STATE OF NEW JERSEY, Plaintiff-Respondent v. **COREY PICKETT** Defendant and Movant-Appellant	SUPERIOR COURT OF NEW JERSEY APPELLATE DIVISION DOCKET NO. **A-4207-19T2** CRIMINAL ACTION On Leave Granted to Appeal an Interlocutory Order of the Superior Court of New Jersey, Law Division, Hudson County. Indictment No. 17-07-470-I Sat Below: Hon. Patrick J. Arre, J.S.C.

BRIEF OF *AMICUS CURIAE* THE INNOCENCE PROJECT IN SUPPORT OF MOVANT-APPELLANT

Michael A. Albert*
Anant K. Saraswat*
WOLF, GREENFIELD & SACKS, P.C.
600 Atlantic Avenue
Boston, MA 02210
Tel: 617.646.8000
Fax: 617.646.8646
malbert@wolfgreenfield.com
asaraswat@wolfgreenfield.com

Dana M. Delger*
Innocence Project Inc.
40 Worth St. Ste. 701
New York, NY 10013
Tel: 212-364-5964
ddelger@innocenceproject.org

Joseph M. Mazraani
(Attorney #023782004)
Mazraani & Liguori, LLP
57 Paterson Street
New Brunswick, NJ 08901
Phone: (732) 951-3100
Fax: (732) 951-3101
jmazraani@mllawnj.com

Amicus on Behalf of Movant-Appellant

*Admitted Pro Hac Vice

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

RULES

PRELIMINARY STATEMENT

DNA can provide powerful evidence of guilt or innocence. If properly handled, analyzed, and interpreted, it can often tie evidence to a specific individual or source with a high degree of certainty. But for that same reason, DNA evidence can also give the prosecution's case an unwarranted imprimatur of scientific certainty. Because of this power, and because DNA analysis often uses complex computer software, the defense must have a full and fair opportunity to test the accuracy of DNA software when it is used, in order for the adversarial testing process to be meaningful and to prevent wrongful conviction. Indeed, nearly half of DNA exonerations involve faulty forensic evidence.[1]

TrueAllele Casework ("TrueAllele") is relatively new software that purports to use probabilistic genotyping to "turn[] inconclusive data into a match statistic strong enough for court." *TrueAllele Forensic E-Brochure* ("*E-Brochure*") at 4.[2] In other words, TrueAllele takes admittedly "inconclusive" data and – in a method entirely unknown and untested by either the State or the defense – purports to create an untestable oracle of innocence or guilt. For "inconclusive" data to suddenly gain the aura of scientific certainty in an unverifiable manner should hardly reassure anyone – least of all courts charged with

[1] *See* https://www.innocenceproject.org/overturning-wrongful-convictions-involving-flawed-forensics/.

[2] https://www.cybgen.com/products/casework/forensic_e-brochure.pdf.

ensuring fundamental fairness and subjecting evidence to "the crucible of meaningful adversarial testing." *U.S. v. Cronic*, 466 U.S. 648, 656-57 (1984). The Constitution requires that Mr. Pickett be allowed to look behind the curtain and learn how the software turns the "inconclusive data" into what it claims is a "match statistic."[3] Without such access, it is impossible to determine whether the "match statistics" are accurate or resulted from programming error, whether deliberate or accidental. Indeed, doubts about TrueAllele's accuracy are plausible — a competing program, STRmix, that performs the same type of analysis as TrueAllele, was found to have coding errors that impacted the data presented in court. David Murray, *Queensland Authorities Confirm "Miscode" Affects DNA Evidence in Criminal Cases*, Courier Mail (Mar. 20, 2015).[4]

Let there be no mistake about the interests at issue here. Cybergenetics is not some bystander who inadvertently or incidentally possesses information material to a criminal matter; rather, Cybergenetics' entire purpose in creating and selling TrueAllele is to create evidence for use in criminal proceedings. *See* Cybergenetics, *TrueAllele Forensic Brochure* at 2 ("*Forensic Brochure*")[5] ("TrueAllele Casework produces reliable

---

[3] TrueAllele's "match statistic" purports to show the probability that a DNA sample contains a given person's DNA.

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

[5] https://www.cybgen.com/solutions/brochures/lab_brochure.pdf.

answers on previously unsolvable DNA evidence."). Yet it effectively refuses to allow a defense expert to test that proposition by limiting access to its code, and conditions that access on onerous conditions that cannot properly be required as the price of exercising a fundamental constitutional right. Indeed, the terms under which Cybergenetics would allow the defense to examine the source code are more restrictive than those of protective orders in civil litigation — where money, as opposed to a man's freedom, is at stake. The law cannot accord less weight to a criminal defendant's constitutional rights than to a commercial litigant's right to obtain discovery.

The Court should either order disclosure of the TrueAllele source code to the defense, subject at most to a reasonable protective order, or hold that absent such disclosure the State cannot meet its burden to show that the TrueAllele analysis is admissible.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

Amicus accepts and incorporates the statement of facts and procedural history contained within Defendant-Movant's briefing.

BACKGROUND REGARDING TRUEALLELE SOFTWARE

I. TrueAllele Software

The TrueAllele software performs "probabilistic genotyping" of DNA samples to "interpret" the DNA data.[6] A YouTube tutorial by Cybergenetics outlines the TrueAllele workflow.[7] First, the

[6] *See Forensic Brochure* at 4.

[7] Cybergenetics, TrueAllele Process Overview ("*TrueAllele Overview*"): https://www.youtube.com/watch?v=OU29b5sW88Y.

data generated by the genetic analyzer is sent to Cybergenetics for interpretation. *Id.* at 0:26-0:33 The TrueAllele source code then assesses the quality of the data. *Id.* at 1:20-1:45. An analyst then inputs various "parameters" – assumptions – that are used in the TrueAllele analysis. *E.g.*, *id.* at 2:25-2:32. Without TrueAllele's source code, there is no way to know how the analyst's assumptions interact with the raw data and TrueAllele's rules to generate results.

TrueAllele then applies additional rules, separate from those used in the preliminary analysis. The result is a "match statistic" that Cybergenetics invites the analyst to simply "paste into their case report." *Id.* at 8:35-8:50. In other words, TrueAllele's source code conceals substantive choices that are insulated from adversarial examination — choices, for example, about what "data issues" are worthy of being reported during the preliminary quality analysis, or how the assumptions and data are merged to generate a match statistic. Defense counsel is given no opportunity to identify potential data errors at any step along the way, be they inherent to the algorithm or simply arising from erroneous coding or input.

Cybergenetics' web site touts TrueAllele as "enabl[ing] analysts to produce accurate results on previously unsolvable DNA evidence."[8] Because these are software-based tools run on a computer, attempting to perform a similar technique by hand

[8] *See* Cybergenetics, *CaseWork* (as of October 27, 2020): https://www.cybgen.com/products/casework.shtml.

could take decades. (Def. Initial Br. ("Db"), 19 n.7) Yet precisely how (or indeed whether) the software actually implements its stated techniques accurately remains an open question. The Court cannot simply assume that this black box contains an oracle accurate enough to incarcerate a defendant.

II. Restrictions on Defense Access

Cybergenetics limits defense access to the TrueAllele source code and documentation by conditioning access on signing a non-disclosure agreement ("NDA," *see* DA 133) whose conditions would deter most reasonable counsel and experts from signing it, thus unconstitutionally burdening fundamental rights. (*See* Appendix on Behalf of Defendant-Movant ("DA") 140.) The NDA obligates the recipient of information not to "decompile, disassemble, reproduce, redesign, or reverse engineer" it (*see* DA 135 § 4(iv)), and to keep it confidential unless "legally compelled" to disclose it by a court (DA 136 § 7). The NDA subjects the recipient of Cybergenetics's information to "automatic liability in the amount of $1,000,000" for any breach (DA 289), along with costs and attorneys' fees, and waives the right to a jury trial in certain instances. (DA 137 § 12(e)). The NDA is governed by Ohio law, and requires consent to jurisdiction and venue in that forum. (*Id.* at § 12(g)).

Cybergenetics also restricts how the defense can access the source code. Cybergenetics' source code is only available on a stand-alone computer in a room supervised by a representative of Cybergenetics. (*See* DA 140.) Anyone inspecting the hundreds of

thousands of lines of code cannot bring in any device with photographic or recording capability and can only take hand-written notes about the code. (*Id.*; *see also* DA 289.) There is no provision in Cybergenetics' access terms to enable the printing of any portion of the source code.

LEGAL STANDARD

"[T]he Constitution guarantees criminal defendants a meaningful opportunity to present a complete defense." *Crane v. Kentucky*, 476 U.S. 683, 690 (1986); *see also State v. Garron*, 177 N.J. 147, 168 (2003) (applying *Crane* to New Jersey Constitution). The defense has a fair opportunity to defend only if it is permitted to subject the State's evidence to "the crucible of meaningful adversarial testing." *Cronic*, 466 U.S. at 656; *Michigan v. Bryant*, 562 U.S. 344, 370 n.13 (2011).

Adversarial testing and confrontation are particularly important where forensic analysis is used against a defendant. The danger from invalid scientific testimony — an acute concern given the number of wrongful convictions resulting from its use — is at its highest in cases where the prosecution relies almost entirely on expert opinions to establish the identity of the alleged perpetrator. *See, e.g.*, *Elcock v. Kmart Corp.*, 233 F.3d 734, 756 n.13 (3d Cir. 2000) (noting that "the opinion of a witness impressed by the court with the label of 'expert' may carry a great deal of weight with a lay jury" and that "[p]ermitting such a witness to offer an opinion unsupported by a sufficient factual foundation would significantly increase the

risk of misleading the jury"). "'Serious deficiencies have been found in the forensic evidence used in criminal trials.'" *Hinton v. Alabama*, 571 U.S. 263, 276 (2014) (quoting *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 319 (2009) (noting "[p]rosecution experts, of course, can sometimes make mistakes")). As a safeguard, "[t]he Constitution guarantees" confrontation as a way to "to challenge or verify the results of a forensic test." *Melendez-Diaz*, 557 U.S. at 318.

The Sixth Amendment's Compulsory Process Clause likewise protects the right to meaningful access to exculpatory evidence. As the Supreme Court has explained, "[t]he ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts." *United States v. Nixon*, 418 U.S. 683, 709 (1974). Accordingly, "[t]o ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the production of evidence needed . . . by the defense." *Id.* The right to compulsory process applies to the production of documentary evidence. *See, e.g., id.* at 688, 713. Under New Jersey law, the "broad governing court rule" in criminal matters is that an indicted defendant "has a right to automatic and broad discovery of the evidence the State has gathered in support of its charges." *State v. Scoles*, 214 N.J. 236, 252 (2013).

ARGUMENT

TrueAllele's analysis is likely to be crucial to the prosecution's case against Mr. Pickett, and so to have a

meaningful defense, he must have a meaningful opportunity to challenge the accuracy of TrueAllele's results. This, in turn, requires access to the source code and validation data, to determine if the software is programmed correctly, and to the user documentation, to determine whether the prosecution's experts used the software correctly ***in his case***. By way of analogy, just as the defense has the right to investigate and examine whether there was a processing error in the "chain of custody" when an item of evidence is handed off from a detective to a lab technician, Mr. Pickett likewise has the right to examine whether a processing error crept into one or more of the billions of calculations performed on the DNA samples as they wended their way through the TrueAllele software. Production of the source code for independent defense analysis is the only way to meaningfully assess it.

The solution that the prosecution advocates instead – requiring defense counsel to accept Cybergenetics' onerous NDA – would allow a private company's business interests to dictate whether, and upon what terms, a defendant can exercise his constitutional protections. Under Cybergenetics' NDA, defense counsel cannot examine the source code and other relevant information without significant liability exposure, including attorneys' fees, in a remote jurisdiction. And if the defense did discover errors in the source code, the NDA would still severely restrict their ability to present this evidence in court. These terms effectively deprive Mr. Pickett of the

meaningful opportunity to present a complete defense solely for the sake of protecting Cybergenetics' commercial interests.

While Mr. Pickett would be entitled to this information regardless of its provenance, Cybergenetics is not a bystander with only incidental or accidental involvement in the criminal justice system or in this case. Rather, TrueAllele is a "machine[] built for criminal accusation," (Andrea Roth, *Machine Testimony*, 126 Yale L. J. 1972, 2043 (May 2017)), designed – and advertised – specifically for use by prosecutors. Having chosen to engage in the criminal justice system, Cybergenetics is obliged to play by the system's rules, which includes the protection of Mr. Pickett's constitutional rights through meaningful access to the "machine." If Cybergenetics is unwilling to do so, its product cannot be used in prosecutions.

The concern about the possibility of errors in the source code is, moreover, well-founded. Such errors are frequent, notwithstanding good-faith efforts by programmers. And a software error could lead to erroneous testimony by the prosecution's expert. Under normal circumstances, the way to expose a dishonest, incompetent, or simply mistaken expert is cross-examination. *See Hinton*, 571 U.S. at 275-76. But without meaningful access to the source code, the defense's ability to cross-examine the prosecution's experts is illusory, as is the defense's ability to present rebuttal testimony from its own experts. For example, if the code contained a bug that returned an incriminating "likelihood ratio" for any defendant whose last

name begins with "P," Mr. Pickett would have no way of knowing that fact, or using it to challenge erroneous expert testimony. In reality, of course, errors are likely to be far more subtle than pointing to defendants whose initial is "P," but the lack of meaningful access would provide no opportunity to correct even such glaring errors. Moreover, even if the software were error-free, Mr. Pickett would still be entitled to explore whether the prosecution's experts ***used*** it properly, which requires access to user the manuals and other documentation showing how it is supposed to be used.

I. Examining How the Source Code Actually Works Is Necessary

A. TrueAllele Is Likely to Have Software Bugs

Source code is written by people, and people make mistakes. Bugs in source code are commonplace, impacting the reliability of underlying calculations. Such errors — often caused by mere oversight, not necessarily mischief, bias or self-interest — can plague even multi-billion-dollar technologies. Forensic source code is not immune from such errors, and defense access to such code has revealed critical errors. *In re Source Code*, 816 N.W.2d 525, 528, 543 (Minn. 2012) (affirming finding, after defense access, that source code contained errors impacting the reliability of a breath alcohol testing device); *State v. Chun*, 194 N.J. 54, 64-65, 68-69 (2008) (finding, after defense access, errors in source code for prosecution product).

Genotyping software in particular has been found error-prone. Source code errors impacting the reliability of STRmix,

a competitor to TrueAllele, materially altered match statistics in DNA mixture analysis in over sixty cases. David Murray, *Queensland Authorities Confirm "Miscode" Affects DNA Evidence in Criminal Cases*, Courier Mail (Mar. 20, 2015).[9] In another case, a New York federal court permitted the inspection of the source code underlying the Forensic Statistical Tool developed by the New York City DNA laboratory. *U.S. v. Johnson*, 15-CR-565, D.I. 67 (S.D.N.Y. July 18, 2016). Given access, a defense computer scientist found that software's accuracy "should be seriously questioned." L. Kirchner, *Traces of Crime: How New York's DNA Techniques Became Tainted*, *N.Y. Times* (Sept. 4, 2017).[10] Two months later, the New York City laboratory notified customers that it would retire that software. *Id.*

It would be unreasonable simply to assume that TrueAllele is free from similar errors. But without access to the source code, defense counsel has no way to identify them.

B. The Prosecution Offers No Adequate Substitute for Access to the Software and Documentation.

The prosecution argues that access to the source code and internal validation data is unnecessary because the defense can examine publicly-available "validation studies" and "peer-reviewed articles" regarding TrueAllele. (State Supp. Br. at 12-13.) But reviewing articles that discuss how TrueAllele is

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

[10] https://www.nytimes.com/2017/09/04/nyregion/dna-analysis-evidence-new-york-disputed-techniques.html.

intended to work is insufficient to determine whether it ***actually*** works that way. Even if the scientific models underlying a given piece of software are valid, researchers have noted that errors in ***implementation*** "can be difficult to detect without access to source code." Morin et al., *Shining Light into Black Boxes*, 336 Sci. 159 (2012). Nor, in any event, is defendant required to trust Cybergenetics' own studies.

The need for access to the TrueAllele source code and validation data to confirm that it accurately implemented its purported scientific models is particularly acute here. As the Supreme Court noted in *Melendez-Diaz*, "[f]orensic evidence is not uniquely immune from the risk of manipulation." 557 U.S. at 318. There is a possibility that the programmers of TrueAllele, perhaps unconsciously, made decisions about how to implement the underlying models in software that may favor their intended customers – prosecutors. *Cf.*, Roth, *Machine Testimony*, 126 Yale L. J. at 1995-96 ("A programmer's conscious or unconscious bias might also influence algorithms' predictions or statistical estimates"; documenting examples). In particular, in the DNA analysis context, certain analytical choices by programmers, such as setting "thresholds" for distinguishing true genetic data from noise, "can affect the accuracy of the [software's] scores and estimates." Roth, *Machine Testimony*, 126 Yale L. J. at 1996. Without access to the source code and validation data, the defense has no way of identifying such errors or biases.

The prosecution argues that the defense does not need to

test the accuracy of TrueAllele because its reliability was shown in publicly available validation studies. (State Supp. Br. at 12-13.) But the notion that a criminal defendant must simply trust the word of a for-profit company that makes software specifically to sell to the police and prosecution cannot be squared with the Constitution, which requires "that reliability [of evidence] be assessed in a particular manner: by testing in the crucible of cross-examination." *Crawford v. Washington*, 541 U.S. 36, 61 (2004). The prosecution's position, if adopted, would "allow[] a jury to hear evidence, untested by the adversary process," based on the word of the prosecution or of businesses whose interests are aligned with the prosecution; this would "replace[] the constitutionally prescribed method of assessing reliability with a wholly foreign one." *Id.* at 62. Moreover, "[d]ispensing with confrontation because [the evidence] is obviously reliable is akin to dispensing with jury trial because a defendant is obviously guilty. That is not what the Sixth Amendment prescribes." *Id.*

The prosecution also argues that access to the source code is not needed because TrueAllele's algorithms and models are publicly available. (State Response Br. ("Rb"),13, 22-23). But computers do not run algorithms or models; they run ***software***, which can have errors even if the underlying algorithms and models which the software purports to implement are correct, as demonstrated by the numerous examples discussed *supra* § I.A. The alleged public availability of the algorithms or models does

not confirm whether the TrueAllele software (containing hundreds of thousands of lines of code) accurately implements those algorithms. Nor can the prosecution credibly maintain that an expert can test the code's accuracy by hand using pen and paper, considering that its use requires over nine trillion calculations. (Db, 19 n.7).

II. The NDA Unconstitutionally Favors Commercial Interests

A. The NDA Does Not Give Meaningful Access

The prosecution argues that "arrangements can be made to inspect the TrueAllele source code," (Rb, 14) but ignores the fact that the access terms Cybergenetics has set prevent the defense from meaningfully assessing TrueAllele's reliability.

Under the conditions imposed by Cybergenetics, if the defense's expert wishes to review the source code, the defense must pay for the ability to review the code on a stand-alone Cybergenetics computer, at a time and place Cybergenetics agrees to, and under constant supervision by a Cybergenetics representative. (*See* DA 140 ¶¶ 5, 8.) The scope and amount of the obligation to pay for the inspection remains undefined (*id.* at ¶ 5); and in any event no such cost is constitutionally permissible. Cybergenetics does not provide any commitment about when or where it will make the code available, nor does Cybergenetics state what "viewing software" it will provide on the computer. (DA 140 ¶ 8(d).) Given the size of the TrueAllele source code (approximately 170,000 lines of code), these conditions could make review last a prohibitively long

time, require multiple trips to some unknown location, and may even then not enable use of the forensic tools necessarily to properly test the software. Undersigned counsel have extensive experience with source code reviews in technically complex cases, and in their experience, assessment of computer software can only be done, as a practical matter, with the assistance of other computers and software, not via pen and paper.

Moreover, if the expert found errors, the defense is effectively barred from sharing them in court. Because Cybergenetics only allows the reviewer to take hand-written notes, (*id.* at ¶ 8(c)), and makes no provision for printing any of the source code, the defense would have no way of presenting documentary evidence of the errors. More alarmingly, any attempt by the defense to explain any errors it found to the court could subject counsel and retained experts to lawsuits in Ohio under Ohio law that could result in significant financial liability. (*See* DA137 §§ 12(e), 12(g).) Although the NDA contains an exception for disclosures that are "legally compelled," (DA136 § 7), it is not clear whether Cybergenetics would treat a disclosure affirmatively made by the defense in order to challenge the validity of a TrueAllele result as a "legally compelled" disclosure. The NDA thus forces the defense to act under a cloud of legal liability and risk of expense.

Subjecting defense counsel and experts to the liability risk created by Cybergenetics' terms would have a chilling effect on the defense's preparation of the case. That the

defense has the choice to avoid this exposure by refusing to sign the NDA solves nothing — such a Catch-22 places the burden on Mr. Pickett's counsel of choosing between liability exposure in Ohio or forfeiture of his right to crucial discovery.

B. Cybergenetics' Commercial Interests Can Be Protected

The prosecution repeatedly refers to TrueAllele as a "trade secret" to be protected from commercial competitors. But Mr. Pickett is not a competitor, and TrueAllele's interests can be protected without violating Mr. Pickett's constitutional rights.

Rules restricting evidence offend due process if they are "arbitrary or disproportionate to the purposes they are designed to serve." *United States. v. Scheffer*, 523 U.S. 303, 308 (1998). The Supreme Court has found that interests far weightier than Cybergenetics' monetary one must yield to protecting a defendant's constitutional rights. For example, in *Davis v. Alaska*, the Supreme Court held that restrictions on a defendant's ability to cross-examine a key prosecution witness about his juvenile delinquency record were unconstitutional because "the right of confrontation is paramount to the State's policy of protecting a juvenile offender." 415 U.S. 308, 319 (1974). As the Court explained, the State's concerns must give way to the defendant's right to "seek out the truth in the process of defending himself." *Id.* at 320.[11]

[11] The few cases in which the Supreme Court has declined to require access to potential evidence for a defendant were in circumstances far different from those here, as when in *Pennsylvania v. Ritchie*, it upheld the refusal of a child protective services agency to disclose a minor's records to a

In fact, orders requiring disclosure under reasonable protective terms are routinely entered even in ***civil*** litigation, such as in intellectual property cases, where a defendant's liberty is not even at stake. Undersigned counsel for *amici* practice in the area of intellectual property litigation, where disclosure of highly sensitive confidential technical information, including source code, is a routine practice. Indeed, some courts require automatic disclosure of source code, even in cases involving direct competitors. In fact, in the District of New Jersey, the local patent rules require an accused patent infringer to "produce or make available for inspection and copying: (a) ***Source code***, specifications, schematics, … formulas, [and] documentation" about allegedly infringing products. U.S. Dist. Ct. for the Dist. of N.J., Local Patent Rule 3-4 (emphasis added). The rules similarly require disclosure of source code in the Eastern District of Texas, one of the top districts for patent litigation.[12] *See* U.S. Dist. Ct. for the Eastern Dist. of Tex., Local Patent Rule

---

defendant accused of crimes against that minor. 480 U.S. 39 (1987). Here, not only is Cybergenetics' commercial interest in its source code far less weighty than the interest inherent in the confidential reporting by children of "rape … [and] incest," *id.* at 43, but that commercial interest can in any event remain protected by an appropriate protective order. Indeed, even in *Ritchie*, the Court held that the defendant was still "entitled to know whether the [child protective services] file contains information that may have changed the outcome of his trial had it been disclosed." *Ritchie*, 480 U.S. at 61.

[12] DocketNavigator, 2019 Year In Review, 15 (as of October 27, 2020), https://brochure.docketnavigator.com/2019-year-in-review/.

3-4. Yet undersigned counsel have never signed a non-disclosure contract ***with a private party*** as a condition for accessing sensitive technical information in discovery, nor are they aware of any case in which such an agreement has been required, much less under the terms Cybergenetics seeks to impose. Instead, technology companies ranging from Fortune 100 companies to Silicon Valley venture-backed start-ups routinely rely on ***court-issued*** protective orders, enforced by the issuing court, to safeguard their most sensitive technical information, even when it is being turned over to a competitor's counsel, without forcing counsel or experts to sign non-disclosure agreements. *See, e.g.*, *Rockstar Consortium U.S. LP v. Google Inc.*, No. 2:13-CV-893, 2014 WL 5831041, at *1-12 (E.D. Tex. June 19, 2014) (source code provisions in a protective order); *E-Contact Techs., LLC v. Apple, Inc.*, 2012 WL 11924448 (E.D. Tex. June 19, 2012) (same); *State Farm Fire & Cas. Co. v. Superior Court*, 54 Cal.App.4th 625, 651 (1997) (requiring disclosure of trade-secret software under a protective order).

The disproportionateness of Cybergenetics' conditions is starkly illustrated by a comparison between Cybergenetics' access terms and the terms found in protective orders in intellectual property cases. Consider, for example, the Northern District of California's Patent Local Rule 2-2 Interim Model Patent Protective Order ("Rule 2-2 Order"), which is the default protective order for all patent cases in that district.[13]

[13] https://www.cand.uscourts.gov/forms/model-protective-orders/.

See N.D. Cal. Patent L.R. 2-2. That district hears some of the most complex and high-profile patent cases in the world, often with billions of dollars at stake. Yet the Rule 2-2 Order does not purport to make the lawyers or experts of any party financially liable to another party. Nor does it prohibit disclosure of sensitive information to the court or to counsel; to the contrary, it expressly permits counsel and the court, as well as experts and certain support personnel, to view sensitive information. *See* Rule 2-2 Order at §§ 7.2, 7.3. Furthermore, the Rule 2-2 Order expressly permits the printing of portions of the source code (see *id.* at§ 9(d)). The Rule 2-2 Order also applies to non-parties and includes provisions permitting non-parties from whom discovery is sought to seek additional protections from the court. *Id.* at § 11. Companies litigating in that district routinely proceed under the default Rule 2-2 Order or make minor modifications to it. *See, e.g.*, Stipulated Modification to Patent L.R. 2-2 Interim Model Protective Order for Purposes of Expedited Discovery, *Apple v. Samsung*, No. 11-cv-01846 (N.D. Cal. Jun. 16, 2011), ECF No. 76.

Surely, if a protective order like the Northern District's Model Order can adequately protect the interests of direct competitors like Apple and Samsung when they are involved in high-stakes litigation, Cybergenetics can hardly claim that such protection would be insufficient to protect its interests in this case. There is no compelling need for Cybergenetics' unduly burdensome NDA requirements.

In sum, having advertised and sold to the State a software tool to be used in criminal prosecution, Cybergenetics' claims of trade secret privilege must yield to Mr. Pickett's constitutional right to have meaningful access to potentially exculpatory evidence regarding how that software works. To impose Cybergenetics' onerous requirements on Mr. Pickett in the name of protecting Cybergenetics' commercial interests would be "disproportionate to the purpose" of protecting Cybergenetics, and would offend due process. *Scheffer*, 523 U.S. at 308.

CONCLUSION

When testimony based on computer software is admitted as evidence, due process requires disclosure of the source code and other documentation about that software so that the accused can mount a meaningful defense. To hold otherwise would elevate error-prone software to the status of an unchallengeable oracle of innocence or guilt. Nor can constitutional rights be constrained or chilled by forcing payment and other commercial terms on an unwilling defendant as the price of their exercise. For the above reasons, the trial court's denial of defendant's motion to compel production of the TrueAllele source code and related documentation should be REVERSED.

Respectfully submitted,

Joseph Mazraani
Amicus on Behalf of
Movant-Appellant

By: */s/* Joseph Mazraani