parallels between black-box technologies like TrueAllele and the *ex parte* examinations that motivated the founders to adopt the Confrontation Clause in the first place. Performed at the behest of the state, intentionally cloaked in secrecy, and unduly impressive to the unwitting juror, both render the defendant powerless to test the credibility of the source and undermine the state's case against him. *See generally Crawford*, 541 U.S. at 43–50 (describing history and development of confrontation right). Allowing the defense access to source code is the only reliable means of ensuring that the state cannot place forensic evidence beyond the reach of the Confrontation Clause, simply by

automating tasks previously performed by humans. Otherwise, regardless of whether courts consider machines witnesses or their products hearsay, our justice system risks "accept[ing] the product of a computer as the equivalent of Holy Writ." *Perma Research & Dev. v. Singer Co*., 542 F.2d 111, 121 (2nd Cir. 1976) (Van Graafeiland, J., dissenting).

3(C) Reliance on a secret algorithm in a criminal trial violates the defendant's rights to due process and to a fair trial.

The Fourteenth Amendment right to due process and the Sixth Amendment right to a fair trial work in tandem to guarantee criminal defendants a fundamentally fair process. "Whether rooted directly in the Due Process Clause of the Fourteenth Amendment or in the Compulsory Process or Confrontation Clauses of the Sixth Amendment, the Constitution guarantees criminal defendants a meaningful opportunity to present a complete defense." *Holmes v. South Carolina*, 547 U.S. 319, 319 (2006) (quoting *Crane v. Kentucky*, 476 U.S. 683, 690 (1986)) (quotation marks omitted). Criminal due process is, "in essence, the right to a fair opportunity to defend against the State's accusations." *Chambers v. Mississippi*, 410 U.S. 284, 294 (1973). Broadly speaking, "a fair trial is one in which evidence subject to adversarial testing is presented to an impartial tribunal for resolution of issues defined in advance of the proceeding." *Strickland v. Washington*, 466 U.S. 668, 685 (1984). The ruling below prevented Mr. Johnson from subjecting the TrueAllele evidence to adversarial testing, thus depriving him of the fair process that the Constitution requires.

Several strands of the due process doctrine are relevant here. First, with respect to evidence withheld from a defendant, due process asks "whether in its absence [the defendant] received a fair trial, understood as a trial resulting in a verdict worthy of confidence," *Kyles v. Whitley*, 514 U.S. 419,

434 (1995). Due process is concerned with all evidence "material either to guilt or to punishment," *Brady v. Maryland*, 373 U.S. 83, 87 (1963), and the assertion of an evidentiary privilege does not end the due process inquiry, *Pennsylvania v. Ritchie*, 480 U.S. 39, 57 (1987). Indeed, the Supreme Court has held that, to preserve the "fundamental fairness of trials," material information covered by an evidentiary privilege should nonetheless have been provided to a criminal defendant, even where it consisted of extremely sensitive information in a state agency's child abuse investigation file. *Id*. at 56-57. *See also Chambers*, 410 U.S. at 302 (cautioning that "[m]echanistic[]" application of hearsay rule to exclude evidence "critical" to a criminal defendant's case can "defeat the ends of justice" and violate due process); *Green v. Georgia*, 442 U.S. 95, 97 (1979). Second, and relatedly, due process requires rejection of asymmetrical evidentiary rules, that is, those that place the prosecution's evidence in a more favorable position than the defendant's. *See Holmes*, 547 U.S. at 331. Finally, due process protects the right to cross-examine witnesses—including adversarial testing of the source code upon which they rely—in part because the jury must be empowered to "judge for itself whether [ ] testimony [is] worthy of belief." *Chambers*, 410 U.S. at 295.

The Sixth Amendment further guarantees a defendant the right "to have compulsory process for obtaining witnesses in his favor." U.S. Const. amend. VI. The Supreme Court has elaborated: "The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts. . . . To ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the production of evidence needed either by the prosecution or by the defense." *United States v. Nixon*, 418 U.S. 683, 709 (1974); *see also Taylor*

v. Illinois, 484 U.S. 400, 409 (1988). At a minimum, compulsory process means that criminal defendants have "the right to put before a jury evidence that might influence the determination of guilt." *Ritchie*, 480 U.S. at 56; *see supra* § 3(B).

These constitutional principles mandate disclosure of the source code behind the probabilistic DNA analysis relied upon by the prosecution. *See United States v. Michaud*, Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing, 3:15-cr-05351RJB (W.D. Wash. May 18, 2016), ECF No. 205 (holding that source code underlying technique used to identify defendant was material and defendant therefore has a due process right to access it); *see also id.*, Motions Hearing and Court's Oral Ruling at 18–22 (May 25, 2016), ECF No. 212.

In the civil context, courts have held that government reliance on secret, proprietary algorithms violates due process. *See K.W. v. Armstrong,* 180 F. Supp. 3d 703, 718 (D. Idaho 2016) (holding that proprietary tool used to allocate Medicaid benefits "arbitrarily deprives participants of their property rights and hence violates due process"); *T. v. Bowling*, No. 2:15-CV-09655, 2016 WL 4870284, at *10 (S.D.W. Va. Sept. 13, 2016) (finding that proprietary algorithm used by government to set Medicaid benefits "present[s] a serious risk of resulting in erroneous determinations and deprivations"). The constitutional stakes—which are even higher in the criminal context—require the same result here.

Evidence based on algorithmic source code was at the very center of the prosecution's case against Mr. Johnson, and was therefore material and relevant to the question of his guilt. *See State v. Schwartz*, 447 N.W.2d 422, 427 (Minn. 1989) (holding that "fair trial and due process rights are implicated when data relied upon by a laboratory in performing [DNA]

tests are not available to the opposing party for review and cross examination"); *Ex parte Perry*, 586 So. 2d 242, 255 (Ala. 1991) (requiring disclosure of full details of DNA analysis methodology and holding "defendant's fair trial and due process rights . . . clearly require that the prosecution allow the defendant access to the DNA evidence"). Mr. Johnson's conviction, obtained in part by denying him the full opportunity to confront, analyze, and interrogate such crucial evidence, violates his constitutional right to a fundamentally fair criminal proceeding.

3(D) <u>In addition to violating Mr. Johnson's rights, the complete lack of transparency as to an algorithm that is material to a criminal trial vitiates the public's First Amendment right of access.</u>

In this case, the trial court denied Mr. Johnson's numerous attempts to obtain, examine, and introduce the algorithmic source code into the record. As explained above, those denials violated Mr. Johnson's Sixth and Fourteenth Amendment rights. But the harm did not end with Mr. Johnson. The trial court's denials also injured the public—by short-circuiting its longstanding First Amendment right of access to criminal proceedings. While that right is not at direct issue in this appeal, its transparency demands provide a different and useful lens for scrutiny of the trial court's decisions below, and offer important context for this Court's consideration of the other constitutional issues in play.

Because of the trial court's error in denying Mr. Johnson access to the source code underlying TrueAllele, that source code is not part of the record below. While that error means that no member of the public intervened below to assert the public's First Amendment right of access, the right would unquestionably have attached to the algorithmic source code (or any agreed-upon protective order) had the trial court correctly ordered disclosure to Mr. Johnson. This Court can vindicate the public's First

Amendment right by correcting the trial court's errors with respect to Mr. Johnson's constitutional rights, and thereby enabling representatives of the public to assert their First Amendment right of access on remand.

The First Amendment right of access attaches to algorithms that are material to a criminal proceeding. The First Amendment exists to enable and protect "uninhibited, robust, and wideopen" debate on public issues, *Watts v. U.S.*, 394 U.S. 705, 708 (1969), and "for the bringing about of political and social changes desired by the people," *Roth v. United States*, 354 U.S. 476, 484 (1957). Neither is possible without public access to judicial proceedings and documents—a principle the Supreme Court recognized almost forty years ago when it held that "the right to attend criminal trials is implicit in the guarantees of the First Amendment," which includes the right to "'receive information and ideas.'" *Richmond Newspapers Inc. v. Virginia*, 448 U.S. 555, 576 (1980) (quoting *Kleindienst v. Mandel*, 408 U.S. 753, 762 (1972)).

Critically, the right of access exists in criminal trials to allow the public to observe and evaluate the workings of the criminal justice system—and to make changes in order to eliminate injustice. See *id*. at 572. As the Supreme Court has explained, "the criminal justice system exists in a larger context of a government ultimately of the people, who wish to be informed about happenings in the criminal justice system, and, if sufficiently informed about those happenings, might wish to make changes to the system." *Gentile v. State Bar of Nev*., 501 U.S. 1030, 1070 (1991). The need for public oversight of government process is strongest in criminal trials, where the state wields its greatest power to affect individual liberty. Public access "enhances the quality and safeguards the integrity" of the judicial process, "heighten[s] public respect" for that process, and "permits

the public to participate in and serve as a check upon the judicial process." *Globe Newspaper Co. v. Superior Court for Norfolk Cnty.*, 457 U.S. 596, 606 (1982).[5]

Under the Supreme Court's prevailing "experience and logic" test, the public's First Amendment right of access attaches to judicial proceedings and records where (a) the type of judicial process or record sought has historically been available to the public, and (b) public access plays a "significant positive role" in the functioning of the process itself. *Press-Enter. Co. v. Superior Court* ("*Press-Enter. II*"), 478 U.S. 1, 9, 11 (1986); *see Globe Newspaper Co.*, 457 U.S. at 605–07. Once the right of access attaches, proceedings and records are presumptively open to the public, but they may be closed where there are "specific, on the record findings" that "closure is essential to preserve higher values and is narrowly tailored to serve that interest." *Press-Enter. II*, 478 U.S. at 13–14 (quoting *Press-Enter. Co. v. Superior Court* ("*Press-Enter. I*"), 464 U.S. 501, 510 (1984)); *see also Globe Newspaper*, 457 U.S. at 606–07; *N.Y. Civil Liberties Union v. N.Y.C. Transit Auth.*, 684 F.3d 286, 296 (2d Cir. 2012) (requiring a

---

[5] The importance of public access to criminal trials is also embedded in the common law, *see, e.g.*, *Lugosch v. Pyramid Co. of Onondaga*, 435 F.3d 110, 119 (2d Cir. 2006), as well as the Sixth Amendment, which guarantees a criminal defendant the right to a public trial, *see, e.g.*, *In re Oliver*, 333 U.S. 257, 268–69 (1948). Indeed, the Supreme Court has suggested that the demands of the Sixth's Amendment's public-trial right—grounded in the defendant's right to a fair trial—may go even further than the First Amendment right in certain cases. *See Presley v. Georgia*, 558 U.S. 209, 213 (2010); *Waller v. Georgia*, 467 U.S. 39, 46 (1984) ("There can be little doubt that the explicit Sixth Amendment right of the accused is no less protective of a public trial than the implicit First Amendment right of the press and public.").

substantial probability of harm to a compelling government interest, and no alternative that can effectively protect against that harm to overcome presumption of access).

Algorithms used to produce evidence introduced to prove the guilt of a criminal defendant fit well within the broad reach of the First Amendment right of access.

There is little question that the right of access attaches to the criminal trial at issue here. Indeed, the Supreme Court first grounded the First Amendment "presumption of openness [that] inheres in the very nature of a criminal trial under our system of justice" in the "unbroken, uncontradicted history" of such access, "supported by reasons as valid today as in centuries past." *Richmond Newspapers*, 448 U.S. at 573; *see also Press-Enter. I*, 464 U.S. at 505–07 (discussing history of openness in criminal trials); *Cal. First Amendment Coal. v. Woodford*, 299 F.3d 868, 874 (9th Cir. 2002); *KNSD Channels 7/39 v. Superior Court*, 63 Cal. App. 4th 1200, 1203–04 (1998).

And once the right attaches to a proceeding, the presumption of access applies broadly to all materials essential to that proceeding—including the algorithmic source code in this case. *See Woodford*, 299 F.3d at 874 (ruling that meaningful access to a proceeding required expansion of access to behind-the-scenes proceedings); *Doe v. Pub. Citizen*, 749 F.3d 246, 267 (4th Cir. 2014) ("[T]he First Amendment right of access extends to materials submitted in conjunction with judicial proceedings that themselves would trigger the right to access."); *see also Application of WFMJ Broad. Co.*, 566 F. Supp. 1036, 1040 (N.D. Ohio 1983) ("Just as the Supreme Court's reluctance to embrace a 'narrow, literal conception of the [First] Amendment's terms', *Globe Newspaper*[, 457 U.S. at 604], gave rise to a constitutional right of access to criminal trials, the same view could

make a constitutional right to evidence an appropriate adjunct to insure that such proceedings are 'open.'"). Here, as in *Woodford*, the government cannot artificially cabin the record of a proceeding in order to deny public access to all but the ultimate result.[6]

Moreover, openness in the context of algorithms used to produce evidence of guilt would have immense public value. There is a long history of junk science being used under the guise of technological advance in criminal cases in this country—and of public access to and analysis of such evidence establishing its invalidity. "Since a series of high-profile legal challenges in the 1990s increased scrutiny of forensic evidence, a range of long-standing crime-lab methods have been deflated or outright debunked," including bite-mark analysis, ballistics testing, fingerprinting, and microscopic-hair-comparison. Shaer, *supra*.

Indeed, the Supreme Court has relied on public scrutiny of forensic processes to inform its interpretation of constitutional protections. *See Melendez-Diaz*, 557 U.S. at 319 ("Serious deficiencies have been found in the forensic evidence used in criminal trials."). And state supreme courts—as well as federal appellate courts—have equally looked to work done by the public, rather than either party or its experts in a criminal case, to determine that evidence based on specific technologies was not sufficiently

---

[6] Courts have held that the public's First Amendment right of access attaches to materials in the record of a criminal case for this reason. *See, e.g., In re Globe Newspaper*, 729 F.2d 47 (1st Cir. 1984) (right of access attaches to memorandum, affidavits and transcripts in criminal case); *In re N.Y. Times Co.*, 828 F.2d 110 (2d Cir. 1987) (same for suppression motions and exhibits); *In re Wash. Post Co.*, 807 F.2d 383 (4th Cir. 1986) (same for plea agreements); *United States v. Peters*, 754 F.2d 753, 763 (7th Cir. 1985) (same for trial exhibits).

reliable to be admissible into evidence. *See, e.g.*, *Han Tak Lee v. Houtzdale SCI*, 798 F.3d 159, 166–67 (3d Cir. 2015) (discussing changes in "fire science"); *People v. Leone*, 25 N.Y.2d 511 (1969) (relying on commentary of outside experts to hold that evidence derived from polygraph tests was not fit for admission); *see People v. Davis*, 343 Mich. 348, 371 (1965) (same).

Public scrutiny has had substantial benefits outside of the courtroom as well, leading to important improvements in investigative fields. For example, after a *New Yorker* article exposed a flawed case based on fire-science evidence, Texas not only "reconsider[ed] old cases that had been improperly handled by the original investigators," but also "reinvented itself as a leader in arson science and investigation" by "revamp[ing] the state's training and investigative standards." Jeremy Stahl, *The Trials of Ed Graf*, Slate, Aug. 15, 2015, http://slate.me/2wdpTUA.

And all of this is true of DNA evidence, as well. In the DNA field, "[b]oth the initial recognition of serious problems and the subsequent development of reliable procedures were aided by the existence of a robust community of molecular biologists" and by "judges who recognized that this powerful forensic method should only be admitted as courtroom evidence once its reliability was properly established." PCAST at 26.

Given the positive effect of public access on the use of arguably simpler technologies in criminal case, public access would plainly enhance the reliability of algorithmic evidence. This is particularly true of technologies that, like the likelihood ratio introduced in this case, have been minimally tested in the field. Most existing validation studies of probabilistic DNA typing have been "conducted under idealized conditions unrepresentative of the challenges of real casework." Roth at 2033; *see also* Christopher D.

Steele and David J. Balding, *Statistical Evaluation of Forensic DNA Profile Evidence*, 1 Ann. Rev. Stat. & App. 361, 380 (2014). While TrueAllele "appear[s] to be reliable for three-person mixtures in which the minor contributor constitutes at least 20 percent of the intact DNA in the mixture and in which the DNA amount exceeds the minimum level required for the method," "there is relatively little published evidence" for "more complex mixtures"—that is, precisely the sort of mixtures for which these programs are used in actual cases. PCAST at 80–81. Moreover, "most of the studies evaluating software packages have been undertaken by the software developers themselves." PCAST at 80. Public access to algorithmic evidence would improve the role such evidence plays in criminal trials—including by preventing the jury from giving it undue weight, where necessary—and increase the public's confidence in the justice system more generally.[7]

Indeed, public review of the sort of source code at issue here has already proven its worth. In a 2008 case, public review of Alcotest 7110 source code led the New Jersey Supreme Court to require modifications to prevent misleadingly high accuracy readings. *State v. Chun*, 943 A.2d 114, 120–21

[7] The government may argue that requiring the release of source code will have a negative effect on the proceedings because it will create additional disputes, but that argument would be misplaced. The government has no interest in unfair proceedings, even if they take longer. Moreover, public vetting of algorithmic source code will surely experience efficiency gains as it becomes a more commonplace check on complex, experimental evidence. As the Supreme Court recently reaffirmed, "the Government's 'interest . . . in a criminal prosecution is not that it shall win a case, but that justice shall be done.'" *Turner v. United States*, 137 S. Ct. 1885, 1893 (2017) (quoting *Berger v. United States*, 295 U.S. 78, 88 (1935)).

(N.J. 2008). Allowing the public, including academics and other experts, to examine DNA typing evidence would markedly improve the reliability and fairness of such evidence in criminal trials. The other checks our judicial system relies upon, like recordation and appeal, "operate rather as cloaks than checks; as cloaks in reality, as checks only in appearance." *In re Oliver*, 333 U.S. at 271. "Without publicity, all other checks are insufficient." *Id.* (quotation marks omitted)).

Moreover, while some courts have (erroneously) applied a narrower test to determining whether the First Amendment right-of-access attaches—looking to the nature of a particular document rather than proceedings themselves, *see In re Bos. Herald*, 321 F.3d 174, 182–84 (1st Cir. 2003) (reviewing case law applying the First Amendment right of access to proceedings and documents)—the right would still attach to algorithmic source code used to produce evidence of guilt in a criminal case under this analysis. Under the test's "experience" prong, it is not only well established but fundamental that the materials essential to the government's case in chief enjoy a presumption of openness in the criminal justice system. *See, e.g.*, *Application of WFMJ Broad. Co.*, 566 F. Supp. at 1040 (tapes played to jury in open court); *United States v. Posner*, 594 F. Supp. 930, 934–35 (S.D. Fla. 1984) (tax returns admitted into evidence); *United States v. Scott*, 48 M.J. 663 (A. Ct. Crim. App. 1998) (materials entered into evidence at trial); *Valley Broad. Co. v. U.S. Dist. Court for Dist. of Nev.*, 798 F.2d 1289, 1292–93 (9th Cir. 1986) (transcripts of exhibits); *In re Times-World Co.*, 488 S.E.2d 677 (Va. 1997) (documents submitted into evidence). And the right also attaches to supporting materials that form a critical component of

the record, especially when they pertain to the "adjudicat[ion] of substantive rights," *Rushford v. New Yorker Mag.*, 846 F.2d 249, 252 (4th Cir. 1988).[8]

While courts have held that the "raw fruits" of discovery may not be subject to the right of access, *see, e.g.*, *id.*; *Seattle Times v. Rhinehart*, 467 U.S. 20 (1984), that conclusion is altered where the parties rely on or incorporate discovery materials into substantive litigation.[9] Indeed, in the civil context courts have held that under the First Amendment, reports relied upon by parties in the "adjudication stages" of litigation are presumptively

---

[8] Moreover, the "experience" prong "is not meant . . . to be construed so narrowly" as to exclude from First Amendment coverage proceedings or documents that are of "relatively recent vintage." *In re Bos. Herald*, 321 F.3d at 184. In such cases, courts look to analogous proceedings and documents of the same "type or kind." *Rivera–Puig v. Garcia–Rosario*, 983 F.2d 311, 323 (1st Cir.1992); *see El Vocero de P.R. v. Puerto Rico*, 508 U.S. 147, 150–51 (1993) (finding pretrial criminal hearings in Puerto Rico analogous to other pretrial hearings to which First Amendment right applies, despite distinctions noted by Puerto Rico Supreme Court); *Press–Enter. II*, 478 U.S. at 10–11 (evaluating California pre-trial hearings by looking to practices of other states and to other types of hearings, including probable cause hearing in Aaron Burr's 1807 trial for treason); *see also United States v. Chagra*, 701 F.2d 354, 363 (5th Cir. 1983) ("Because the first amendment must be interpreted in the context of current values and conditions, the lack of an historic tradition of open bail reduction hearings does not bar our recognizing a right of access to such hearings." (citations omitted)).

[9] It is plain from Mr. Johnson's arguments below and on appeal that the source code or some part of it would have been the subject of litigation on the record, even if initially under a protective order. 4 CT 902; 4 RT 430-491; 23 RT 4090-4111; App.'s Br. 55–65; *see Grove Fresh Distribs., Inc. v. Everfresh Juice Co.*, 24 F.3d 893, 898 (7th Cir. 1994) ("Although the media's right of access does not extend to information gathered through discovery that is not part of the public record, the press does have standing to challenge a protective order for abuse or impropriety.").

"available for public inspection unless exceptional circumstances require confidentiality." *In the Matter of Continental Ill. Sec. Litig.*, 732 F.2d 1302, 1314 (7th Cir.1984); *accord Joy v. North*, 692 F.2d 880, 893 (2d Cir. 1982); *see also Rushford*, 846 F.2d at 253 (documents filed in connection with summary judgment motion); *NBC Subsidiary (KNBC-TV), Inc. v. Superior Court*, 20 Cal. 4th 1178, 1211 n.28 (1999) (applying the same principle in a civil context).[10] Those principles apply with even greater force in the criminal context to evidence and its attendant documents, *see, e.g.*, *In re Wash. Post Co.*, 807 F.2d 383, 389–90 (4th Cir. 1986)—and would encompass the algorithmic source code that produced the evidentiary results that played a central role in the conviction of Mr. Johnson. *See Doe*, 749 F.3d at 267.

And apropos of the policy arguments discussed above, "logic" also dictates that the First Amendment right of access attaches in this context. Public access to the highly complex algorithmic source code that produced the evidence used to convict Mr. Johnson would—had the trial court's constitutional errors not excluded it from the record—have "enhance[d] the quality and safeguard[ed] the integrity of the factfinding process, with benefits to both the defendant and to society as a whole," *Globe Newspaper Co.*, 457 U.S. at 606; *see also, e.g.*, *Grove Fresh Distribs.*, 24 F.3d at 897 (citing *Richmond Newspapers*, 448 U.S. at 555); *Int'l Fed'n of Prof'l & Tech. Eng'rs, Local 21, AFL-CIO v. Superior Court*, 42 Cal. 4th 319, 333

[10] Even courts that have rejected the attachment of a First Amendment right of access in particular contexts have acknowledged that the right may well attach where "the material is important and the decision to which it is relevant amounts to an adjudication of an important substantive right." *Anderson v. Cryovac, Inc.*, 805 F.2d 1, 11 (1st Cir. 1986).

(2007).[11]

Public access to the complex foundation of the algorithmic evidence introduced to prove Mr. Johnson's guilt would have allowed for a thorough public vetting of a new technology, with all its salutary consequences. In particular, in the context of criminal cases in which defendants and their counsel have limited resources, public access to algorithmic evidence would bolster the purpose of the *Kelly-Frye* inquiry at trial to "ensure that any and all scientific testimony or evidence admitted is not only relevant, but reliable," *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 589 (1993), by providing the public with an opportunity to evaluate and test evidentiary material.[12]

---

[11] *See also Leucadia, Inc. v. Applied Extrusion Techs., Inc.*, 998 F.2d 157, 161 (3d Cir. 1993) ("As with other branches of government, the bright light cast upon the judicial process by public observation diminishes the possibilities for injustice, incompetence, perjury, and fraud. Furthermore, the very openness of the process should provide the public with a more complete understanding of the judicial system and a better perception of its fairness." (quoting *Rep. of Phil. v. Westinghouse Elec. Corp.*, 949 F.2d 653, 660 (3d Cir. 1991)); *United States v. Hubbard*, 650 F.2d 293, 315 n.79 (D.C. Cir. 1980) (Like the public trial guarantee of the Sixth Amendment, the First Amendment right of access serves to "safeguard against any attempt to employ our courts as instruments of persecution," to promote the search for truth, and to assure "confidence in . . . judicial remedies."); *Ibrahim v. Dep't of Homeland Sec.*, 62 F. Supp. 3d 909, 934–45 (N.D. Cal. 2014) ("Public oversight of courts and therefore public access to judicial operation is foundational to the functioning of government. Without such oversight, the government can become an instrument for injustice.").

[12] To be clear, a *Kelly-Frye* (or *Daubert*) hearing—which, in any case, was denied here, *see* 4RT 494—is plainly an insufficient substitute for scrutiny of algorithmic source code, as it goes only towards admissibility (a matter decided by the judge), rather than weight (a matter decided by the jury).

Of course, the fact that the First Amendment right of access would have *attached* to algorithmic source code properly entered into the record does not dictate that the source code itself would have been made public, in part or in its entirety. Because the right is a qualified one, the outcome (in this case or any other) would depend upon the strength of the government's interest in continued secrecy, as well any measures taken to narrowly tailor the denial of the source code to the public, including through a protective order. *See Press-Enter. II*, 478 U.S. at 13–14; *see also Globe Newspaper Co.*, 457 U.S. at 608 (explaining that even a compelling government interest "does not justify a *mandatory* closure rule, for it is clear that the circumstances of the particular case may affect the significance of the interest"); *United States v. Amodeo*, 71 F.3d 1044, 1049 (1995); *Grove Fresh Distribs.*, 24 F.3d at 898. And that process would require the government, and then the court, to make on-the-record findings concerning the reasons justifying full or partial secrecy. *See Press-Enter. II*, 478 U.S. at 13–14.

It is clear, however, that where a criminal case involves algorithmic source code that produced material evidence like that in Mr. Johnson's case, the strength of the public's right of access should favor some level of disclosure. Indeed, the Supreme Court has explained that the "circumstances" in which "the right to an open trial may give way . . . to other rights or interests . . . will be rare." *Waller*, 467 U.S. at 45. Such

---

See, e.g., *People v. Barney*, 8 Cal. App. 4th 798, 817 (1992). Any flaws or errors in source code would tend to undermine the value of state evidence based on it, and would permit the defendant to argue to the jury to disregard the experimental test results introduced into evidence.

sufficiently weighty rights and interests might include, for example, "the defendant's right to a fair trial or the government's interest in inhibiting disclosure of sensitive information." *Id.* But the government's interest in this case and those like it does not approach that class of gravity. To the contrary, the defendant's right to a fair trial dovetails—rather than conflicts—with the public's right of access. *See supra* § 3(C).

Here, the government's only interest in secrecy appears to be derivative of a private company's intellectual-property interest in purported trade-secrets information. This private interest, on its own, will likely fail strict scrutiny. *See DVD Copy Control Ass'n v. Bunner Inc.*, 31 Cal. 4th 864, 883 (2003) (explaining that the U.S. Supreme Court has "recognized that the First Amendment interests served by the disclosure of purely private information like trade secrets are not as significant as the interests served by the disclosure of information concerning a matter of public importance") (citing *Bartnicki v. Vopper*, 532 U.S. 514, 533 (2001); *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 759 (1985)); *see also Woodford*, 299 F.3d at 880 (explaining that narrow tailoring does not comport with "forc[ing the public] to rely on the same prison officials who are responsible for administering the execution to disclose and provide information about any difficulties with the procedure").

This makes it very likely that the public's oversight role would be realized in one form or another. Regardless, the complete denial of source code used on the public's behalf to convict a criminal defendant would surely be an "exaggerated response" to private-interest concerns. *Woodford*, 299 F.3d at 880. In the context of the First Amendment analysis, the compelling nature of private concerns like trade secrets will be highly suspect when balanced against the momentous and bedrock constitutional

rights held by a criminal defendant and the public.

4. CONCLUSION

For the foregoing reasons, this Court should reverse the court below and remand to the district court to remedy the violations of Mr. Johnson's constitutional rights.

Respectfully submitted,

Dated: September 13, 2017 */s/ Peter Bibring*

Brett Max Kaufman
Brandon Buskey
Rachel Goodman
Vera Eidelman
Andrea Woods
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, New York 10004
T: 212.549.2500
bkaufman@aclu.org

Peter Bibring (SBN 223981)
American Civil Liberties Union Foundation of Southern California, Inc.
1313 W 8th Street, Suite 200
Los Angeles, CA 90017
T: 213.977.9500
pbibring@aclusocal.org

Attorneys for Amici Curiae

CERTIFICATE OF COMPLIANCE

I certify that the text in the attached Brief contains 10,134 words—as calculated by Microsoft Word, including footnotes but not the caption, the table of contents, the table of authorities, signature blocks, or this certification—and that this document was prepared in a 13-point Times New Roman font. *See* Rule of Court 8.204(c)(1), (3).

Dated: September 13, 2017

By: __*/s/ Peter Bibring*___
Peter Bibring

PROOF OF SERVICE

STATE OF CALIFORNIA, COUNTY OF LOS ANGELES

I am employed in the County of Los Angeles, State of California. I am over the age of 18 and not a party to the within action. My business address is 1313 West Eighth Street, Los Angeles, California 90017. I am employed in the office of a member of the bar of this court at whose direction the service was made.

On September 13, 2017, I served the foregoing document:

Brief of Amici Curiae American Civil Liberties Union and American Civil Liberties Union of Southern California In Support of Defendant–Appellant Seeking Reversal

on the parties in this action by transmitting a true copy via this Court's TrueFiling system and by placing a true copy, enclosed in a sealed envelope, addressed as follows:

Party	Attorney/Address Served
Billy Ray Johnson, Jr. *Defendant and Appellant*	Laura Schaefer Attorney at Law 934 23rd St. San Diego, CA 92102 ls@boyce-schaefer.com
The People *Plaintiff and Respondent*	Office of the Attorney General P. O. Box 944255 Sacramento, CA 94244 sacawttruefiling@doj.ca.gov Caely E. Fallini Office of the Attorney General P.O. Box 944255 Sacramento, CA 94244 Caely.Fallini@doj.ca.gov

Central California Appellate Program	Central California Appellate Program 2150 River Plaza Dr., Ste. 300 Sacramento, CA 95833 eservice@capcentral.org
Kern County Superior Court Clerk	Clerk of the Court Hon. Gary T. Friedman 1415 Truxtun Ave Bakersfield, CA 93301
Kern County District Attorney	Lisa Green Kern County District Attorney 1215 Truxton Ave. Bakersfield, CA 93301
Innocence Project, Inc., The CA Innocence Project, The Northern CA Innocence, Loyola Law School *Amicus curiae for appellant*	Gerald Bill Hrycyszyn Wolf Greenfield & Sacks PC 600 Atlantic Ave Ste 2300 Boston, MA 2210 gerald.hrycyszyn@wolfgreenfield.com

I caused such envelope(s) fully prepaid with U.S. Postage to be placed in the United States Mail at Los Angeles, California. I am "readily familiar" with the firm's practice of collection and processing correspondence for mailing. Under that practice it would be deposited with the U.S. Postal Service on that same day with postage thereon fully prepaid at Los Angeles, California in the ordinary course of business.

I declare under penalty of perjury under the laws of the State of California and the United States of America that the above is true and correct.

Executed on September 13, 2017, at Los Angeles, California.

_____

Casey Kasher