NOT FOR PUBLICATION WITHOUT THE
APPROVAL OF THE APPELLATE DIVISION

SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-4207-19T4

STATE OF NEW JERSEY,

Plaintiff-Respondent,

v.

COREY PICKETT,

Defendant-Appellant.

APPROVED FOR PUBLICATION

February 3, 2021

APPELLATE DIVISION

Argued January 19, 2021 – Decided February 3, 2021

Before Judges Fasciale, Rothstadt and Susswein.

On appeal from an interlocutory order of the Superior Court of New Jersey, Law Division, Hudson County, Indictment No. 17-07-0470.

Tamar Y. Lerer, Assistant Deputy Public Defender, argued the cause for appellant (Joseph E. Krakora, Public Defender, attorney; Tamar Y. Lerer, of counsel and on the briefs).

Stephanie Davis Elson, Assistant Prosecutor, argued the cause for respondent (Esther Suarez, Hudson County Prosecutor, attorney; Stephanie Davis Elson, of counsel and on the briefs).

Amanda G. Schwartz, Deputy Attorney General, argued the cause for amicus curiae Attorney General of New Jersey (Gurbir S. Grewal, Attorney General,

attorney; Amanda G. Schwartz, of counsel and on the brief).

Karen Thompson argued the cause for amicus curiae American Civil Liberties Union of New Jersey and Electronic Frontier Foundation (American Civil Liberties Union of New Jersey, Kit Walsh (Electronic Frontier Foundation) of the California and Massachusetts bars, admitted pro hac vice, and Hannah Zhao (Electronic Frontier Foundation) of the New York bar, admitted pro hac vice, attorneys; Karen Thompson, Alexander Shalom, Jeanne LoCicero, Kit Walsh and Hannah Zhao, on the joint brief).

Christopher D. Adams argued the cause for amicus curiae The Association of Criminal Defense Lawyers of New Jersey (Greenbaum, Rowe, Smith & Davis LLP, attorneys; Christopher D. Adams, of counsel and on the brief; Abdus-Sami M. Jameel, on the brief).

Dana M. Delger (Innocence Project Inc.) of the New York bar, admitted pro hac vice, argued the cause for amicus curiae The Innocence Project (Dana M. Delger (Innocence Project Inc.) of the New York bar, admitted pro hac vice, Mazraani & Liguori, LLP, Michael A. Albert (Wolf, Greenfield & Sacks, P.C.) of the Massachusetts bar, admitted pro hac vice, and Anant K. Saraswat (Wolf, Greenfield & Sacks, P.C.) of the Massachusetts bar, admitted pro hac vice, attorneys; Dana M. Delger, Joseph M. Mazraani, Michael A. Albert and Anant K. Saraswat, on the brief).

Dino L. LaVerghetta (Sidley Austin LLP), of the District of Columbia and New York bars, admitted pro hac vice, argued the cause for amici curiae Drs. Mats Heimdahl and Jeanna Matthews (Coughlin Duffy LLP, Dino L. LaVerghetta, (Sidley Austin LLP) of the District of Columbia and Virginia bars, admitted pro hac vice, and Iain C. Armstrong (Sidley Austin LLP)

of the District of Columbia and Virginia bars, admitted pro hac vice, attorneys; Dino L. LaVerghetta, Iain C. Armstrong, Matthew Hopkins, and Mark K. Silver, on the brief).

J. David Pollock, attorney for amicus curiae The Legal Aid Society.

Singer & Fedun, LLC and Kendra K. Albert (Cyberlaw Clinic, Harvard Law School) of the Massachusetts bar, admitted pro hac vice, attorneys for amicus curiae Upturn, Inc. (William Singer and Kendra K. Albert, on the brief).

The opinion of the court was delivered by

FASCIALE, P.J.A.D.

In this case of first impression addressing the proliferation of forensic evidentiary technology in criminal prosecutions, we must determine whether defendant is entitled to trade secrets of a private company for the sole purpose of challenging at a Frye[1] hearing the reliability of the science underlying novel DNA analysis software and expert testimony. At the hearing, the State produced an expert who relied on his company's complex probabilistic genotyping software program to testify that defendant's DNA was present, thereby connecting defendant to a murder and other crimes. Before cross-examination of the expert, the judge denied defendant access to the trade secrets, which include the software's source code and related documentation.

[1] Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).

This is the first appeal in New Jersey addressing the science underlying the proffered testimony by the State's expert, who designed, utilized, and relied upon TrueAllele, the program at issue. TrueAllele is technology not yet used or tested in New Jersey; it is designed to address intricate interpretational challenges of testing low levels or complex mixtures of DNA. TrueAllele's computer software utilizes and implements an elaborate mathematical model to estimate the statistical probability that a particular individual's DNA is consistent with data from a given sample, as compared with genetic material from another, unrelated individual from the broader relevant population. For this reason, TrueAllele, and other probabilistic genotyping software, marks a profound shift in DNA forensics.

TrueAllele's software integrates multiple scientific disciplines. At issue here—in determining the reliability of TrueAllele—is whether defendant is entitled to the trade secrets to cross-examine the State's expert at the Frye hearing to challenge whether his testimony has gained general acceptance within the computer science community, which is one of the disciplines. The defense expert's access to the proprietary information is directly relevant to that question and would allow that expert to independently test whether the evidentiary software operates as intended. Without that opportunity, defendant is relegated to blindly accepting the company's assertions as to its reliability.

And importantly, the judge would be unable to reach an informed reliability determination at the Frye hearing as part of his gatekeeping function.

Hiding the source code is not the answer. The solution is producing it under a protective order. Doing so safeguards the company's intellectual property rights and defendant's constitutional liberty interest alike. Intellectual property law aims to prevent business competitors from stealing confidential commercial information in the marketplace; it was never meant to justify concealing relevant information from parties to a criminal prosecution in the context of a Frye hearing.

Requiring access to trade secrets in criminal cases is not new in New Jersey. In State v. Chun, 194 N.J. 54, 64, 66, 68-70 (2008), our Supreme Court ordered Draeger Safety Diagnostics Inc. (Draeger), the company that produces the Alcotest 7110 breathalyzer, to disclose its proprietary source code for independent review. Outside objective analysis revealed significant source code errors. Id. at 126-32.

In other jurisdictions, and directly on point here, courts have also made available under protective orders proprietary information of genotyping software, with noteworthy results. For example, as part of a Daubert[2] hearing,

[2] Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579 (1993). Under Daubert, trial judges perform a "preliminary assessment of whether the reasoning or

a federal judge unsealed the source code of Forensic Statistical Tool (FST), a probabilistic genotyping software that had been developed and used by the New York City Office of Chief Medical Examiner (OCME). In 2017, that review demonstrated the software—employed in thousands of criminal prosecutions—was unreliable, did not work as intended, and had to be eliminated. And in 2015, after TrueAllele's competitor, STRmix, was forced to reveal its source code, analysts discovered coding errors that led to misleading results. The analysis of that proprietary information substantially affected the software's reliability. In appropriate circumstances, especially where civil liberties are on the line, independent source-code review is critical when determining reliability at a Frye hearing. These case studies illustrate that software is not immune from error. Fundamental due process and fairness demand access.

We hold that if the State chooses to utilize an expert who relies on novel probabilistic genotyping software to render DNA testimony, then defendant is entitled to access, under an appropriate protective order, to the software's

---

(continued)
methodology underlying the testimony is scientifically valid" and "whether that reasoning or methodology properly can be applied to the facts in issue." Id. at 592-93. And under Daubert, general acceptance can still "have a bearing on the inquiry" but "is not a necessary precondition" to admissibility. Id. at 594, 597.

source code and supporting software development and related documentation—including that pertaining to testing, design, bug reporting, change logs, and program requirements—to challenge the reliability of the software and science underlying that expert's testimony at a Frye hearing, provided defendant first satisfies the burden of demonstrating a particularized need for such discovery. To analyze whether that burden has been met, a trial judge should consider: (1) whether there is a rational basis for ordering a party to attempt to produce the information sought, including the extent to which proffered expert testimony supports the claim for disclosure; (2) the specificity of the information sought; (3) the available means of safeguarding the company's intellectual property, such as issuance of a protective order; and (4) any other relevant factors unique to the facts of the case. Defendant demonstrated particularized need and satisfied his burden.

Importantly, the President's Council of Advisers on Science and Technology (PCAST) emphasized that probabilistic genotyping is in its infancy and such "subjective methods" must be subject to "careful scrutiny." President's Council of Advisors on Sci. & Tech., Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods 5 (2016) [PCAST Report]. We did that here. Specifically, PCAST found in 2016—and pertinent to questions of reliability—that probabilistic genotyping programs

should be independently evaluated to determine whether the methods are scientifically valid and, importantly, whether the software itself correctly implements the methods. Id. at 79. The latter has never been done for TrueAllele. Full independent access in an adversarial system is a prerequisite to meaningful cross-examination of the State's expert at the Frye hearing, and essential to the judge's threshold gatekeeping reliability determination of whether the science underlying the proposed expert testimony has "gained general acceptance in the particular field in which it belongs." State v. Harvey, 151 N.J. 117, 169 (1997) (quoting Frye, 293 F. at 1013-14).

We therefore reverse and remand for further proceedings consistent with this opinion.

I.

Just after 10:00 p.m. on April 16, 2017, two police officers traveling in an unmarked vehicle along Ocean Avenue in Jersey City observed two men, later identified as defendant and co-defendant Jonathan Ferrara, approach a group gathered near the intersection with Van Nostrand Avenue, simultaneously raise their handguns, and fire into the crowd. One victim sustained a bullet wound to the head and was pronounced dead at the scene. A second victim, a ten-year old girl, suffered a non-fatal wound to the abdomen when a bullet entered a vehicle in which she was sitting.

After the shooting, the officers pursued defendant and Ferrara as they fled down a side street with their guns still in hand. The police arrested them within a few blocks of the incident.[3] Police found a Colt .45 caliber semi-automatic handgun while retracing Ferrara's path, and recovered a .38 caliber Smith and Wesson revolver and ski mask while retracing defendant's path.

A forensic scientist detected the presence of amylase, a constituent of saliva, on the ski mask, and investigators swabbed the trigger guard, grip, and front sight of both weapons and the magazine of the Colt .45 for DNA evidence. The forensic scientist forwarded the mask and swabs to a laboratory, where analysts determined that the samples from the guns and one from the mask failed to meet the criteria for traditional DNA analysis, but that two specimens from the mask each reflected a mixture of DNA profiles, one with two contributors and the other with three. A comparison with buccal swab samples taken from defendant and Ferrara showed that defendant was the major source contributor for the DNA profiles from both the ski mask specimens conducive to traditional analysis.

---

[3] A Hudson County Grand Jury indicted and charged defendant with first degree murder, N.J.S.A. 2C:11-3(a)(1) or (2); conspiracy to commit murder, N.J.S.A. 2C:5-2; two counts of aggravated assault, N.J.S.A. 2C:12-1(b)(1) and (2); unlawful possession of a weapon, N.J.S.A. 2C:39-5(b)(1); possession of a weapon for an unlawful purpose, N.J.S.A. 2C:39-4(a)(1); hindering apprehension, N.J.S.A. 2C:29-3(b)(1); and two counts of resisting arrest, N.J.S.A. 2C:29-2(a)(2) and (3).

Because the remaining samples failed to satisfy the criteria for traditional DNA analysis, the State forwarded the testing data to Cybergenetics Corp. Laboratory (Cybergenetics), a private firm in Pittsburgh, for analysis using its proprietary TrueAllele computer software program. Ferrara could not be identified as a contributor to any of the samples under the statistical analysis, but defendant was identified as a source of the DNA on the Smith and Wesson and the ski mask.

There is a substantial difference between testing DNA utilizing traditional DNA methods and analyzing low levels or complex mixtures of DNA relying on probabilistic genotyping software.

In traditional DNA analysis, DNA is chemically extracted from a biological sample and amplified at a predetermined set of segments, or loci, using polymerase chain reaction (PCR), a technique that replicates the desired segments to generate millions of copies of each. PCAST Report, at 69. The lengths of the resulting fragments are then extrapolated, by comparison with known molecular size standards, from the distance each travels through a polymer solution during a process called capillary electrophoresis. Ibid. The analyst then generates a profile from the pair of lengths measured at each locus—one for each of the genetic variants, or alleles, inherited from each

parent—and uses the resulting list of alleles for comparison to known samples. Ibid.

For a single-source sample, identifiable by the presence of at most two distinct fragment lengths—one reflecting each allele—for each locus, the profile may be directly compared with that for a known individual to assess whether the profiles match. Id. at 70. For a simple mixture involving genetic material from two individuals, on the other hand, analysis proceeds in much the same manner, but requires first distinguishing the two separate profiles, either by an imbalance in material rendering one contributor more dominant than the other or by the presence of a known individual's DNA in the mixture, such as is often the case in the sexual assault context. Id. at 70, 73. In conjunction with the simple determination of a match in the list of alleles, human analysts also typically calculate a "random match probability"—a statistic measuring the likelihood that another individual in the relevant population, selected at random, would have the same genotype as the contributor to the sample. Id. at 72-73. The smaller the probability, the more solid the match.

But analysis is more difficult with complex mixtures, particularly where the genetic material involved is small:

> Such samples result in a DNA profile that superimposes multiple individual DNA profiles.

> Interpreting a mixed profile is different for multiple reasons: each individual may contribute two, one or zero alleles at each locus; the alleles may overlap with one another; the peak heights may differ considerably, owing to differences in the amount and state of preservation of the DNA from each source; and the "stutter peaks" that surround alleles (common artifacts of the DNA amplification process) can obscure alleles that are present or suggest alleles that are not present. It is often impossible to tell with certainty which alleles are present in the mixture or how many separate individuals contributed to the mixture, let alone accurately to infer the DNA profile of each individual.
>
> [Id. at 75-76.]

Compounding that problem, analysis of small samples often entails allele "drop-in"—the detection of an allele from a contaminant DNA fragment that was not part of the original sample—or "drop-out"—the failure to detect an allele from DNA belonging to the sample, usually due to insufficiency of the quantity for analysis. John M. Butler, Advanced Topics in Forensic DNA Typing 324-26 (2011). The consequence is that analysis of these samples is inherently more probabilistic and leaves more room for interpretation than for the single-source or simple-mixture samples that have been traditionally subject to DNA testing using the above procedures. PCAST Report, at 76.

The TrueAllele Casework system is one of several software programs developed with the goal of undertaking analysis of these more complex samples in as objective a manner as possible. PCAST Report, at 78-79. Such

programs employ probabilistic genotyping, the "use of biological modeling, statistical theory, computer algorithms, and probability distributions," to "assist," rather than "replace," "the DNA analyst in the interpretation of forensic DNA typing results." Science Working Group on DNA Analysis Methods (SWGDAM), Guidelines for the Validation of Probabilistic Genotyping Systems 2 (June 2015) [SWGDAM Guidelines].

Specifically, the programs use mathematical models and simulations, subject to parameters programmed into the software to account for drop-in or drop-out effects and other issues, id. at 3, to calculate a likelihood ratio—a statistic measuring the probability that a given individual was a contributor to the sample against the probability that another, unrelated individual was the contributor. Justice Ming W. Chin et al., Forensic DNA Evidence § 5.5 (2020). In contrast to the implication for a random match probability, the higher the likelihood ratio, the more solid the match.[4]

The State requested a Frye hearing, acknowledging that TrueAllele has not yet been found reliable and admissible in New Jersey. The judge

[4] The reason for the inverse relationship is that the random match probability represents the likelihood that someone other than defendant was the contributor, while essentially the same probability constitutes the standard of comparison—the denominator—in the likelihood ratio. In the trivial case of a single-source sample, the figures should be direct reciprocals of one another. PCAST Report, at 70 n.178.

commenced the hearing, at which a co-founder of Cybergenetics, Dr. Mark Perlin, testified for two days ending in April 2019. The judge qualified Dr. Perlin as an expert in "the fields of DNA Evidence, Interpretation, and Likelihood Ratio."

Prior to cross-examination, defendant moved for TrueAllele's software source code and related documentation. Specifically, the defense sought the source code and "all software dependencies such as third-party code libraries, toolboxes, plug-ins, and frameworks," as well as "[s]oftware engineering and development materials describing the development, deployment, and maintenance" of the code. Defendant challenged the reliability of the probabilistic genotyping program, refusing to blindly accept validation studies involving Dr. Perlin, none of which were, as PCAST called for, independent studies to investigate whether the program's software correctly implemented the underlying probabilistic genotyping methods.

The parties submitted written declarations by experts detailing, among other things, the uncertainty involved in DNA mixture interpretation, the need for verification and validation (V&V) of software engineering, the existence of software engineering failures, and materials relevant to testing probabilistic genotyping software. Defense counsel produced a declaration written by defendant's expert, Nathaniel Adams, a systems engineer retained to address

the reliability of the science underlying testimony based on TrueAllele. The State produced a declaration by Dr. Perlin. The parties were apparently satisfied—as was the judge—that the detailed declarations, Dr. Perlin's testimony over two days, and the documentation introduced at the Frye hearing, established a sufficient motion record. We reach that conclusion because the State did not move to require testimony from Mr. Adams or further testimony from Dr. Perlin, or otherwise seek a limited remand for that purpose. In our view, that is not surprising given the detailed record and declarations submitted by the experts addressing the source code.

Mr. Adams has important and extensive experience performing probabilistic genotyping analyses, including undertaking review of source codes. He reviewed "software development materials, including source code, for [the] probabilistic genotyping systems STRmix[] and FST used in criminal cases in New York, Illinois, United States, and Australian courts." He explained:

> Since the likelihood calculations are dependent on the statistical models (algorithms) underlying the probabilistic software, and software behaviors affecting the models will necessarily impact the calculated likelihoods and ultimately the reported likelihood ratio. Complex systems such as TrueAllele[] involve a hierarchy of models with dozens or hundreds of parameters, each affecting the overall system's behavior.

Mr. Adams pointed out that forensic DNA analysis "lacks formal standards specific to the development and validation of probabilistic genotyping software."[5] But software quality unquestionably depends in part on the "quantity and severity of defects present in the program." He spelled out that defects cause incorrect and misleading results. One goal of the V&V processes is to assure "appropriate . . . methods have been used throughout the software development process and have produced an acceptable product." V&V involves reviewing software development materials for "correctness, completeness, consistency, and accuracy." We need not detail every aspect of his declaration; suffice it to say that Mr. Adams provided the judge with an in-depth and thorough basis to grant the motion.

Dr. Perlin submitted a seventy-eight-paragraph declaration, which the State attached to its September 13, 2019 letter opposition brief to the judge.

---

[5] Mr. Adams explained that, although there is no "common standard for the development of software specific to genotyping systems such as TrueAllele[], general industry standards and principles of software engineering can be used to ensure correctness of the systems." As the International Society of Forensic Genetics (ISFG) stated, international industry standards applicable to software validation, verification, and test documentation "can be simplified and extrapolated to forensic genetics." ISFG referenced four levels of system integrity standards identified by the Institute of Electrical and Electronics Engineers (IEEE) encompassing "all software programs and systems." Mr. Adams is unaware of "any formal guidance on probabilistic genotyping system validation methods." But there are IEEE standards setting forth a checklist for "stages of verification" especially pertinent to source-code and related documentation review.

His declaration covered such topics as the role of TrueAllele in DNA analysis; TrueAllele's purported widespread acceptance; whether TrueAllele is reliable; background on the software source code; an explanation for why TrueAllele is a trade secret; the risks of disclosing the source code; and importantly, the reasons for why TrueAllele's source code is not needed. His declaration, therefore, developed the record for the judge's consideration of defendant's discovery motion.

Dr. Perlin explained that the source code details "step-by-step human-readable instructions that describe to the computer and programmers how the program operates." According to Dr. Perlin, who has degrees in chemistry, mathematics, medicine, and computer science, the source code "contains the software design, engineering know-how, and algorithmic implementation of the entire computer program." Although the software program itself is patented, its source code is not disclosed in patent documents; instead, Cybergenetics "considers the . . . source code to be a trade secret."[6] Dr. Perlin,

---

[6] TrueAllele's source code qualifies as a trade secret. Cybergenetics has closely guarded this information and, indeed, defendant emphasizes that fact in attacking the program's purported inscrutability. See Hammock by Hammock v. Hoffmann-LaRoche, Inc., 142 N.J. 356, 384 (1995) (defining trade secret as "compilation of information . . . used in one's business" so as to afford "advantage over competitors," and recognizing protection to the extent information kept is secret (quoting Smith v. Bic Corp., 869 F.2d 194, 199 (3d Cir. 1989))).

although he was the State's expert, advocated on behalf of his company that access to the source code would be "immaterial to [a criminal] case," "[un]reasonable," and not "in the interests of justice."

According to Dr. Perlin, TrueAllele's software program consists of approximately 170,000 lines of source code written in MATLAB, a mathematical programming language designed specifically for visualizing and programming numerical algorithms. Dr. Perlin volunteered that it could take hours to decipher only a few dozen lines of the "dense mathematical text" comprising the code, and estimated that it would take a person, reading at a rate of ten lines per hour, about eight and a half years to review the code in its entirety.

Dr. Perlin explained that Cybergenetics operates in a "highly competitive commercial environment." According to him, at least ten other groups have developed "similar software." He defended confidentiality by asserting "for-profit companies [like Cybergenetics] generally do not make their source codes available to the public." Such secrecy gives Cybergenetics a commercial "advantage over its competitors" because they do not know—nor does anyone else—the proprietary code. Once divulged, proprietary trade secrets, Dr. Perlin explained, are "valuable to competitors" and can be "sold for profit." He declared that ample material for this case had already been

provided, including "over thirty validation studies and publications." His declaration omits reference to his own involvement in those studies, or the participation in the studies of current or former employees of Cybergenetics, and he neglected to acknowledge the lessons learned from STRmix and FST, which were revealed once other courts forced them to make accessible their source codes for independent review under protective orders.

Dr. Perlin explained that Cybergenetics permits testing the software online through cloud computing without having to purchase the product, and makes its methodology, which has long been published, and testing results available for review and questioning, either at its Pittsburgh office or by teleconference. Cybergenetics offered defendant an opportunity for "inspection" of the source code under a severely restrictive non-disclosure agreement (NDA), which limited inspection to an expert witness retained by defendant at a time and place determined by the company, under supervision by a company representative, and video surveillance and recording at all times. According to the NDA, a stand-alone computer that would not accept storage devices would be provided for viewing the source code, and, although the expert could make handwritten notes, the expert would be forbidden from bringing any photographic devices, including smart phones or tablets, into the room, and would be bound to turn any notes over to Cybergenetics. The expert

would be broadly bound to accept responsibility for any legal and financial consequences, including a $1,000,000 automatic fine, in the event of a breach and could not "be a developer of competing software products" or "have any (direct or indirect) commercial, research or employment interest in such products."

Mr. Adams emphasized that several of the restrictions Cybergenetics imposed would undermine an effective review of the source code for purposes of assessing TrueAllele's reliability. Specifically, the prohibitions on taking notes except by hand and on accessing the Internet or any removable storage device would inhibit adequate "documentation of the inspection process and collection of demonstrative materials," and his inability to compile or execute the source code would be detrimental to any "rigorous . . . inspection." The ban on email communication, meanwhile, would restrict his consultation with defense experts in other relevant fields, such as biology, statistics, or software development, which would be necessary for understanding and evaluating the source code and related proprietary information. Mr. Adams did not believe any expert would agree to the automatic assumption of all liability for a breach.

Defendant's separate proposed protective order provided that the materials would remain confidential and used solely for purposes of

preparation of defendant's defense in this matter, that no recipient could "reveal, use, or disclose any part" of it, except in compliance with the restrictions in the order, and that no third-party could be granted access without first agreeing to be bound by the same terms. Defendant's order would forbid any disclosure at all to a consultant or expert who was "the developer of" or who "have any direct or indirect commercial or employment interest in competing software products." The source code would be made available in a specified accessible format on a stand-alone computer provided by Cybergenetics for the expert to review and, as necessary, "make inspection notes, use necessary software, [and] create snippets or screen shots of relevant lines of code for use in his/her report." All materials, moreover, would be filed under seal, and all counsel would be bound to take all "reasonable and appropriate measures to prevent unauthorized disclosure," with any violation subject to civil and criminal sanction.

In response, Cybergenetics offered to remove some of the conditions for disclosure in its initial agreement, including the requirement for the expert to turn over any notes, but left most in place, most notably the broad acceptance of liability and the prohibition on taking notes or documenting the inspection in any other manner than by pen and paper. But the parties were unable to reach an agreement despite "[e]xtensive communications between the parties."

Indeed, at oral argument in October 2019, the judge and counsel agreed that an appropriate protective order would accommodate all concerns. To that end, defense counsel produced a sample protective order utilized in Illinois, when a court there ordered STRmix to make its source code accessible for independent review. Although the assistant prosecutor stated this case had a "long and torturous procedural history," and eventually conceded that the source code had never been independently examined or tested, especially by software scientists, he agreed with the judge that "all [the State] need[ed]" before access was given were "conditions and parameters to protect [Cybergenetics'] proprietary interests." Oral argument was carried at least seven times during which counsel unsuccessfully discussed negotiating a protective order.

On June 23, 2020, the judge entered an order denying defendant's motion. The judge did not explicitly—for purposes of the discovery motion and his reliability determinations under Frye—address the importance of allowing defendant an opportunity to independently evaluate whether TrueAllele's software correctly implements the probabilistic genotyping methods, as emphasized by PCAST, rather than relegating defendant to blindly accepting that the software operated as intended. The judge omitted reference to whether the software's program contained bugs, glitches, or defects, and if

so, whether such problems—untested in an adversarial system—could affect the software's output, which would in turn affect the reliability of TrueAllele. Pointing to unilateral conditions imposed solely by the State, the judge noted, however, that

> [t]he State is willing to make the source code available for defense expert review. The State submits the defense expert is welcome to come to the prosecutor's office, view the source code on a provided device, and take notes.

Understandably, the State never contended before the judge that the judge was missing any substantial pertinent information to make an informed decision on defendant's motion for the discovery. We believe that is primarily because the judge had the detailed source-code declarations by the experts, Dr. Perlin's testimony over two days, validation studies and peer-reviewed articles, as well as out-of-state case law addressing the reliability of TrueAllele. Indeed, the State's willingness to permit limited access demonstrates its main objection pertained not to accessing the source code but rather reasonable parameters surrounding inspection. Defendant, meanwhile, maintains the parameters the State has thus far offered are unreasonably burdensome and restrictive.

In July 2020, we granted leave to appeal from the June 23, 2020 order; we later granted amici permission to participate. As we pointed out, and as

part of defendant's motion for leave to appeal, and thereafter, the State never requested a limited remand to expand the Frye record with additional testimony by Dr. Perlin or anyone else. The record therefore demonstrates the parties did not in any meaningful way dispute the adequacy of the motion record.

II.

On appeal, defendant argues the following points, which we have partially re-numbered:

> POINT I
>
> THE RELIABILITY OF TRUEALLELE CANNOT BE DETERMINED WITHOUT COMPLETE DEFENSE ACCESS TO ITS SOURCE CODE AND THE TOOLS NECESSARY TO INSPECT THAT CODE.
>
> > 1. TrueAllele Is Dramatically Different Than Traditional DNA Analysis And Its Reliability Has Never Been Established In New Jersey.
> >
> > 2. A Complete Review Of Source Code Is Necessary For A Rigorous Assessment Of TrueAllele's Reliability.
> >
> > > i. Errors in software programs are ubiquitous and often have devastating results. Nothing short of full source-code review can catch and correct these errors.
> > >
> > > ii. Errors in the source code of probabilistic genotyping software have been found. There is no reason to assume

that TrueAllele, whose source code has never been subject to outside inspection, is immune from these errors.

iii. Validation studies and peer-reviewed articles are not a substitute for source-code review.

3. Defendant Is Entitled To The Source Code And Related Materials Under Our Discovery Rules And Jurisprudence. Any Proprietary Interests Cybergenetics Has Can Be Accommodated By A Protective Order.

4. This Court Should Not Repeat The Mistake Of Other Courts By Failing To Subject TrueAllele To Source-Code Review Before Ruling On Its Admissibility.

5. Disclosure Is Necessary To Preserve The Fairness Of Any Trial In Which TrueAllele May Be Used In The Future.

In his reply letter brief, defendant makes the following additional contentions, which we have re-numbered:

[POINT II]

THE MATERIALS THE DEFENSE SEEKS ARE NECESSARY IN ORDER FOR TRUEALLELE'S RELIABILITY, AND THEREFORE ADMISSIBILITY, TO BE DETERMINED.

1. The State's Conclusory Assertion That The Materials At Issue Are A Trade Secret Does Not Shield These Materials From Disclosure.

2. The State Has Failed To Demonstrate That TrueAllele's Reliability Can Be Assessed Without Access To These Materials.

III.

We have the benefit of extraordinarily thoughtful amici briefs from a multitude of organizations, including the New Jersey Attorney General and other interested entities from around the nation. Before directly analyzing the issues, we detail their positions. Doing so informs our analysis and holding.

(i)

New Jersey Attorney General (AG)

The AG asserts that defendant requires the State to prove that TrueAllele is "infallible," which the AG argues is not required under Frye. The AG argues the State satisfied its burden under Frye by offering three things: testimony by Dr. Perlin; "validation studies and publications"; and opinions from other jurisdictions in which those courts have deemed TrueAllele reliable without independent inspection of the proprietary information. The AG states that access to the source code is therefore unnecessary to determine whether TrueAllele is generally accepted in the scientific community. The AG argues complete general acceptance is not required, and that "any concerns are best served during cross-examination."

The AG suggests that if this court deems full access is possibly necessary, then we should remand and allow testimony from Dr. Perlin and Mr. Adams about whether access to proprietary information is appropriate. The AG cites State v. Ghigliotty, 463 N.J. Super. 355, 384-85 (App. Div. 2020), for the proposition that defendant must "provide the [judge] with a rational basis" before allowing reasonable access. According to the AG, defendant failed to do so here.[7]

At oral argument, the AG conceded the State will not be prejudiced by disclosure of the discovery. The AG argues the State is willing to make the trade secrets available to defendant, but contends defendant is unreasonably unsatisfied with the State's terms of inspection. The AG contends that defense counsel wanted "unsupervised and unrestricted access to proprietary information." In affording access to the information, the AG asserts that the State "removed many of the typical restrictions required." The AG states "[a] protective order that offers no protections is not adequate in a competitive market." As the AG points out, the parties unsuccessfully attempted negotiating terms of such an order.

---

[7] The AG's written submission omitted any reference to the significant reliability problems uncovered once STRmix and FST produced their proprietary information by court order for independent review under protective orders.

(ii)

The Innocence Project

The Innocence Project maintains that analyzing the source code is critical to determining the reliability of TrueAllele because it would reveal, among other things, errors in coding or input. The Innocence Project underscores these indisputable facts: people write source codes; people make mistakes.

The Innocence Project states that genotyping software is prone to error, as exemplified by the problems associated with STRmix and FST. It is not enough—as the State argues—to allow inspection of articles discussing how TrueAllele is intended to work; without the source code it is impossible to detect errors in implementation. Without access to the source code one cannot identify errors or biases, which the Innocence Project explains are relevant to reliability at the Frye hearing. Although algorithms and models are publicly available, TrueAllele's source code, which the Innocence Project contends is prone to error even when the corresponding algorithms and models may be correct, is known only by individuals at Cybergenetics. At oral argument, the Innocence Project emphasized that, while validation studies are important and programs may find their way into court without them, independent review and the judge's Frye gatekeeping should not be perfunctory.

(iii)

Upturn, Inc. (Upturn)

Upturn, an organization seeking to advance equity and justice in the design, governance, and use of technology, points out that TrueAllele's source code has never been independently reviewed, and that such a review is a basic and necessary step in ensuring reliability. Importantly, the version of TrueAllele software utilized in defendant's case postdates every one of the validation studies cited by Cybergenetics and the State. It explains this is critical because subsequent source code variations may introduce new errors not previously present. Undertaking an independent review establishes whether the software is properly implementing the program's design specifications and that the code itself is devoid of bugs, glitches, and defects that could affect the software's output. And equally important is that TrueAllele's source code has never been scrutinized by any party outside of Cybergenetics; therefore, the validation studies produced by the State to date are limited.

Upturn points out that looking at what happened with FST in New York—when a federal judge required OCME to make available the source code for the program, revealing errors—demonstrates the significance of what is at stake. Mr. Adams examined FST's code and discovered two critical

problems: the code did not implement FST's methods and models utilized in FST's validation studies, and there were coding errors. The New Jersey Supreme Court did the same thing in Chun, by requiring Draeger to produce its source code. Upturn encourages this court to take the same action to assess TrueAllele's reliability at the Frye hearing.

Upturn maintains that trade secrets should not be prioritized over considerations of justice, especially because production of a for-profit company's trade secret can be reviewed under an appropriate protective order. Upturn relies on N.J.S.A. 2A:84A-26 (rejecting application of trade secret privilege where it "tend[s] to conceal fraud or otherwise work[s] injustice"), and it contends that interpreting evidentiary privileges narrowly, Pierce Cnty. v. Guillen, 537 U.S. 129, 144 (2003), provides further support for resisting application of the privilege whenever that would impede justice.

(iv)

The Association of Criminal Defense Lawyers of New Jersey (ACDL-NJ)

ACDL-NJ asserts that probabilistic genotyping has not yet been used or tested in New Jersey. Like other amici, ACDL-NJ argues that, given that TrueAllele's leading competitor, STRmix, has produced its source code and conceded its software had errors, rigorous scrutiny of TrueAllele's source code becomes even more compelling. If anything, STRmix's source-code problems

reaffirm the basic principle in computer engineering that software is prone to human error.

ACDL-NJ argues the source code is discoverable under New Jersey law. Of course, the United States Constitution and the New Jersey Constitution guarantee a meaningful opportunity to present a complete defense. But ACDL-NJ asserts that New Jersey's robust discovery practices are broader than those of other jurisdictions. For example, Rule 3:13-3(b) provides a non-exhaustive list of discoverable materials. And in Chun, the Court allowed the defendants to analyze the source code of the software that ran the Alcotest, which disclosed two errors that affected the way Alcotest results had been used in prosecutions. 194 N.J. at 94.

Finally, ACDL-NJ argues that requiring a defense attorney to sign any order that preconditions a defense expert's review of the source code in practical ways—such as in this case—is prohibitive. Doing so impedes counsel's ability to provide an effective defense, which would be free from any conflict of interest. Here, there are enormous problems associated with the State's proposed protective order: defense counsel could only make handwritten notes while looking at hundreds of thousands of lines of code; counsel could not use electronic devices; the only computer available to counsel would be one provided by Cybergenetics; counsel would be under

constant supervision; and counsel would be exposed to monetary damages, including fees and costs, as spelled out under the State's terms. Rather, ACDL-NJ contends that the judge should issue an appropriate protective order that protects Cybergenetics' proprietary interests, while simultaneously protecting defendant's liberty interests. ACDL-NJ notes that protective orders have safeguarded trade secrets in high-risk civil litigation for years and can therefore do so here.[8]

(v)

The Legal Aid Society (LAS)

LAS is the primary public defender in New York City. LAS has first-hand experience litigating the admissibility of a proprietary probabilistic genotyping program—FST—including successfully obtaining access to FST's source code, which led to an alarming discovery: significant flaws existed in

---

[8] ACDL-NJ also argues that the source code is hearsay and considered a testimonial statement; without it, defendant's confrontation rights are violated. ACDL-NJ relies on a New York appellate opinion, People v. Wakefield, 107 N.Y.S.3d 487, 496-97 (App. Div. 2019), which held that TrueAllele was testimonial, but that Dr. Perlin was the declarant and his availability for cross-examination cured any confrontation right issues. We need not address issues that may arise at trial; at this point the question is whether defendant is entitled to the proprietary information for the sole purpose of challenging at a Frye hearing the science underlying novel DNA analysis software and expert testimony. Having concluded that defendant is entitled to the review—under a protective order—questions of defendant's confrontation rights at trial need not be addressed at this point.

the software program. Without access to the source code, the defects and glitches in the software would not have been uncovered. The bugs in the program were substantial enough for OCME to cease using FST, which up to that point had been used in thousands of criminal prosecutions over several years.

Like the other amici, LAS emphasizes the extraordinary complexity of probabilistic genotyping. LAS urges us to carefully consider the inherent limitations of the expert testimony, scientific and legal writings, and judicial opinions submitted by the State: none required an examination of TrueAllele's source code. Consequently, LAS implores us to consider the State's submissions with healthy skepticism.

LAS explains that probabilistic genotyping software is intended to address interpretational challenges of testing low levels or complex mixtures of DNA. For example, stochastic effects and artifacts complicate determining genotypes, or DNA profiles: alleles not belonging to true donors appear, they can be distorted, and artifacts appear as real alleles. LAS points out PCAST emphasized that probabilistic genotyping is in its infancy and must be subject to "careful scrutiny." PCAST Report, at 79. Specifically, PCAST found in 2016—and pertinent to questions of Frye reliability—that probabilistic genotyping programs should be evaluated to determine "whether the methods

are scientifically valid" and importantly, "whether the software correctly implements the methods." Ibid. And critical to the determination, according to PCAST, is testing by independent entities "not associated with the software developers." Ibid. LAS states that the only way to determine whether a program operates as intended is to evaluate how the program performs its calculations, which requires access to the source code.

Fortunately, due to its own efforts, LAS points to the case study of FST, troubling that it is, which demonstrates the importance of an independent and full source-code review when a judge makes a threshold reliability determination of whether novel forensic software has achieved general acceptance in the relevant scientific community. The creators of FST fought tooth and nail not to disclose its source code. But after a federal judge denied OCME's motion to quash a subpoena for the source code, a stark discovery was made about the program: the FST did not work as promised. FST was utilized in thousands of criminal prosecutions before the discovery was made. OCME announced—after the production of the source code—that it would phase out using FST in criminal prosecutions.

According to LAS, the State's assertion that the source code was not needed in any of TrueAllele's "numerous [prior] nationwide admissibility rulings," is at best misguided. LAS implores us to carefully examine the

premise of that body. LAS contends that what matters is not the number of cited opinions, but rather, the power of the court's reasoning. LAS reminds us, as the New York Court of Appeals recently stated in People v. Williams, 147 N.E.3d 1131, 1140-42 (N.Y. 2020), that it was a mistake to rely on the repetition of case law to establish reliability; rather, for purposes of a Frye hearing, lower courts were bound to ensure that FST was "supported by those [in the relevant scientific community] with no professional interest in its acceptance." LAS urges us to heed the lessons of FST and permit full independent access to the source code under a protective order.

(vi)

Drs. Mats Heimdahl and Jeanna Matthews

Drs. Heimdahl and Matthews are experts in engineering, testing, and validating computer systems, including forensic evidentiary software. They, together with eight other experts in this specific field that they have identified, argue that reliability of the TrueAllele software cannot be evaluated without full access to "executable source code and related documentation," something that no one to date has seen. They contend that doing so is not only prudent, but essential to determining whether TrueAllele operates as Cybergenetics claims, which is fundamental to any fair, legitimate, and impartial assessment of reliability.

Drs. Heimdahl and Matthews remind us that software faults are ubiquitous. They argue that even simple software programs are prone to failure, and that an error in any one of the three domains of software engineering—problem identification, algorithm development, and software implementation—undermines the trustworthiness of the science underlying the relevant expert testimony, because the system is consequentially compromised. After providing examples illustrating various errors in more simplistic software, they demonstrated that a greater risk of flaws in more complex programs are likely.

For example, a source code review revealed at least thirteen STRmix coding faults. Drs. Heimdahl and Matthews argue, in one important example, a miscode impacted sixty criminal cases, requiring new likelihood ratios to be issued in twenty-four of them. These errors were not discovered until the source code was independently examined.

In FST, alarming discoveries were also made. But the findings did not come to light until a federal judge ordered disclosure of FST's source code. Once that occurred, it was uncovered that a "secret function . . . was present in the software, tending to overestimate the likelihood of guilt." And the functioning of the software did not use the "methodology publicly described in

sworn testimony and peer-reviewed publications." These discoveries led to the overturning of a high-profile conviction.

Drs. Heimdahl and Matthews assert that thousands of faults were discovered in the source code of breathalyzer systems. They point out that judges in Massachusetts and New Jersey threw out more than 30,000 breath tests in a twelve-month period. Drs. Heimdahl and Matthews urge us not to ignore these facts.

Drs. Heimdahl and Matthews argue that the testing of TrueAllele is incomplete. Thirty-five of the thirty-six validation studies produced by the State, which were written by or included involvement from current or former employees of Cybergenetics or law enforcement agencies, did not consider the source code, and they were otherwise incomplete because the number of samples tested was relatively small. They note that TrueAllele's software is non-continuous, meaning that correct results for the samples used in the validation studies do not preclude the possibility of erroneous results for others that do not match those samples. Thus, for a reliability determination, independent and full access to the software is required. Supporting software development documentation must be produced, including that pertaining to testing, design, bug reporting, change logs, and program requirements, which will provide a road map to understanding the source code.

(vii)

American Civil Liberties Union of New Jersey (ACLU-NJ)

The ACLU-NJ argues that independent review is essential. Questioning Dr. Perlin, reviewing validation studies and peer-reviewed articles in which he or his current or former employees were involved, or relying on out-of-state judicial opinions citing his testimony and those studies misses the importance of objective analysis of the science underlying his forensic testimony. Most importantly, it cannot substitute for independent analysis of the code itself, which would demonstrate whether the software operates as intended.[9]

---

[9] We need not address the ACLU-NJ's additional contention—raised for the first time—that use of likelihood ratio evidence so inherently undermines a criminal defendant's right to a fair trial, by eroding the prosecution's burden of proof and biasing the jury, that it should be excluded at trial regardless of its scientific reliability. Defendant did not raise these points, no related record has been assembled, and the judge made no pertinent factual findings or legal conclusions. It is well established that generally, an amicus curiae "must accept the case before the court as presented by the parties and cannot raise issues not raised by the parties." State v. Lazo, 209 N.J. 9, 25 (2012) (quoting Bethlehem Twp. Bd. of Educ. v. Bethlehem Twp. Educ. Ass'n, 91 N.J. 38, 48-49 (1982)). The parties are not, however, precluded from addressing these contentions at the right time.

We, however, make the following brief remarks. Criminal defendants, of course, enjoy a presumption of innocence, and may be convicted only on proof beyond a reasonable doubt, In re Winship, 397 U.S. 358, 363-64 (1970), but those principles do not appear to be inherently implicated by this evidence. The probability of defendant's contribution to a DNA sample is a component of the likelihood ratio, but the denominator—the standard of comparison—is the probability that another, unrelated individual from the relevant population

IV.

As the New Jersey Supreme Court recently stated, "the Judiciary must ensure that proceedings are fair to both the accused and the victim. Trial judges partly fulfill that responsibility by serving as a gatekeeper. In that role, they must assess whether expert testimony is sufficiently reliable before it can be presented to a jury." State v. J.L.G., 234 N.J. 265, 307-08 (2018). When the evidence is labeled as scientific and expert, there is substantial danger that juries will accord excessive weight to testimony that might otherwise be unreliable. Ghigliotty, 463 N.J. Super. at 373. The law accounts for this eventuality.

(continued)
contributed to the sample instead—a presumption of innocence. Indeed, random match probability widely accepted for use as to traditional DNA analysis essentially embodies the same probabilities, just subject to the reverse comparison. PCAST Report, at 70 n.178.

The authority on which the ACLU-NJ relies is not to the contrary. The courts in State v. Hartman, 426 N.W.2d 320, 326 (Wis. 1988), and State v. Skipper, 637 A.2d 1101, 1103-08 (Conn. 1994), both rejected admission of a probability-of-paternity figure on the ground that its calculation presumed the defendant had engaged in intercourse with the victim he was alleged to have sexually assaulted. But at issue in both cases was not a composite statistic, such as the likelihood ratio, but a simple probability estimate directly calculated using the very presumption it was meant to prove. Here, in contrast, the probability that defendant was a contributor to the sample was calculated based on simulations from the sample data, not on any presumption of his contribution. The likelihood ratio calculated from that probability likewise does not presume his guilt but effectively compares the probability of his guilt against a presumption of innocence.

To fulfill their gatekeeping responsibility, judges begin by applying N.J.R.E. 702, which states that, "[i]f scientific . . . knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education may testify thereto in the form of an opinion or otherwise." To satisfy this requirement,

> the proponent of expert evidence must establish three things: (1) the subject matter of the testimony must be "beyond the ken of the average juror"; (2) the field of inquiry "must be at a state of the art such that an expert's testimony could be sufficiently reliable"; and (3) "the witness must have sufficient expertise to offer the" testimony.
>
> [J.L.G., 234 N.J. at 280 (quoting State v. Kelly, 97 N.J. 178, 208 (1984)).]

In general, these prongs "are construed liberally in light of [N.J.R.E.] 702's tilt in favor of the admissibility of expert testimony." State v. Jenewicz, 193 N.J. 440, 454 (2008). The first and third prongs are not at issue here; rather, the second prong is. The parties and amici have focused—as do we—on whether defendant is entitled to independently review the source code and related documents pertaining to the reliability prong before cross-examination of Dr. Perlin and before the judge completes his important Frye reliability gatekeeping function.

In criminal cases, the Supreme Court of New Jersey has continued to apply the Frye standard to assess scientific reliability lying beneath the expert testimony.[10] J.L.G., 234 N.J. at 280. The Frye test requires trial judges to determine whether the particular science underlying the proposed expert testimony has "gained general acceptance in the particular field in which it belongs." Frye, 293 F. at 1014; accord J.L.G., 234 N.J. at 280; Harvey, 151 N.J. at 169; see also State v. Torres, 183 N.J. 554, 568 (2005). "Although we look for wide support within the relevant scientific community, complete agreement is not required for evidence to be admitted." J.L.G., 234 N.J. at 281. Importantly—like here—there might be more than one scientific community to consider. Thus, to assess the reliability prong of N.J.R.E. 702, and relevant to the issues on appeal, the judge should consider—as to general acceptance in the scientific community—whether Cybergenetics' TrueAllele probabilistic genotyping computer program is scientifically valid and importantly, whether the source code itself correctly implements the methods. But to do that raises the question of whether defendant is first entitled to discovery of the proprietary information he seeks, which brings us to our legal analysis.

---

[10] The parties and amici have not asked us to depart from Frye and adopt the Daubert test utilized by federal courts.

V.

The right to a fair trial is fundamental and guaranteed pursuant to the Fifth and Sixth Amendments of the United States Constitution, as well as the New Jersey Constitution. U.S. Const. amend. V, VI; N.J. Const. art. I, ¶ 10. Our Constitutions also ensure criminal defendants "a meaningful opportunity to present a complete defense." State v. Garron, 177 N.J. 147, 168 (2003) (quoting Crane v. Kentucky, 476 U.S. 683, 690 (1986)). These fundamental legal rights are the hallmark of our judicial process, a process which technology has recently heavily impacted. Forensic evidentiary computer software itself generates expert evidence, and the New Jersey Rules of Evidence enable the introduction and, consequently, cross-examination of expert witnesses. N.J.R.E. 702. Without access to the source code—the raw materials of the software programming—a defendant's right to present a complete defense, by meaningful cross-examination at the appropriate juncture, may be substantially compromised. Relevant to this case, "[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." State in the Interest of A.B., 219 N.J. 542, 556 (2014) (quoting Ake v. Oklahoma, 470 U.S. 68, 77 (1985)). We must keep these principles in mind and front and

center during our review of the judge's order denying full access to the discovery sought.

In criminal cases, we ordinarily apply an abuse of discretion standard on discovery motions, State v. Stein, 225 N.J. 582, 593 (2016), and on evidentiary determinations, State v. Prall, 231 N.J. 567, 580 (2018), but here defendant sought access—at a Frye hearing—to proprietary information solely to challenge the reliability of the science underlying novel DNA analysis evidentiary software and expert testimony. An appropriate review therefore requires that we also independently scrutinize the record, including the comprehensive and amplified declarations of the experts, the scientific validation studies and peer-reviewed publications, and judicial opinions. See In re Commitment of R.S., 339 N.J. Super. 507, 531 (App. Div. 2001) (noting that when matters involve "novel scientific evidence in a criminal proceeding, 'an appellate court should scrutinize the record and independently review the relevant authorities, including judicial opinions and scientific literature'" (quoting Harvey, 151 N.J. at 167)).

Information pertinent to the Frye inquiry is subject to the same "broad pretrial discovery" otherwise afforded a criminal defendant under Rule 3:13-3(b). State v. Scoles, 214 N.J. 236, 252 (2013). Our state's "'open-file approach to pretrial discovery in criminal matters' is intended '[t]o advance the

goal of providing fair and just criminal trials.'" State v. Hernandez, 225 N.J. 451, 461-62 (2016) (alteration in original) (quoting Scoles, 214 N.J. at 252); see State v. Cook, 43 N.J. 560, 564 (1965) (noting that "discovery has long . . . been found to be a sound tool for truth"). Because of the meaningful role that the disclosure of evidence to a defendant has in promoting the search for truth—and reliability at a Frye hearing—pretrial discovery in criminal trials has long received favorable treatment in this state. See State in the Interest of W.C., 85 N.J. 218, 221 (1981) (noting sharing of pretrial information "encourage[s] the presentation of all relevant material to the jury as an aid in the establishment of truth through the judicial process"). Although that discovery is not so broad, for example, as to indulge an "unfocused, haphazard search for evidence," Hernandez, 225 N.J at 463 (quoting State v. D.R.H., 127 N.J. 249, 256 (1992)), judges are authorized to order discovery even "beyond that mandated by our court rules when doing so will further the truth-seeking function or ensure the fairness of a trial," ibid. (quoting A.B., 219 N.J. at 560).

As to the evidence at issue here, a party seeking to shield information from discovery on intellectual property grounds generally bears the burden of showing good cause to demonstrate "that the information sought is a trade secret or is otherwise confidential or proprietary." Cap. Health Sys., Inc. v. Horizon Healthcare Servs., Inc., 230 N.J. 73, 80 (2017); see also R. 4:10-3(g)

(providing that a protective order may be sought to ensure "[t]hat a trade secret or other confidential research, development, or commercial information not be disclosed or be disclosed only in a designated way"); N.J.S.A. 2A:84A-26 (providing that "[t]he owner of a trade secret has a privilege . . . to refuse to disclose the secret and to prevent other persons from disclosing it if the judge finds that the allowance of the privilege will not tend to conceal fraud or otherwise work injustice"). Yet, even once that showing of privilege is made, a criminal defendant should nonetheless be entitled to discovery of the information sought to the extent necessary to ensure a fair trial. Hernandez, 225 N.J. at 463. But the burden must shift to defendant to demonstrate a sufficient need for the evidence. See Ghigliotty, 463 N.J. Super. at 384-85 (requiring "definitive" demonstration of need for disclosure of algorithm); cf. Tractenberg v. Twp. of W. Orange, 416 N.J. Super. 354, 367 (App. Div. 2010) (discussing burden shift in the context of deliberative process privilege).

As we stated earlier, the Court ordered production of the source code in Chun. Although we ordinarily consider published decisions from other jurisdictions as persuasive, they are not binding on us. See Lewis v. Harris, 188 N.J. 415, 436 (2006) (noting that our courts are "not bound by . . . the precedents of other states, although they may provide guideposts and persuasive authority"). The rationale undergirding Chun is binding. More

recently, in Ghigliotty, 463 N.J. Super. at 360, 384-85, we too addressed the disclosure of proprietary information, algorithms underlying the software for BULLETTRAX, a novel device used for three-dimensional ballistics imaging, in contemplation of a Frye hearing. We vacated a motion judge's order requiring the State to produce the algorithms, but only because we viewed the order as prematurely issued. Id. at 384. We explicitly contemplated—as did the motion judge—that "this information might be needed by defendant's experts to evaluate the reliability of the new technology," but noted that—unlike here—there was nothing in the record to support that order. Ibid. We explained that a "defendant is required to make a more definitive showing of his need for th[e] material to provide the [judge] with a rational basis to order the State to attempt to produce" the proprietary algorithms. Id. at 384-85.

Before going any further, we stress one important point. Evaluating the issues on appeal requires a working knowledge of computer software. Without such a foundation, one can miss subtle consequences germane to this Frye hearing. Allowing independent access to the requested information, for the sole purpose of addressing whether the technology underlying the expert testimony is reliable—specifically, whether the source code for that technology is properly implementing the program's design specifications—is obvious. An accused individual's liberty is at stake; DNA evidence is

powerful and compelling.[11] Practically speaking, if, as Dr. Perlin maintains, the source code he wrote is free of harmful defects, and therefore will not impact the reliability of TrueAllele, then it is to everyone's advantage to learn that at the Frye hearing. If it should turn out there are source code errors that might affect TrueAllele's reliability, the time to discover that information is now, as part of the judge's gatekeeping role. Reliability must be resolved at the Frye hearing rather than in post-conviction relief proceedings.

We are also mindful of the important need to maintain the confidentiality of trade secrets in—as Dr. Perlin emphasized in his own declaration—a "highly competitive commercial environment." All agree on that. But shrouding the source code and related documents in a curtain of secrecy substantially hinders defendant's opportunity to meaningfully challenge reliability at a Frye hearing. The confluence of these competing and powerful interests compels our holding.

We hold that if the State chooses to utilize an expert who relies on novel probabilistic genotyping software to render DNA testimony, then defendant is

---

[11] It goes without saying that denying the State access to the source code is equally consequential in that, should a defendant attempt utilization of TrueAllele for exoneration purposes—as the State points out has been done in other jurisdictions—then the rights of the public, including the victims, would be similarly impacted. Indeed, in this case, TrueAllele did not find co-defendant's DNA match.

entitled to access, under an appropriate protective order, to the software's source code and supporting software development and related documentation—including that pertaining to testing, design, bug reporting, change logs, and program requirements—to challenge the reliability of the software and science underlying that expert's testimony at a Frye hearing, provided defendant first satisfies the burden of demonstrating a particularized need for such discovery. To analyze whether that burden has been met, a trial judge should consider: (1) whether there is a rational basis for ordering a party to attempt to produce the information sought, including the extent to which proffered expert testimony supports the claim for disclosure; (2) the specificity of the information sought; (3) the available means of safeguarding the company's intellectual property, such as issuance of a protective order; and (4) any other relevant factors unique to the facts of the case. Applying this framework to the facts, we conclude defendant satisfied his burden.

(i)

Rational basis for accessibility and expert testimony

In addressing this prong—whether there exists a rational basis for accessibility of the proprietary information—we must address the "three ways to establish general acceptance under Frye: expert testimony, authoritative scientific and legal writings, and judicial opinions." J.L.G., 234 N.J. at 281.

We do this by independently scrutinizing these categories with the benefit of lessons learned by the consequential software errors associated with STRmix and FST. Doing so convinces us that there is a rational basis for full access to TrueAllele's source code and related documentation for purposes of a Frye reliability analysis.

The troubling FST case study demonstrates a rational basis for independent source-code review of probabilistic DNA programs like TrueAllele. After being subjected to an adversarial audit when ProPublica obtained an order for the release of FST's source code, it was revealed that FST had a problem with a certain calculation that was only learned through the adversarial examination of the source code. Steven M. Bellovin et al., Seeking the Source: Criminal Defendants' Constitutional Right to Source Code, 17 Ohio State Tech. L.J. 1, 38 (2021). The audit discovered that certain "loci were removed from the likelihood ratio calculation" without "notice, either intended or actual, provided to the user of FST," nor any "indication that this behavior [was] intended during [the] examination of FST-related publications and the FST [v]alidation materials."[12] Ibid.; see also Stephanie J. Lacambra et

[12] It is also suggested that this calculation existed in the source code after a validation study had been conducted. Bellovin et al., 17 Ohio State Tech. L.J. at 39.

al., Opening the Black Box: Defendants' Rights to Confront Forensic Software, Champion 28, 30 (May 2018) (providing a snippet of the source code and explaining that "if the sum of frequencies is greater than 0.97, a row in the raceTable is removed").[13] As a result, the software was overestimating the likelihood of guilt. Beyond undocumented calculations, it was discovered that FST exhibited code smells,[14] which suggested that "the program is below normal professional standards and may have other, not yet detected problems" which are "extremely difficult to detect . . . without access to [the] source code." Bellovin et al., 17 Ohio State Tech. L.J. at 39. At oral argument, the Innocence Project pointed out that, like TrueAllele, FST was subject to multiple validation studies but errors were still found in the source code, proving that validation of this type of evidentiary software is not determinative when evaluating computer science reliability.

Likewise, code errors and miscodes were discovered in TrueAllele's competitor STRmix after it had been developed, validated, and used in

---

[13] Available at https://www.eff.org/files/2018/07/30/champion_article_-_lacambra_forensic_software_may_2018_07102018.pdf.

[14] "A code smell is a surface indication that usually corresponds to a deeper problem in the system. In this sense, a smell is not a defect in itself but is a deviation from good coding practices, which can indicate underlying software defects." Ibid. (internal quotation marks omitted).

criminal prosecutions, further showing that errors in source code are not obvious or always timely found. When the source code was reviewed by independent forensic analysts, it was uncovered that the program produced false results in sixty cases.[15] Mr. Adams also reviewed STRmix's code in 2015 and "was able to identify potential issues in STR[m]ix's source code that negatively affected the functioning of the software and could not have been learned from any other source."

Defendant points out that any program's output could potentially be skewed not only by the inadvertent errors routinely found in lengthy code but by the numerous subtle choices made by programming developers regarding how to interpret input data. Defendant asserts, in part by reference to Mr. Adams' declaration, that many of those biases and errors may be conducive to detection only by a full examination and testing of the code and points to the consequential software errors of STRmix and the FST. Indeed, exacerbating

---

[15] 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 (noting that while true that "[t]he DNA likelihood ratios in both the new and original statements appear[ed] to be the same," this still raised serious concerns as to the reliability of such software). As the developer of STRmix stated, "the error had been present since [the version with the erroneous source code's] inception in 2012," nearly three years prior. Ibid.

the danger of inherent bias or error specifically with respect to probabilistic genotyping software is that the likelihood ratio is not conducive to independent calculation or other precise verification, but highly sensitive to modeling assumptions embodied in the code. Defendant surmises that errors of similar magnitude and consequence to those in STRmix and FST may infect TrueAllele's code, noting that the program is likely to return vastly different likelihood ratios for the same physical sample in successive tests without explanation, and that the code has been edited numerous times without any explanation as to whether errors were remedied or any scrutiny as to whether others were inadvertently introduced. Defendant disputes that the validation studies and judicial reliability determinations of other jurisdictions, both of which the judge here found significant, were viable substitutes for source-code review in this case.

As discussed above, many of the amici amplify defendant's argument that full access to the source code is essential to evaluation. The Innocence Project, LAS, and Upturn all concur on that point, with LAS highlighting the discontinued FST program as a cautionary tale, and Upturn warning that a failure to require production would encourage secrecy and erode criminal defendants' constitutional rights. Drs. Heimdahl and Matthews, meanwhile, confirm and reiterate that errors are ubiquitous in software code and strongly

believe that TrueAllele's code likely contains them. Moreover, they discount the validation studies on which the State relies, asserting that none entailed genuinely independent review, and that none involved computer science testing of whether the software operated as intended.

We acknowledge the State, on the other hand, disputes the notion that source-code review is essential to validation, noting that the SWGDAM guidelines require no such review, only testing, such as the sort that uncovered errors in the STRmix software. To be sure, the State is correct that the mechanism for evaluation contemplated in the SWGDAM guidelines is testing rather than source-code review, SWGDAM Guidelines, at 4-11, and that errors found in the STRmix program had been detected first through testing rather than visual examination of the code, Duncan A. Taylor et al., Commentary, A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution, 8 Frontiers in Genetics art. 33, at 1 (2017).[16] But production and review of the code for the since-discontinued FST program proved crucial to identification of significant errors, albeit not before compromised test results had already been used in many prosecutions. Lauren Kirchner, Doubts and DNA Evidence, N.Y. Times, Sept. 5, 2017, at A1. We cannot ignore these

[16] Available at https://www.frontiersin.org/articles/10.3389/fgene.2017.00033/full.

facts when evaluating whether there exists a rational basis for access to the proprietary information here.

The parties have cited expert testimony, authoritative scientific and legal writings, and judicial opinions that were generated before and after the STRmix and FST's software errors became public. This information bolsters our conclusion that there is a rational basis for the discovery. The State, of course, urged the judge to rely on that body of information to conclude there was no such basis. The testimony predominantly cited was that of Dr. Perlin, the scientific writings were mainly from Dr. Perlin (together with his then current or former employees),[17] and the judicial opinions referred to that testimony and those scientific writings. But none of this information explicitly deals with whether TrueAllele's source code itself correctly implements the intended methods, as PCAST emphasized. PCAST Report, at 79.

As to expert testimony, Mr. Adams submitted a twenty-four-page declaration in which he asserted a need for production of the source code and related documentation. In his declaration, he addressed: his qualifications; an overview of his engagement, including whether TrueAllele "has been demonstrated to be in accordance with software engineering standards and principles"; the uncertainty in DNA mixture interpretation; a background on

[17] Many of the studies explicitly acknowledge Dr. Perlin's conflict of interest.

software engineering; details as to V&V, including definitions in the field of software engineering, system integrity, methodologies, code reviews, software testing, documentation, independence, and re-validation and performance checks; software engineering failures; materials relevant for review; requirement specifications, including design descriptions, source code, build instructions and dependencies, executable versions, tests, issue/bug tracking; user manuals, V&V, qualification and user testing, and miscellaneous processes; comment on Cybergenetics' proposed terms of inspection and nondisclosure agreement; and preferred terms for inspection. He also produced a detailed appendix to his declaration including documentation as to the software development process, the IEEE "risk-based, integrity-level scheme."

Unlike in Ghigliotty, where there was "nothing concrete in the record" to support access to the algorithms the defendant sought for the BULLETTRAX algorithms at issue there, the opposite is true here. 463 N.J. Super. at 384. In Ghigliotty, we concluded the defendant was "required to make a more definitive showing of his need for th[e] material." Id. 384-85. Here, defendant did that with the proffered expert testimony supporting the claim for disclosure.

As to the validation studies and peer-reviewed articles issued during this timeframe, we have scrutinized them and make the following observations about their application. Since 2009, thirty-six validation studies have been conducted by Cybergenetics, law enforcement crime labs, or both, intending to establish the reliability of TrueAllele. These studies have utilized TrueAllele on both laboratory-generated and casework DNA samples and have tested TrueAllele to determine how it handles mixtures of varying DNA compositions and weights.

Seven of the thirty-six studies have been published in peer-reviewed journals, the first of which was published in 2009. The peer-review process entails a review for accuracy and quality of a scientific paper, in which a scientist describes his or her research and conclusions, and it is either accepted or rejected by two anonymous members of the relevant scientific community. A "laboratory-generated" validation study uses data that has been synthesized in a DNA laboratory and is of a known genotype composition. Four published papers are of this type.[18] A "casework" validation study uses DNA data

[18] See Mark W. Perlin & Alexander Sinelnikov, An Information Gap in DNA Evidence Interpretation, 4 PLoS ONE e8327 (2009) [Information Gap]; Jack Ballantyne, Erin K. Hanson, Mark W. Perlin, DNA Mixture Genotyping by Probabilistic Computer Interpretation of Binomially-Sampled Laser Captured Cell Populations: Combining Quantitative Data for Greater Identification Information, 53 Sci. & Just. 103 (2013); Mark W. Perlin et al., TrueAllele

exhibiting real-world issues developed by a crime laboratory in the course of their usual casework activity. Three published papers are of this type.[19]

Notably here, six of the seven peer-reviewed publications were authored by Dr. Perlin himself. The one study not authored by Dr. Perlin does note that he provided professional guidance.[20] PCAST explicitly noted the software developer's participation in such studies as an impediment to reliable validation, noting that, "[w]hile it is completely appropriate for method developers to evaluate their own methods, establishing scientific validity also requires scientific evaluation by other scientific groups that did not develop the method." PCAST Report, at 80. That was not done here, where Dr. Perlin, a developer with a vested interest in the program's scientific acceptance, was

---

(continued)
Genotype Identification on DNA Mixtures Containing Up to Five Unknown Contributors, 60 J. Forensic Scis. 857 (2015); Susan A. Greenspoon et al., Establishing the Limits of TrueAllele Casework: A Validation Study, 60 J. Forensic Scis. 1263 (2015) [Establishing the Limits of TrueAllele Casework].

[19] See Mark W. Perlin et al., Validating TrueAllele DNA Mixture Interpretation, 56 J. Forensic Scis. 1430 (2011) [hereinafter Validating TrueAllele]; Mark W. Perlin et al., New York State TrueAllele Casework Validation Study, 58 J. Forensic Scis. 1458 (2013); Mark W. Perlin et al., TrueAllele Casework on Virginia DNA Mixture Evidence: Computer and Manual Interpretation in 72 Reported Criminal Cases, 9 PLoS ONE e92837 (2014).

[20] See Establishing the Limits of TrueAllele Casework, 60 J. Forensics Scis. at 1276.

directly involved. Law enforcement agencies, which also sometimes participated, likewise share an interest in the continued viability of the program. In the end, for purposes of reliability in a criminal context, it stands to reason that such an evaluation should be performed by an expert working on behalf of someone in defendant's shoes, with full access to the tools required for evaluation. See United States v. Gissantaner, 417 F. Supp. 3d 857, 880 (W.D. Mich. 2019) (addressing Daubert and the admissibility of STRmix and noting that "studies and articles . . . have determined that review of probabilistic genotyping software, independent of that of the developers, is critical for an assessment of its reliability with respect to use in the courts").

Moreover, despite Dr. Perlin's and the State's insistence that the TrueAllele program affords analysts a tool for objective analysis, it does not inexorably follow that that analysis is reliable. We consider the concept of "programmer blindless" a common pitfall of non-independent review. "Just as writers are often bad at proofreading their own text, programmers are bad at reading their own code. . . . It is often the case that peers are not truly independent reviewers because programmers often have similar training—and thus tend to make the same mistakes." Bellovin et al., 17 Ohio State Tech. L.J. at 32. Further, even if the program's operation is objective, numerous judgments regarding the appropriate interpretation of data are already baked

into the source code, and may not be conducive to detection, comprehension, and analysis except by review of that source code. See Katherine Kwong, The Algorithm Says You Did It: The Use of Black Box Algorithms to Analyze Complex DNA Evidence, 31 Harv. J. L. & Tech. 275, 291 (2017) (noting that "[d]ifferent programs incorporate subtly different choices into their algorithms about how to interpret data, which can yield different results when analyzing the exact same complex mixture," and that identification of consequent biases requires a "look at the software"). That is particularly so for a probabilistic genotyping program, whose output is not conducive to independent calculation or otherwise verifiable with precision like other analyses. See Christopher D. Steele & David J. Balding, Statistical Evaluation of Forensic DNA Profile Evidence, 1 Ann. Rev. Stat. & Its Application 361, 380 (2014) (explaining that a likelihood ratio "expresses our uncertainty about an unknown event and depends on modeling assumptions that cannot be precisely verified in the context of noisy . . . data").

As to judicial opinions, we note that eighteen courts have rejected calls to allow independent evaluation of TrueAllele's source code, many of which did so after the issues with STRmix and FST came to light. But critically, prior determinations of reliability in other jurisdictions entailed no scrutiny of

computer science or source code.[21] Instead, the courts depended in large part on Dr. Perlin's own testimony and the existing validation studies which, even if diligently conducted and sound, were not truly independent and did not even evaluate the source code.

The first court to address the question of admissibility was Commonwealth v. Foley, 38 A.3d 882, 889-90 (Pa. Super. Ct. 2012), where the court accepted Dr. Perlin's assertion that validation studies are the best tests of the reliability of source codes. The court reasoned that "scientists can validate the reliability of a computerized process even if the 'source code' underlying that process is not available to the public," emphasizing that making the source code available would have market consequences. Id. at 889. The court reasoned also that TrueAllele "ha[d] been tested and validated in peer-reviewed studies," citing two studies that had been "published in peer-reviewed journals" and thus "reviewed by other scholars in the field." Id. at 889-90. At that time, in 2012, TrueAllele had been the subject of two studies, one laboratory-generated validation study, conducted and authored by Dr.

---

[21] We emphasize that when it comes to balancing the rights of the accused against other interests, including the intellectual property rights of private companies, New Jersey errs on the side of disclosure. Chun taught us that. See generally 194 N.J. at 68-70.

Perlin himself,[22] and one casework validation study, which was also co-authored by Dr. Perlin.[23] The court made no mention of the fact that Dr. Perlin was involved in both the validation studies conducted up to that point. Subsequent courts have placed great emphasis on the observation made in Foley, without further scrutiny, creating an authority "house of cards." See, e.g., People v. Superior Court (Chubbs), No. B258569, 2015 WL 139069, at *8 (Cal. App. Ct. Jan. 9, 2015); State v. Daniels, No. 2015CF009320AMB (Fla. Cir. Ct. Oct. 31, 2018) (slip op. at 3); State v. Wakefield, 9 N.Y.S.3d 540, 541 (Sup. Ct. 2015); State v. Shaw, No. CR-13-575691 (Ohio C.P. Ct. Cuyahoga Cnty. Oct. 10, 2014) (slip op. at 23); Commonwealth v. Knight, No. 379 WDA 2017, 2017 WL 5951725, at *6 (Pa. Super. Ct. Nov. 29, 2017); State v.

---

[22] Dr. Perlin and his co-author in Information Gap, 4 PLoS One e8327, at 1-2, compared the effectiveness of newer quantitative computer-based methods, such as TrueAllele, with that of existing qualitative manual methods in extracting information from samples with low levels of genetic material. They found an "information gap between the two approaches," in that the newer quantitative methods could "extend meaningful interpretation" to samples with far less material. Id. at 2.

[23] Dr. Perlin and his co-authors in Validating TrueAllele, 65 J. Forensic Scis. at 1443, concluded that the use of genetic calculators like TrueAllele could improve DNA mixture interpretation in several ways. Ibid. A computer could process information faster than a human analyst, thereby reducing DNA case backlogs. Ibid. Genetic calculators could also extract more DNA information from lower template samples. Ibid. And the use of computers would increase the objectivity of the analysis, given the concern that prematurely exposing a human analyst to a suspect's profile could introduce observer bias. Ibid.

Watkins, No. 2017-C-1811 (Tenn. Crim. Ct. Davidson Cnty. Dec. 17, 2018) (slip op. at 13-14).[24] Published out-of-state judicial decisions, although persuasive rather than binding, carry great weight, especially after they are cited by other courts. A long line of decisions uniformly in favor of a legal proposition suggests that a legal proposition is generally accepted. We are mindful, however, that in science, the repetition of authority does not automatically establish reliability for purposes of a Frye hearing. The cases identified by the State include a laundry list of admissibility rulings, but to reiterate, none consider whether the TrueAllele source code itself correctly implements its methods, which can only be tested in the manner defendant and amici advocate for here.

We need not risk the same result. Our Supreme Court deemed source-code review of sufficient import to a reliability determination in Chun, 194 N.J. at 68-70, to order production, and we clearly contemplated the same in Ghigliotty, 463 N.J. Super. at 384-85, as to the algorithms at issue there. Here, Mr. Adams explained with particularity his need for full access to the code, not simply for visual examination, but for execution and testing, and the terms

[24] The State also provided this court with an extended list of admissibility rulings which may be found at Cybergenetics' website. See TrueAllele Admissibility, Cybergenetics, https://cybgen.com/information/admissibility/page.shtml (last visited Jan. 27, 2021).

imposed in Cybergenetics' NDA, such as surveillance, time limits, and restrictions on note-taking and communication, would impede that review. Indeed, Dr. Perlin's own estimate that it would take an individual more than eight years to decipher the code by simple visual inspection belies the State's position that the limited access already offered would be adequate for meaningful review.

In light of the concerns that arise when examining the "black box" validation studies, the out-of-state judicial opinions and orders that have accepted TrueAllele's reliability without source code examination, and errors found in the source codes of the breathalyzer in Chun, FST, and STRmix, judges should examine the reliability of such software with healthy skepticism. Even if the DNA science underpinning probabilistic genotyping analysis has been proven scientifically valid, computer software such as TrueAllele must also properly implement that analysis in its source code; the source code must do as Cybergenetics says it does. We do not suggest that errors found in the source code of other probabilistic genotyping software necessarily means that such errors are present in TrueAllele's source code, but we must ensure that the constitutional rights of criminal defendants are protected by permitting an adversarial review of TrueAllele's source code to ensure that such errors do not

also exist there as well. We therefore conclude that there is a rational basis under Frye for production.

(ii)

The specificity of the information sought

In his discovery motion, defendant specifically identified the proprietary information sought. In regard to the validation studies, defendant requested discovery of all materials generated, including "[a]ll records and electronic data used as 'input' to the TrueAllele system and the software parameters used to analyze this data," "[a]ll records and electronic data generated by the TrueAllele system and/or laboratory personnel during the course of the study," "[a]ny analyses . . . including bench notes, measurements, statistics, memos, summaries, conclusions, tables, graphics, and any resulting publications, presentations, and reports," "[a]ll communication relating to the design and results of the study, both within and external to the laboratory," "[a]ll records of unexpected results, including false positives (false inclusions), false negatives (false exclusions), and the conditions under which the unexpected results were granted," "[a]ll records of software glitches, crashes, bugs, or errors encountered during the study," and "[s]oftware version numbers of the components of the TrueAllele[] system used for the study."

Defendant further requested "[s]ource code for the version(s) of the TrueAllele system used in the instant case," including "all software dependencies such as third-party code libraries, toolboxes, plug-ins, and frameworks," and "[s]oftware engineering and development materials describing the development, deployment, and maintenance of the version(s) of the TrueAllele software system used in the instant case . . . , including the software engineering documents recommended by organizations such as the [IEEE] or the Internal Organization for Standardization (ISO)."

Defendant also specifically requested "[c]ommunication logs and records relating to TrueAllele testing, analysis, and reporting in the instant case, including requests for technical or procedural assistance, bug/crash reports, corrective actions, and software updates" along with "[d]ocumentation of corrective actions for discrepancies and errors."

Finally defendant requested the forensic casefile generated by the New Jersey State Forensic Laboratory in the matter including: "notes, documents, and data resulting from each phase of testing and analysis," "documentation related to the evidence collection and examination by the lab, serological testing, DNA extraction, quantitation, amplification, electrophoresis, analysis, and comparison of the samples," and "all positive and negative controls, allelic ladders, and electronic raw data."

Defendant provided the necessary information to justify his particularized need for the information requested and limited the scope of his request to that required for an independent analysis and review in this case. The information requested ensures that TrueAllele's source code operates as intended and that any changes to the source code have not negatively affected the intended operation of the program.

(iii)

Safeguarding the company's intellectual property—protective order

Entering a protective order for use as part of the Frye hearing will accommodate safeguarding the proprietary information while simultaneously protecting the interests of defendant's liberty and justice. On remand, we direct the judge to issue a protective order that accomplishes these objectives. We leave to the discretion of the judge the details of that task. Two points about that: the judge should retain jurisdiction to enforce the order should that become necessary; and the judge should follow these remarks.

The parties recognize that the entry of a protective order is necessary since they invested "[e]xtensive communications" attempting the negotiate one for the judge to enter. As counsel acknowledged before us, the State made

several concessions but "two key areas of disagreement remain."[25] The two areas pertained to liquidated damages for breach of the order, and the terms of the inspection itself. We will generally address both.

First, as to the damages, the State insisted that there be a $1,000,000 automatic civil liability "in the event that the proprietary materials are improperly handled, negligently or otherwise." Moreover, the State required—on this automatic liability term—that the defense submit to jurisdiction in Pennsylvania and that the defense obtain liability insurance with $3,000,000 in coverage.

But, as the Innocence Project points out, a model protective order from the Northern District of California, whose docket includes among the most complex and financially consequential patent cases in the world, includes no provision for financial liability. U.S. Dist. Ct. for the N.D. of Cal., Model Protective Order for Litigation Involving Patents (Model Protective Order).[26] We have not found—and the parties have not provided—any case authorizing

---

[25] For example, an assistant prosecutor wrote in a February 5, 2020 letter to the judge that the State agreed to a court-ordered protective order, rather than an NDA; the State removed prerequisites to expert qualifications prior to review; the requirement that the defense expert's notes be turned over to Cybergenetics; the imposition of significant fees for inspections; and participation of Cybergenetics' attorneys during the inspection.

[26] Available at https://www.cand.uscourts.gov/forms/model-protective-orders/ (last visited Jan. 27, 2020).

disclosure of source code and related proprietary information under a protective order with the restrictions as rigid as Cybergenetics' terms, particularly as to liquidated automatic financial liability for breach of a protective order. Indeed, defendant produced the reasonable protective order issued in Illinois governing access to the source code and related documents by STRmix, and there is no such provision.

Acknowledging that there must be teeth to the protective order, in a proposed order for the judge's consideration, defendant reasonably proposed the following sanctions for breach: "Any person who willfully violates the terms of this Order is subject to civil and criminal sanctions, in addition to any other remedy or proceeding allowed by law." Defendant did not specifically identify the civil and criminal sanctions, but as counsel for ACDL-NJ pointed out at oral argument, such sanctions could generally include license suspension, disciplinary actions, and civil penalties, just to mention a few. Civil and criminal contempt charges for violating a court order are also a potential consequence for breach. See In re Adoption of N.J.A.C. 5:96 & 5:97, 221 N.J. 1, 17-18 (2015) (noting that Rule 1:10-3 provides relief to a litigant for another party's failure to abide by a court order); State v. McCray, 458 N.J. Super. 473, 493 (App. Div. 2019) (noting that "[t]he goal of the criminal contempt statute[, N.J.S.A. 2C:29-9(a),] is to promote compliance with judicial

orders by punishing those who purposely or knowingly fail to comply with those orders").

Second, as to the terms of the inspection, the State offered to host defense counsel and their experts at the prosecutor's office, which obviates the need for travel, but then prohibited meaningful inspection by permitting only handwritten notes of 170,000 lines of code. According to Dr. Perlin, comprehending the code through such an austere visual inspection would likely take more than eight years. Moreover, the State required the inspection to be supervised and would not allow photographs or copying of any material.

But, as the Innocence Project points out, the model protective order from the Northern District of California includes provisions explicitly permitting certain personnel other than the experts themselves access to the sensitive information, Model Protective Order §§ 7.2, 7.3, and allows the printing of portions of the source code for purposes of analysis, id. § 9(d). Defendant's proposed order, on the other hand, provides reasonable protections, including a prohibition on disclosure to any individual with "any direct or indirect commercial or employment interest in competing software products." Although a requirement that all notes be handwritten may be included to prevent unauthorized copying and disclosure of source code, such a requirement could be impractical given the form and syntax of source code.

Such a requirement may be considered "burdensome in the extreme" because "[m]odern computer source code was never intended to be handwritten even by the original programmer." Lydia Pallas Loren & Andy Johnson-Laird, Computer Software-Related Litigation: Discovery and the Overly-Protective Order, 6 Fed. Cts. L. Rev. 1, 47 (2012).

As defendant and amici point out, jurisdictions across the country often authorize disclosure of source code in civil litigation to one extent or another on an adequate showing, subject only to a court-issued protective order. See, e.g., WeRide Corp. v. Kun Huang, 379 F. Supp. 3d 834, 854 (N.D. Cal. 2019); Northrop v. Inventive Commc'ns, L.L.C., 199 F.R.D. 334, 335-36 (D. Neb. 2000); Jagex Ltd. v. Impulse Software, 273 F.R.D. 357, 358 (D. Mass. 1997); Dynamic Microprocessor Assocs. v. EKD Comput. Sales, 919 F. Supp. 101, 106 (E.D.N.Y. 1996). The provisions entailed in each order tend to reflect a balance of the rights of the interested parties in light of the circumstances that are attendant to each case.

(iv)

Any other relevant factors unique to the facts of the case

Unique to this case is the type of software that is proposed to be used. Probabilistic genotyping differs from traditional methods of DNA analysis in the resulting likelihood ratio that it provides. Rather than providing a result

which can be verified against a true value, such as a breathalyzer being compared to a blood draw to ascertain the true blood alcohol content and whether the breathalyzer is within an acceptable margin of error, a likelihood ratio has no precise, independently ascertainable value with which to compare to ensure that the software is providing an acceptable estimation. As Christopher D. Steele and David J. Balding explain,

> [l]aboratory procedures to measure a physical quantity such as a concentration can be validated by showing that the measured concentration lies within an acceptable range of error relative to the true concentration. Such validation is infeasible for software aimed at computing a [likelihood ratio] because it has no underlying true value (no equivalent to a true concentration exists). The [likelihood ratio] expresses our uncertainty about an unknown event and depends on modeling assumptions that cannot be precisely verified in the context of noisy [crime scene profile] data.
>
> [Steele & Balding, 1 Ann. Rev. Stat. & Its Application at 380 (fourth alteration in original).]

Additionally, Mr. Adams noted that "[s]ince the likelihood calculations are dependent on the statistical models . . . underlying the probabilistic software, any software behaviors affecting the models will necessarily impact the calculated likelihoods and ultimately the reported likelihood ratio." Because probabilistic genotyping analysis cannot be tested to ensure that is reaching a near-correct result by comparing it to a true value, the closest substitute is to

examine the way in which the source code is written to ensure that it functions as the science underpinning probabilistic genotyping necessitates. This is particularly important when even slight changes in the statistical models converted into source code can affect the resulting likelihood ratio. In this way, STRmix and FST serve as important cautionary tales.

Additionally, Drs. Heimdahl and Matthews note that TrueAllele's software integrates multiple scientific disciplines, therefore requiring cross-disciplinary validation to determine reliability. During oral argument, they informed us that each discipline will validate a program under different standards. In particular, V&V in the computer science field cannot be achieved without a thorough examination of the source code which translates validated probabilistic genotyping into executable software. See Natalie Ram, Innovating Criminal Justice, 112 Nw. U. L. Rev. 659, 688 (2018) (noting that "[c]omputer scientists . . . have shown that black-box evaluation of systems is the least powerful of a set of available methods for understanding and verifying system behavior. More powerful and effective is white-box testing, in which the person doing a test can see the system's code and uses that knowledge to more effectively search for bugs" (alteration and omission in original) (internal citations and quotation marks omitted)). So, while TrueAllele may be generally accepted in the field of DNA forensics as

methodologically sound, such validation may be too narrow, thereby making access to the source code even more important to test whether Dr. Perlin's testimony has gained general acceptance in the computer science community to which it also belongs.

VI.

As technology proliferates, so does its use in criminal prosecutions. Courts must endeavor to understand new technology—here, probabilistic genotyping—and allow the defense a meaningful opportunity to examine it. Without scrutinizing its software's source code—a human-made set of instructions that may contain bugs, glitches, and defects—in the context of an adversarial system, no finding that it properly implements the underlying science could realistically be made. Consequently, affording meaningful examination of the source code, which compels the critical independent analysis necessary for a judge to make a threshold determination as to reliability at a Frye hearing, is imperative.

In summary, defendant articulated a particularized need for the proprietary source code and related information for use at the Frye hearing by (1) demonstrating a rational basis for ordering the State to attempt to produce it, including through expert testimony supporting the claim for disclosure; (2) providing specificity for the information sought; (3) showing through

examples from other jurisdictions that the company's intellectual property can be safeguarded by a protective order; and (4) demonstrating that source-code review is particularly crucial to evaluating the unique technology at issue here.

Anything less than full access contravenes fundamental principles of fairness, which indubitably compromises a defendant's right to present a complete defense.

Reversed and remanded for further proceedings. On remand, the judge is directed to compel the discovery of TrueAllele's source code and related materials pursuant to an appropriate protective order, then complete his gatekeeping function at the continued Frye hearing. We do not retain jurisdiction.