2020

Secret Conviction Programs

Meghan J. Ryan
Southern Methodist University, Dedman School of Law

Secret Conviction Programs

Meghan J. Ryan*

Abstract

Judges and juries across the country are convicting criminal defendants based on secret evidence. Although defendants have sought access to the details of this evidence—the results of computer programs and their underlying algorithms and source codes—judges have generally denied their requests. Instead, judges have prioritized the business interests of the for-profit companies that developed these "conviction programs" and which could lose market share if the secret algorithms and source codes on which the programs are based were exposed. This decision has jeopardized criminal defendants' constitutional rights.

Table of Contents

---

* Associate Dean for Research, Altshuler Distinguished Teaching Professor, and Professor of Law. I thank Miriam Baer, Rachel Barkow, Paul Butler, Bennett Capers, Sharon Dolovich, Jeff Fagan, Andrew Ferguson, Bernard Harcourt, Josh Kleinfeld, Kate Levine, Adi Leibovitch, Anna Lvovsky, Sandy Mayson, Tracey Meares, Erin Murphy, John Pfaff, Dan Richman, David Sklansky, Crystal Yang, and all of the participants at the 2017 Columbia Criminal Justice Roundtable for their helpful comments. I also thank Tim Gallina for his excellent research assistance and Jenia Turner, Hillel Bavli, and Tré Welch for their helpful advice on this piece.

I. Introduction

Across the country, judges and juries are convicting defendants based on secret evidence. Prosecutors regularly present expert testimony on breathalyzer results, fingerprint matches, and DNA matches, but courts have generally not allowed defendants to scrutinize how the prosecutions' testifying experts produced this evidence.[1] In fact, these experts likely do not themselves know how the results of their tests were reached.[2] That is because much of this complicated, "scientific" evidence is generated by computer programs—"conviction programs"—built on secret algorithms and source codes developed in many instances by for-profit companies.[3] These companies refuse to reveal their secret formulas because they understandably do not want copycat companies to purloin

1. *See infra* Parts III–IV.
2. *See infra* Parts III–IV.
3. *See infra* Part IV.C.

their market shares.[4] While judges, lawyers, and jurors generally trust conviction programs' results as rooted in science, in truth there are real questions about the accuracy of the results these programs produce.[5] Because the programs' underlying algorithms and source codes are held as company secrets, there is generally little opportunity to sufficiently test the validity of their outputs.[6]

Even without access to the nuances of conviction programs, there is some evidence that these programs do not produce reliable evidence. In New York alone, thousands of convictions have been rooted in complex statistical analyses of DNA evidence that has since been seriously questioned.[7] When a court recently granted limited access to the source code of a conviction program used in these cases, an independent data analyst found that the program, which purported to accurately assess the likelihood that a defendant's DNA was found in a mixture of various individuals' DNA, was deficient; it excluded several variables that would be important to reach an accurate conclusion on this point.[8] This is incredibly troubling. In one case, when experts used competing conviction programs of complex statistical DNA analysis to assess the probability that a defendant was at the scene of the crime, each program produced a different result.[9] One indicated a likely DNA match and thus likely presence at the scene, whereas the other indicated that a match was unlikely and thus it was improbable that the defendant was at the crime scene.[10]

---

4. *See infra* Part IV.

5. *See infra* Part IV.

6. *See infra* Part IV.

7. *See* Lauren Kirchner, *Thousands of Criminal Cases in New York Relied on Disputed DNA Testing Techniques*, PROPUBLICA (Sept. 4, 2017, 6:00 PM), https://perma.cc/7ZAZ-V4MQ (last visited Oct. 27, 2019) ("Over the past decade, the DNA laboratory in the office of New York City's chief medical examiner emerged as a pioneer in analyzing the most complicated evidence from crime scenes. . . . Now these DNA analysis methods are under the microscope, with scientists questioning their validity.") (on file with the Washington and Lee Law Review).

8. *Id.*

9. *See* Seth Augenstein, *Subjective DNA Mixture Analysis, Used in Thousands of Cases, Blasted by WH Panel*, FORENSIC MAG. (Sept. 8, 2016, 12:37 PM), https://perma.cc/XZY3-ZAPB (last visited Oct. 27, 2019) (on file with the Washington and Lee Law Review).

10. *See id.* ("TrueAllele found the various DNA mixtures at the crime scene

Some commentators have criticized criminal justice actors' reliance on computer programs in setting bail and sentences, and in determining when to grant an offender parole.[11] But commentators have not been as vocal about the dangers associated with police officers and prosecutors relying on computer programs as investigatory tools and, more troublingly, as evidence for conviction.[12] Yet even more is at stake—a defendant's liberty or even his life—where conviction programs are involved. This happens when, for example, juries convict defendants based on the results of breathalyzer tests, police officers and fingerprint examiners rely on automated fingerprint identification systems (AFISs), and DNA analysts depend on programs like TrueAllele or STRmix for DNA matches.[13] In the context of assessing guilt, the accuracy of the programs on which the criminal justice system relies is critical.

Within the criminal justice system, the primary methods of ensuring the accuracy of evidence are by assessing the "reliability" of the information to determine whether it is admissible at trial and through adversarial testing—in the crucible of cross-examination—at trial.[14] Today, neither of these tools is truly available to criminal defendants inculpated by these programs aimed at conviction. Ordinarily, the algorithms and source codes on which these conviction tools are based are not made available to defendants.[15] Instead, the businesses responsible for creating the complicated algorithms, and the source codes implementing

---

could not place Hillary there, while the prosecution was relying on a STRmix interpretation of fingernail scrapings that indicated he was there.").

11. *See infra* Part II; *see also, e.g.*, Rebecca Wexler, *When a Computer Program Keeps You in Jail*, N.Y. TIMES (June 13, 2017), https://perma.cc/K368-QG93 (last visited Oct. 27, 2019) ("Technological advancement is, in theory, a welcome development. But in practice, aspects of automation are making the justice system less fair for criminal defendants.") (on file with the Washington and Lee Law Review).

12. *See infra* Part III.

13. *See infra* Part III.

14. *Cf.* Meghan J. Ryan, *Escaping the Fingerprint Crisis: A Blueprint for Essential Research*, 2020 U. ILL. L. REV. (forthcoming 2020) (on file with author) ("Beyond cross-examination, the defense often is unable to present its own evidence about the inaccuracies and unreliability of fingerprint evidence.").

15. *See infra* Part IV.

them, are kept secret in the name of the producing companies' business interests and based on the assumed accuracy of the programs.[16] This prevents criminal defendants facing conviction by computer algorithm and source code from mounting potentially viable defenses based on these secrets.

At least some level of transparency is necessary to probe the important questions tied up with using computer programs to convict criminal defendants. Without access to the details of the algorithms and source codes, actors within the criminal justice system cannot clearly discern the accuracy of these programs and the extent to which improper factors contribute to their outputs.[17] Simply trusting the creators of these programs cannot suffice—especially where the creators are for-profit businesses and especially where defendants' liberties and lives are on the line.

The persistence of questionable convictions based on purported "scientific" evidence stems from lawyers' blind faith in science and, relatedly, courts' refusal to allow investigation into the validity of these conviction programs.[18] Generally, judges and lawyers do not seem to be exceptionally troubled by the secret nature of the evidence used to convict criminal defendants.[19] As in other areas where evidence has been labeled as science-based, the criminal justice system has often given experts in this arena a free pass. Certainly, science has its allure. It can offer an objective approach to decisionmaking, and, when linked with the impressive power of computing, it can survey a broad array of data in a significantly more cost-effective and reliable way than humans alone can ordinarily accomplish.[20] But those not familiar with

---

16. *See infra* Part IV.

17. *See infra* Part IV.

18. *See infra* Part IV.C; *see also* NAT'L INST. OF JUSTICE, NATIONAL CONFERENCE ON SCIENCE AND LAW PROCEEDINGS 7 (April 15–16, 1999), https://perma.cc/X46M-LV8Y (PDF) ("[L]awyers would like to see science, when it is used in the courtroom, if not infallible, at least mostly accurate, mostly immutable, and certain. That is the very factor that, in the legal mind, makes the evidence also 'reliable.'").

19. *But see infra* Part III.B (discussing challenges to the admissibility of DNA evidence reached through analyses based on TrueAllele and STRmix computer programs).

20. *See* Lance Whitney, *Are Computers Already Smarter Than Humans?*, TIME (Sept. 29, 2017), https://perma.cc/DA9E-ZMXS (last visited Oct. 27, 2019)

these disciplines, including lawyers, often over-hype science and technology.[21] These disciplines are not a panacea.[22] Human error is often built into these fields, and the powers of science and technology have their limits.[23] By venerating these disciplines, lawyers risk surrendering one of their most valuable assets: skepticism.

More than of just general concern, the secrecy shrouding the algorithms and source codes leading to defendant convictions is of constitutional proportions.[24] It strikes at the heart of a defendant's due process right to have a meaningful opportunity to make a full defense.[25] Without the necessary information about the evidence that is being used to convict him, a defendant is denied the opportunity to properly challenge this evidence.[26] Further, the defendant's Sixth Amendment confrontation right loses its meaning when the expert testifying to the results of a breathalyzer test, fingerprint match, or DNA analysis does not fully understand the nuances of how the conviction program computed the results used as evidence against the defendant.[27] Because the police officer testifying about a breathalyzer result ordinarily is not familiar

---

("Computers can take in and process certain kinds of information much faster than we can. They can swirl that data around in their 'brains,' made of processors, and perform calculations to conjure multiple scenarios at superhuman speeds.") (on file with the Washington and Lee Law Review).

21. *See infra* Part IV.C; *see also* Peter Huber, *Junk Science in the Courtroom*, 26 VAL. U. L. REV. 723, 724 (1992) ("Lawyers may seize upon a researcher's first expression of concern, and give it much import, even as later developments fail to support the concern.").

22. *Cf.* Huber, *supra* note 21, at 739 (conceding that "the views of the establishment are sometimes wrong, in science and medicine as in law" and noting that "Galileo gained fame by challenging one orthodoxy but eventually became part of another: he refused to believe that the moon caused tides, or that planets moved in ellipses").

23. *See id.* at 724–29.

24. *See infra* Part V (explaining how withholding such relevant evidence from the defense raises serious due process and confrontation issues).

25. *See* Holmes v. South Carolina, 547 U.S. 319, 324 (2006) (stating that the Due Process Clause guarantees a defendant the opportunity to make a complete defense at trial); Chambers v. Mississippi, 410 U.S. 284, 294 (1973) ("The right of an accused in a criminal trial to due process is, in essence, the right to a fair opportunity to defend against the State's accusations.").

26. *See infra* Parts IV–V.

27. *See infra* Part V.

with the underlying algorithm and source code, for example, a full examination about the accuracy of the result is impossible.[28] The officer will not be able to explain how the breathalyzer transformed the defendant's breath into a 0.10 reading as a machine estimate of the defendant's blood alcohol concentration.[29] Similarly, even a DNA analyst on the stand will ordinarily lack sufficient knowledge about a computer program such as TrueAllele or STRmix so that defense counsel can effectively use cross-examination to fully probe the reliability of evidence produced by these programs.[30] And a fingerprint examiner lacks the necessary expertise of the underlying algorithms and source codes of AFISs to be able to competently testify about how they generate suspect fingerprints for analysis and, ultimately, conviction. With insufficient expertise on the conviction programs producing the results introduced at trial, defense counsel's opportunity to cross-examine these experts is insufficient to meet the demands of the Sixth Amendment right to confront witnesses against the defendant.[31] Finally, the secrecy shielding all of this evidence from discovery is also questionable

---

28. *See infra* Parts IV–V; *see also generally* CRIMINAL JUSTICE STANDARDS & TRAINING COMM'N, FLA. DEP'T OF LAW ENFORCEMENT, BREATH TEST OPERATOR: A SPECIALIZED TRAINING COURSE 6 (2015) (summarizing the science behind breathalyzers without referencing the algorithm and source code that are integral to producing the relevant values admissible in court).

29. *See infra* Parts III–IV; *see also generally* CRIMINAL JUSTICE STANDARDS & TRAINING COMM'N, *supra* note 28 (neglecting to explicate the algorithms and source codes underlying breathalyzers).

30. When TrueAllele and STRmix have been used in courts recently, the government has called the computer programs' developers to the stand to testify about the accuracy and reliability of the programs. *See* Lauren Kirchner, *Sentenced by an Algorithm: Where Traditional DNA Testing Fails, New Technology Takes Over*, PAC. STANDARD (Nov. 9, 2016), https://perma.cc/LJB6-E2RH (last updated June 14, 2017) (last visited Feb. 20, 2020) (on file with the Washington and Lee Law Review). This is not generally the case with evidence based on, for example, breathalyzer programs or AFISs. The difference, it seems, is the newness of these DNA-focused computer programs. The programs used to calculate breathalyzer results and match fingerprints are generally not challenged in court, and they certainly are not challenged in the same way by calling on an expert familiar with the underlying algorithms and source codes. In a sense, these technologies seem to have been grandfathered in under the criminal justice system.

31. *See infra* Part V.

under *Brady v. Maryland*[32] and its progeny, as well as the statutory discovery requirements of some states.[33]

This Article challenges the use of conviction programs—their algorithms and source codes—under these secret conditions, arguing that greater disclosure is generally necessary to meet the constitutional requirements essential to the defendant having an opportunity to make his defense, confront witnesses, and truly benefit from due process guarantees. Part II describes the rise of the criminal justice system's confidence in and dependence on predictive algorithms and their underlying source codes to aid judges and parole boards in making bail, sentencing, and parole decisions. It outlines the reasons why decisionmakers within the criminal justice system increasingly rely on these programs and also summarizes the common criticisms of this reliance. Part III explains that, while the benefits and drawbacks of relying on these predictive algorithms and their source codes are relatively well known, the more concerning reliance on computer programs in the context of *convicting* criminal defendants has largely gone unnoticed. This Part delineates three program-based conviction tools that prosecutorial teams use to help convict defendants: breathalyzers, AFISs,[34] and computerized DNA interpretation programs.[35] It also explains that the details of these programs are generally kept secret and that there are real questions about the accuracy of these programs. Part IV expands upon the secrecy shrouding the details of the conviction programs that prosecutors employ, explaining how defendants are generally denied access to

---

32. 373 U.S. 83 (1963).

33. *See infra* Part V; *see also, e.g.*, N.C. GEN. STAT. § 15A-903 (2018) (requiring the state upon motion to provide "the complete files of all law enforcement agencies, investigatory agencies, and prosecutors' offices involved in the investigation of the crimes committed or the prosecution of the defendant").

34. As explained in Part IV.A.2, AFISs are not usually directly used in securing convictions. Instead, these programs usually provide human fingerprint examiners with a handful of the most likely candidate fingerprints to match against, for example, a fingerprint found at a crime scene. The human interpreter then determines whether there is a match and may testify at trial. *Id.* However, because fingerprint examiners employ questionable methods themselves in determining whether there is a match, the AFIS potential matches from which they often begin their analyses play a large part in the evidence that is eventually introduced at trial to convict criminal defendants. *Id.*

35. The computer programs I refer to here are probabilistic genotyping systems (PGSs).

this information that could prove material to their cases. It also emphasizes the importance of transparency for testing the accuracy of these programs. Further, this Part explains that lawyers and the criminal justice system tend to revere computer programs and science and technology in general. Certainly, there is value in pursuing an objective approach to criminal justice determinations, but science and technology are not infallible, and it is important that actors within the criminal justice system recognize this. Finally, Part V argues that this secrecy is of constitutional proportions, as it denies defendants their due process rights to have meaningful opportunities to present full defenses, and it detracts from their confrontation rights to examine witnesses about the algorithms and source codes upon which their convictions are ultimately based. Employing these secret conviction programs even has implications for prosecutors' duties under *Brady* and other applicable statutory disclosure requirements. Where police officers, prosecutors, and experts employ secret conviction programs, criminal defendants' constitutional rights are in jeopardy.

II. Predictive Criminal Justice Programs

Judges, parole boards, and even prosecutors and police officers have all begun relying on computer algorithms and source codes in their roles within the criminal justice system.[36] Some judges employ programs in setting bail to help them predict whether suspects are likely to appear for their court dates and whether they pose a danger to the public.[37] And some judges use programs to assess the future dangerousness of offenders so that they can

---

36. *See* Ric Simmons, *Big Data and Procedural Justice: Legitimizing Algorithms in the Criminal Justice System*, 15 OHIO ST. J. CRIM. L. 573, 573 (2018) (describing criminal justice actors' uses of algorithms in the criminal justice system).

37. *See* Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109, 1124, 1120 (2017) ("In the pretrial detention stage, judges in many states routinely rely on risk assessment instruments to predict future dangerousness before deciding on release conditions."); Lauryn P. Gouldin, *Defining Flight Risk*, 85 U. CHI. L. REV. 677, 713–18 (2018).

properly sentence them.[38] Many parole boards similarly rely on computer programs to assess the likelihood of recidivism to determine whether an offender should be granted parole.[39] There are both benefits and drawbacks to relying on such a systematized approach to justice. To fully understand the advantages and disadvantages, though, it is first necessary to understand the different working parts of modern computer programs.

A. Computer Programs—Algorithms and Source Codes

Various actors within the criminal justice system regularly rely on computer programs to predict behavior.[40] Like typical computer programs, these prediction programs consist of algorithms and the underlying source codes to implement those algorithms. An algorithm is a set of rules used to solve a problem through a series of discrete steps.[41] And "algorithm" is the term commentators often use to describe the programs jurisdictions in recent years have used to help set bail, determine sentences, and make parole decisions.[42] How experts put these algorithms to use, though, complicates matters. In the age of computers, they often computerize these algorithms to increase efficiency. This requires that the algorithm be translated into source code.[43] A computer

38. *See* Ferguson, *supra* note 37, at 1120 ("[M]ost states have adopted some measure of actuarial prediction in sentencing or parole determinations.").

39. *See id.*

40. This is sometimes referred to as "[a]ctuarial prediction." *Id.* at 1118–19.

41. *See Algorithm*, OXFORD ENGLISH DICTIONARY (3d ed. 2012) ("A procedure or set of rules used in calculation and problem-solving . . . a precisely defined set of mathematical or logical operations for the performance of a particular task.").

42. *See, e.g.*, Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://perma.cc/2FSK-27MK (last visited Oct. 5, 2019) (referring to "algorithms" used to predict recidivism) (on file with the Washington and Lee Law Review); Lauren Kirchner, *Where Traditional DNA Testing Fails, Algorithms Take Over: Powerful Software Is Solving More Crimes and Raising New Questions About Due Process*, PROPUBLICA (Nov. 4, 2016, 8:00 AM), https://perma.cc/9DQZ-5YKG (last visited Oct. 5, 2019) (discussing "algorithms" used to determine the likelihood that a DNA sample from a crime scene came from a particular individual) (on file with the Washington and Lee Law Review).

43. *See* PELIN AKSOY & LAURA DENARDIS, INFORMATION TECHNOLOGY IN THEORY 102–04 (2008); JUNE JAMRICH PARSONS, NEW PERSPECTIVES ON COMPUTER CONCEPTS 2018, at 777, 785 (2018) (briefly describing algorithms and source

programmer can convert the algorithm into a variety of source code or programming languages—such as C, C++, BASIC, Python, Java, JavaScript, IOS, or SQL—each of which would look slightly different but could be generally recognizable by those competent in the field.[44] A compiler or interpreter then translates the source code into object or machine code, which presents as a series of ones and zeros.[45] This string of numbers is generally incomprehensible to humans. But it effects an output, which can then be used for various purposes, such as to predict the behaviors of criminal offenders.[46] The technicalities and nuances of this process, though, generally remain hidden from the users of the program, making it difficult for them to understand the way in which the task is performed.

B. A History of Seeking Predictions

The criminal justice system's harnessing of predictive power dates back to the late 1920s.[47] Even without the power of computing, the criminal justice system turned to prediction algorithms to assess the risk of offenders' recidivism on parole.[48] In recent years, as evidence-based practices have gained steam, use of these tools has ballooned.[49] Not only do jurisdictions use

---

codes).

44. *See* AKSOY & DENARDIS, *supra* note 43, at 102–04; PARSONS, *supra* note 43, at 786; MICHAEL L. SCOTT, PROGRAMMING LANGUAGE PRAGMATICS 4–5, 11, 14 (4th ed. 2016).

45. *See* AKSOY & DENARDIS, *supra* note 43, at 102–04.

46. *See* Angwin et al., *supra* note 42.

47. *See* BERNARD HARCOURT, AGAINST PREDICTION 47 (2007); *Timeline of Computer History*, COMPUTER HISTORY MUSEUM, https://perma.cc/R9A2-LKQF (last visited Oct. 5, 2019) (on file with the Washington and Lee Law Review).

48. *See* Ferguson, *supra* note 37, at 1117–20 (briefly relating the history of an actuarial approach to criminal justice); *see also* HARCOURT, *supra* note 47, at 47 (explaining that "[t]he actuarial impulse was strong [even] in the 1920s").

49. *See* Megan Stevenson, *Assessing Risk Assessment in Action*, 103 MINN. L. REV. 303, 312–14 (2018) (explaining that "their use has rapidly accelerated over recent years"); Angwin et al., *supra* note 42 ("[R]isk assessments . . . are increasingly common in courtrooms across the nation. . . . In Arizona, Colorado, Delaware, Kentucky, Louisiana, Oklahoma, Virginia, Washington, and Wisconsin, the results of such assessments are given to judges during criminal

these tools in making parole decisions, but now judges also use them in setting bail and sentencing.[50] Rapidly advancing technology has even further magnified the power of these prediction programs, and several jurisdictions now employ computer-based risk-assessment tools such as Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)—a risk assessment tool created and licensed by Northpointe.[51]

---

sentencing."); *cf.* Kirchner, *supra* note 42 (explaining that "[t]he emergence of algorithmic analysis programs . . . is creating a new frontier of DNA science," that these "tools are so new and expensive that only a handful of local crime labs use them regularly," and that "as law enforcement looks to DNA more and more frequently to solve even minor crimes, that seems almost certain to change").

50. *See* Ferguson, *supra* note 37, at 1120–21 ("Today, actuarial prediction impacts almost all aspects of the criminal justice system, from the initial bail decision to the final parole release."). One additional area in which computer programs are today playing a significant role is in policing. *See* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 2 (2017) (describing "big data policing"). Police departments throughout the country now employ sophisticated programs to assess the likelihood of crime taking place in particular locations. *See id.* at 67 ("Today, several dozen cities are using some form of predictive policing technology."). Although police departments have long tried to find patterns in reported crimes to try to predict the locations of future crime and marshal their resources accordingly, technological advances have allowed these departments to more firmly put the power of statistics behind them to improve their predictions. *See* Ferguson, *supra* note 37, at 1117–20. Today, various companies license programs like PredPol and HunchLab to help police departments make more informed decisions about how best to fight crime. *See HunchLab—Next Generation Predictive Policing Software*, HUNCHLAB, https://perma.cc/5FUX-DGPY (last visited Oct. 6, 2019) (stating that it employs "advanced statistical models [to] forecast when and where crimes are likely to emerge"); *Predict Prevent Crime—Predictive Policing Software*, PREDPOL, https://perma.cc/W98H-H56L (last visited Oct. 6, 2019) (stating that PredPol "predict[s] where and when specific crimes are most likely to occur"). Select police departments across the country rely on programs like these to assist their decisions about where, when, and how to best police their communities. *See* FERGUSON, *supra*, at 67.

51. *See* NORTHPOINTE, PRACTITIONER'S GUIDE TO COMPAS CORE 2 (2015), https://perma.cc/3NDH-YVAK (PDF); Sam Corbett-Davies et al., *A Computer Program Used for Bail and Sentencing Decisions Was Labeled Biased Against Blacks. It's Actually Not That Clear.*, WASH. POST (Oct. 17, 2016, 5:00 AM), https://perma.cc/375A-VT4Y (last visited Oct. 6, 2019) (on file with the Washington and Lee Law Review).

In general, these assessment tools are based on answers to a number of questions, such as: What is the offender's marital status?[52] What is his highest education level?[53] Does he have any history of drug use?[54] Based on the answers to these questions, the particular tool will predict, at least to some degree, the likelihood that the offender will engage in certain conduct, such as future criminal acts or fleeing the jurisdiction. When using an automated tool like COMPAS, the algorithm and underlying source code used to calculate the relevant risk scores are often not available to the defendant or even the program user.[55]

COMPAS—and programs like it—are meant to improve objectivity, fairness, and efficiency in setting bail and doling out sentences.[56] Finding these factors desirable, jurisdictions throughout the country rely on such algorithms and source codes to predict recidivism, which can affect bail, sentencing, and parole.[57]

C. The Allure

Proponents of these predictive criminal justice programs explain that such a methodical, evidence-based approach to difficult criminal justice questions will usher in a system with greater fairness, consistency, and accuracy.[58] Our criminal justice

---

52. *See* Sonja B. Starr, *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, 66 STAN. L. REV. 803, 805, 811–12 (2014); VRAG-R SCORING SHEET 2, https://perma.cc/RM63-7GWC (PDF).

53. *See* Starr, *supra* note 52, at 811–12; Christopher T. Lowenkamp et al., *The Predictive Validity of the LSI-R on a Sample of Offenders Drawn from the Records of the Iowa Department of Corrections Data Management System*, FED. PROBATION, 2 (2001), https://perma.cc/5CQC-2G45 (PDF).

54. *See id.*; VRAG-R SCORING SHEET, *supra* note 52, at 2.

55. *See infra* Part IV.

56. *See* NORTHPOINTE, *supra* note 51, at 2 ("In overloaded and crowded criminal justice systems, brevity, efficiency, ease of administration, and clear organization of key risk/needs data are critical. COMPAS was designed to optimize these practical factors.").

57. *See id.*

58. *See* Anna Maria Barry-Jester et al., *Should Prison Sentences Be Based On Crimes That Haven't Been Committed Yet?*, FIVETHIRTYEIGHT (Aug. 4, 2015), https://perma.cc/SLH8-4ACW (last visited Oct. 6, 2019) (examining some of the

system is riddled with concerns of biases. For example, the disproportionate number of black males in American prisons has been described as resulting from "the new Jim Crow";[59] blacks and Hispanics are more often the targets of stops and frisks than whites;[60] and there have been vociferous outcries against the large numbers of black male youths who have recently been killed by law enforcement officers.[61] Trying to address these problems is

---

risks and benefits of using these predictive models) (on file with the Washington and Lee Law Review); Adam Neufeld, *In Defense of Risk-Assessment Tools*, MARSHALL PROJECT (Oct. 22, 2017, 10:00 AM) https://perma.cc/53VZ-TK5B (last visited Oct. 6, 2019) (acknowledging that "[i]t may seem weird to rely on an impersonal algorithm to predict a person's behavior given the enormous stakes" but arguing that "the gravity of the outcome—in cost, crime, and wasted human potential—is exactly why we should use an algorithm" in these circumstances) (on file with the Washington and Lee Law Review); SARAH PICARD-FRITSCHE ET AL., CTR. FOR COURT INNOVATION, DEMYSTIFYING RISK ASSESSMENT: KEY PRINCIPLES AND CONTROVERSIES 11–12 (2017), https://perma.cc/U9PP-5HQR (PDF) (emphasizing the usefulness of predictive criminal justice programs but also noting critics' concerns).

59. *See generally* MICHELLE ALEXANDER, THE NEW JIM CROW: MASS INCARCERATION IN THE AGE OF COLORBLINDNESS (2010) (arguing that the mass incarceration of black men in the name of the War on Drugs amounts to a "new Jim Crow").

60. *See* Floyd v. City of New York, 959 F. Supp. 2d 540, 562 (S.D.N.Y. 2013) (concluding that New York City's "policy of indirect racial profiling . . . has resulted in the disproportionate and discriminatory stopping of blacks and Hispanics in violation of the Equal Protection Clause"); ELIZABETH DAVIS & ANTHONY WHYDE, BUREAU OF JUSTICE STATISTICS, CONTACTS BETWEEN POLICE AND THE PUBLIC, 2015, at 9 (2018), https://perma.cc/F3UZ-2T5M (PDF) (highlighting that "[a] greater percentage of blacks than whites experienced police-initiated contact during their most recent contact").

61. *See, e.g.*, Mario L. Barnes, *Criminal Justice for Those (Still) at the Margins—Addressing Hidden Forms of Bias and the Politics of Which Lives Matter*, 5 U.C. IRVINE L. REV. 711, 713–14 (2015) (explaining that the "Black Lives Matter" movement arose out of police killings of young, unarmed black men); Collier Meyerson, *Another Black Boy Was Killed by Police. Will Justice Be Done This Time?*, THE NATION (May 5, 2017), https://perma.cc/X9VS-JERC (last visited Oct. 6, 2019) (reacting to the many recent killings of black children by police officers) (on file with the Washington and Lee Law Review); Brentin Mock, *How Structural Racism is Linked to Higher Rates of Police Violence*, CITYLAB (Feb. 15, 2018), https://perma.cc/V2D7-EEH4 (last visited Oct. 6, 2019) ("Many studies do show that racism plays a part in causing police to pull the trigger more quickly on black suspects. That's usually because of the implicit racial biases of the individual police officer involved.") (on file with the Washington and Lee Law Review). Further, Project Implicit at Harvard University suggests that biases are deeper and more difficult to correct than may at first be apparent. *See About Us*,

difficult, though. Decisionmakers in the criminal justice arena—whether judges, prosecutors, jurors, or parole board members—are human beings with built-in prejudices and biases, whether conscious or unconscious.[62] Harvard University's Project Implicit—an ongoing study collecting data on individuals' biases—has found that nearly everyone suffers from bias.[63] Whether biases are a result of evolution—allowing our brains to take mental shortcuts to more easily survive[64]—upbringing,[65] or culture,[66] biases can be detrimental and unjust to criminal defendants. Biases might result in a particular defendant being

---

PROJECT IMPLICIT (2011), https://perma.cc/8NUZ-Y5DB (last visited Oct. 6, 2019) [hereinafter PROJECT IMPLICIT] (collecting data on individuals' implicit biases) (on file with the Washington and Lee Law Review); *see also* Kristin A. Lane et al., *Implicit Social Cognition and Law*, 3 ANN. REV. L. & SOC. SCI. 427, 431–39 (2007) (pointing out that nearly everyone possesses implicit biases, explaining that these biases are very strong and that they also predict behavior, and noting that this link between bias and behavior can be moderated under certain conditions).

62. *See* PROJECT IMPLICIT, *supra* note 61; Lane et al., *supra* note 61; Annie Murphy Paul, *Where Bias Begins: The Truth About Stereotypes*, PSYCHOL. TODAY (May 1, 1998), https://perma.cc/6FY8-KJL8 (last visited Oct. 6, 2019) ("Psychologists once believed that only bigoted people used stereotypes. Now the study of unconscious bias is revealing the unsettling truth: We all use stereotypes, all the time, without knowing it. We have met the enemy of equality, and the enemy is us.") (on file with the Washington and Lee Law Review).

63. *See* PROJECT IMPLICIT, *supra* note 61; *see also* Meghan J. Ryan & John Adams, *Cultivating Judgment on the Tools of Wrongful Conviction*, 68 SMU L. REV. 1073, 1101 (2015) ("One of the major sources of information about the existence of implicit biases comes from the Implicit Association Test (IAT). In this test, subjects are asked to 'rapidly classify individual stimuli into' particular categories, and the subjects' rates of classification are then measured." (internal citations omitted)).

64. *See* Martie G. Haselton et al., *The Evolution of Cognitive Bias*, *in* 2 HANDBOOK OF EVOLUTIONARY PSYCHOLOGY 968, 968–69 (David M. Buss ed., 2d ed. 2016); *see also* Christopher Dwyer, *12 Common Biases that Affect How We Make Everyday Decisions*, PSYCHOL. TODAY (Sept. 7, 2018), https://perma.cc/CFL8-CMC5 (last visited Oct 6. 2019) (suggesting that in-group bias is evolutionary) (on file with the Washington and Lee Law Review).

65. *See* Eva H. Telzer et al., *Amygdala Sensitivity to Race Is Not Present in Childhood but Emerges over Adolescence*, 25 J. COGNITIVE NEUROSCI. 234, 234, 240, 242 (2013) (suggesting that racial bias is a product of upbringing); Robert Wright, *Nature vs. Nurture? New Research Shows Racism Isn't Innate*, ATLANTIC (Oct. 18, 2012), https://perma.cc/HW2H-XDXN (last visited Oct. 6, 2019) (on file with the Washington and Lee Law Review).

66. *See* Paul, *supra* note 62 ("Much of what enters our consciousness, of course, comes from the culture around us.").

convicted when he would not have been convicted in the absence of bias, receiving a longer sentence than someone who committed the same crime but was not of the same race, getting his bail set at a higher amount than someone of a different religion, or not being granted parole when someone of a different ethnicity would have been granted parole.[67] Decisionmakers can mitigate their biases through education if the decisionmaker acknowledges the problem and has an open mind about the offered education,[68] so there is some hope for alleviating biases within the criminal justice system. Despite being a concern that commentators have recognized for years, though, biases within the system persist.

Aside from biases within the system, there is also the problem of other inequities, which is inherent in a system that generally relies on different decisionmakers in each case.[69] This concern about lack of uniformity explains the rise of mandatory sentencing guidelines in this country[70] (which were later found to be unconstitutional[71]) and, to some extent, mandatory minimum sentences.[72] As Marvin Frankel famously explained, a judge might

---

67. *See* Angwin et al., *supra* note 42 ("For more than two centuries, the key decisions in the legal process, from pretrial release to sentencing to parole, have been in the hands of human beings guided by their instincts and personal biases.").

68. *See* Lane et al., *supra* note 61, at 437–39 (stating that implicit social cognitions may change based on varied experiences and environments); Jeffrey J. Rachlinski et al., *Does Unconscious Bias Affect Trial Judges?*, 84 NOTRE DAME. L. REV. 1195, 1226–32 (2009) (describing how training can mitigate judicial bias); Ryan & Adams, *supra* note 63, at 1102 ("Providing some hope for limiting how these biases might affect decisionmaking, . . . studies suggest that implicit biases can possibly be reduced or at least that decisionmakers, provided proper motivation, are capable of compensating for their biases.").

69. *See generally* Anthony Niblett, *Tracking Inconsistent Judicial Behavior*, 34 INT'L REV. L. & ECON. (2013) (examining inconsistencies in judicial decisionmaking).

70. *See* United States v. Booker, 543 U.S. 220, 255 (2005) ("Congress enacted the sentencing statutes in major part to achieve greater uniformity in sentencing, *i.e.*, to increase the likelihood that offenders who engage in similar real conduct would receive similar sentences.").

71. *See generally id.* at 245 (holding that the mandatory federal sentencing guidelines are unconstitutional).

72. *See* U.S. SENTENCING COMM'N, MANDATORY MINIMUM PENALTIES IN THE FEDERAL CRIMINAL JUSTICE SYSTEM: A SPECIAL REPORT TO CONGRESS 13–14 (1991), https://perma.cc/LBH5-A4CG (PDF) ("Mandatory minimums are meant to ensure that defendants convicted of similar offenses receive penalties that at least begin

sentence a defendant to an entire additional year in prison just because the defendant spoke disrespectfully to the judge.[73] This concern of one offender receiving harsher treatment than a similarly situated offender just because of his bad luck is a continuing one.

Even if defendants are not affected by biases or other inequities within the system, they are often subject to guesswork by judges and parole boards.[74] Judges and parole boards may base

---

at the same minimal point."). *But see* Stephen J. Schulhofer, *Rethinking Mandatory Minimums*, 28 WAKE FOREST L. REV. 199, 210 (1993) (explaining that "[e]nsuring equal treatment of like offenders prevents one form of disparity, but the resulting equal treatment of unlike offenders creates another serious problem—excessive uniformity" and stating that "[e]xcessive uniformity is inevitable under mandatories because the statutes necessarily single out just one or a very small number of factors to determine the minimum sentence").

73. MARVIN E. FRANKEL, CRIMINAL SENTENCES: LAW WITHOUT ORDER 18 (1972). Frankel famously related:

> One story concerns a casual anecdote over cocktails in a rare conversation among judges touching the subject of sentencing. Judge X, to designate him in a lawyerlike way, told of a defendant for whom the judge, after reading the presentence report, had decided tentatively upon a sentence of four years' imprisonment. At the sentencing hearing in the courtroom, after hearing counsel, Judge X invited the defendant to exercise his right to address the court in his own behalf. The defendant took a sheaf of papers from his pocket and proceeded to read from them, excoriating the judge, and "kangaroo court" in which he'd been tried, and the legal establishment in general. Completing the story, Judge X said, "I listened without interrupting. Finally, when he said he was through, I simply gave the son of a bitch five years instead of four." None of the three judges listening to that (including me) tendered a whisper of dissent, let alone a scream of outrage. But think about it. . . . a year in prison for speaking disrespectfully to a judge.

Id.

74. *See* Sheri Lynn Johnson, *The Politics of Predicting Criminal Violence*, 86 MICH. L. REV. 1322, 1325 (1988) (explaining Stephen Gottfredson and Marc Miller's response to questions about the usefulness of actuarial tools: "Because judges and parole boards do predict and because their unaided predictions are even less accurate than chance, actuarial predictions are better than the current system of implicit and ignorant guesses."); Sam B. Warner & Henry B. Cabot, *Changes in the Administration of Criminal Justice During the Past Fifty Years*, 50 HARV. L. REV. 583, 607 (1937) (referring to judges' and parole boards' sentencing and release decisions as "a matter of guesswork"); *cf.* William W. Wilkins et al., *Competing Sentencing Policies in a "War on Drugs" Era*, 28 WAKE FOREST L. REV. 305, 309 (1993) (explaining that, before the federal guidelines, "judges frequently engaged in the 'guessing game' of imposing sentences in anticipation of potential release dates authorized by the Parole Commission").

their bail, sentencing, and parole decisions on a broad array of factors, including their own experiences both inside and outside of the courtroom and parole board hearing room.[75] But they historically have not made their decisions based on social science research meant to assess the probability that any particular defendant will make his court appearances, recidivate, or pose other risks to society.[76]

Using computer programs in setting bail, sentencing, and deciding parole issues can be effective in achieving fairness across cases. Computer algorithms and their source codes are automated approaches to criminal justice, and the individual decisionmakers within the system—from judges to parole board members—can potentially dole out justice without being influenced by, for example, what they had for breakfast, if they depend on computer programs to make their decisions for them. Relying on these programs can also help judges and other decisionmakers avoid injecting their own biases into decisions on bail, sentencing, and parole.[77] In these senses, computer-program-based decisionmaking serves the goals of system-wide fairness and consistency. Further, these computer programs are generally built on social science data to produce more accurate predictions about human behavior.[78] In this sense, they may be considered better than the hunches on which judges and parole boards base their decisions.

Employing computer programs to resolve criminal justice issues can also inject efficiency into the system.[79] Automated

---

75. *See* Jill D. Weinberg & Laura Beth Neilsen, *Examining Empathy: Discrimination, Experience, and Judicial Decisionmaking*, 85 S. CAL. L. REV. 313, 324 (2012) (stating that "judges do not completely abandon their experiences when deciding cases").

76. *See* Johnson, *supra* note 74, at 1325 (noting that judges' and parole boards' "unaided predictions are even less accurate than chance"); Warner & Cabot, *supra* note 74, at 607 (referring to judicial "guesswork" in sentencing and noting that the information on which sentencing judges have traditionally based these decisions has been quite limited).

77. *See* Neufeld, *supra* note 58 ("[A]lgorithms aren't *directly* subject to human cognitive biases . . . ." (emphasis added)).

78. *See* PICARD-FRITSCHE ET AL., *supra* note 58, at 8–10 (describing the development of risk assessment tools using social science research).

79. *See* Sarah Fishel et al., *Computer Risk Algorithms and Judicial Decision-making*, AM. PSYCHOL. ASS'N (Jan. 2018), https://perma.cc/S2XY-9ZFS (last visited

justice is often swift justice.[80] Not surprisingly, then, players within the criminal justice system are beginning to rely more heavily on computer programs to keep the machinery of justice—or at least of the system—moving. [81]

D. Predictable Criticisms

Although adopting a data-driven approach to criminal jusitce is alluring, some commentators have criticized the use of computer programs in all of these areas—in setting bail, sentencing, and making parole decisions—for embedding and exacerbating biases in the criminal justice system.[82] Most often, these commentators focus their criticisms on the particular factors that control the algorithms' outputs.[83] For example, factors like employment status, marital status, and educational level—factors often used in assessments of future dangerousness—are often proxies for race.[84]

Oct. 6, 2019) (on file with the Washington and Lee Law Review).

80. *See id.* ("[L]egal decision-makers can drastically increase the expediency of their decision-making within an often slow and overburdened system.").

81. *See* STEPHANOS BIBAS, THE MACHINERY OF CRIMINAL JUSTICE 110 (2012) (stating that, "[w]hen judges and scholars evaluate criminal procedure, they tend to focus on efficiency").

82. *See, e.g.*, Starr, *supra* note 52, at 821; Angwin et al., *supra* note 42 (asserting that COMPAS results "turned up significant racial disparities").

83. A study by ProPublica exposed racial disparities in the results produced by Northpointe's predictive algorithm COMPAS. *See* Angwin et al., *supra* note 42. According to the study, the algorithm was "particularly likely to falsely flag black defendants as future criminals, wrongly labeling them this way at almost twice the rate as white defendants." *Id.*

84. *See* CHRISTINE S. SCOTT-HAYWARD & HENRY F. FRADELLA, PUNISHING POVERTY: HOW BAIL AND PRETRIAL DETENTION FUEL INEQUALITIES IN THE CRIMINAL JUSTICE SYSTEM 121 (2019) (explaining that "there is little doubt that both general and pretrial risk assessment instruments rely on static risk factors"—"such as age, sex, marital status, education level, employment history, and financial status"—"that are statistically associated with race and ethnicity"); Angele Christin et al., *Courts and Predictive Algorithms*, DATA & CIVIL RIGHTS: A NEW ERA OF POLICING AND JUSTICE, DATACIVILRIGHTS.ORG (Oct. 27, 2015), https://perma.cc/DA7Z-KVR5 (PDF) (arguing that, "[r]egardless of their impact, the very method used to build these algorithms might make them unconstitutional" because, even though "[n]one of the sentencing instruments use race as a variable, . . . many variables included in the models play the role of 'proxies' for race, in that they strongly correlate with race and reflect racial bias"); Bernard E. Harcourt, *Risk as a Proxy for Race: The Dangers of Risk Assessment*,

Even if including these factors leads to more accurate predictions, many consider it morally or politically repugnant to use them in decisions affecting individuals' futures because they lead to negative outcomes disproportionately affecting certain races.[85]

In addition to these race-based criticisms, one might argue that, in achieving greater uniformity and fairness across cases, the system is sacrificing fairness in individual cases. This is the same criticism lodged against other attempts to achieve system-wide fairness, such as the mandatory guideline sentencing regimes of the 1980s, 1990s, and early 2000s.[86] Requiring judges to impose pre-set punishments for particular crimes meant that judges often could not tailor offenders' sentences to their individual circumstances or the particulars of the committed offense.[87] According to many, this resulted in great injustices.[88] Attempts to achieve uniformity among cases often translates into not being able to individualize the sentence or other criminal justice outcome in the particular case at bar.[89] In some sense, then, fairness across cases comes at the price of fairness within an individual case.

---

27 FED. SENT'G REP. 237, 237 (2015); Kelly Hannah-Moffat, *Actuarial Sentencing: An "Unsettled" Proposition*, 30 JUST. Q. 270, 279–84 (2013).

85. *See supra* note 84 and accompanying text.

86. *See* Albert W. Alschuler, *The Failure of Sentencing Guidelines: A Plea for Less Aggregation*, 58 U. CHI. L. REV. 901, 920 (1991) ("Guidelines designed to promote equality have produced unequal results—results that scatter years of imprisonment almost by lottery. These results would have been inconceivable in the old regime of discretionary sentencing."); Don J. DeBenedictis, *How Long Is Too Long?*, 79 A.B.A. J. 74, 74 (1993) ("Critics charge that mandatory sentences, by denying use even of the guidelines' adjustments and departures, prevent judges from considering a defendant's individual circumstances or culpability. Mandatory minimums are inherently unfair, they say, because they force judges to sentence crimes, not criminals."); David Yellen, *What Juvenile Court Abolitionists Can Learn from the Failures of Sentencing Reform*, 1996 WIS. L. REV. 577, 587 (1996) ("Judges throughout the country complain that some sentencing guidelines and virtually all mandatory minimum statutes force them to impose unjust sentences because the judges are precluded from considering the unique circumstances of offenders.").

87. *See* Yellen, *supra* note 86, at 587.

88. *See* MICHAEL TONRY, MALIGN NEGLECT: RACE, CRIME, AND PUNISHMENT IN AMERICA 167–70 (1995); Alschuler, *supra* note 86, at 920; DeBenedictis, *supra* note 86, at 74; Yellen, *supra* note 86, at 587.

89. *See supra* notes 87–88 and accompanying text.

For example, one of these programs might find that, in general, a single man who has not received a high school diploma (and who happens to be black) is more likely to recidivate than a married man who has graduated from college (and who happens to be white). But that does not mean that a *particular* single man who has not received a high school diploma may be more likely to recidivate than anyone else. One might say that his race—even though not specifically being taken into account—is being held against him because it correlates with his marital status and educational level. This is a valid criticism, but it is of course true that, regardless of race or any other factor, these predictions of future dangerousness, or anything else, are only risk assessments.[90] They are generalizations based on the limited data available.[91]

Beyond these race- and individualization-based criticisms, some commentators have argued that these criminal justice programs are not as accurate as they might seem anyway.[92] First, the predictions the programs generate are only as good as the data on which they rely.[93] As Professors Wayne Logan and Andrew Ferguson have explained, there are numerous sources of error involved with both the collection and generation of this data.[94] Relatedly, there are questions about the accuracy of the algorithms' and source codes' outputs. In certain studies, some of these prediction programs' results have proved to be only about as

---

90. *See* Sam Corbett-Davies et al., *supra* note 51.

91. *See id.*

92. *See, e.g.*, Starr, *supra* note 52, at 842 ("The instruments' first serious limitation is that they do not provide anything even approaching a precise prediction of an individual's recidivism risk."); Angwin et al., *supra* note 42 ("When a full range of crimes were taken into account—including misdemeanors such as driving with an expired license—the algorithm was somewhat more accurate than a coin flip. Of those deemed likely to re-offend, 61 percent were arrested for any subsequent crimes within two years.").

93. *See* Elizabeth E. Joh, *Feeding the Machine: Policing, Crime Data, & Algorithims*, 26 WM. & MARY BILL RTS. J. 287, 294 (2017) (explaining that "algorithmic decisionmaking has been subjected to the 'garbage in, garbage out' critique: that any decision is as good or as bad as the data relied upon by the program").

94. *See generally* Wayne A. Logan & Andrew Guthrie Ferguson, *Policing Criminal Justice Data*, 101 MINN. L. REV. 541 (2016) (summarizing the numerous sources of error associated with data used within the criminal justice system).

accurate as outcomes based purely on chance.[95] For example, in 2016, *ProPublica* investigated the "largely hidden effect of algorithms in American life" and found risk assessment measures to be "remarkably unreliable."[96] In particular, *ProPublica* gathered risk assessment scores assigned to a large sample of arrestees in Broward County, Florida.[97] It then examined how many of these arrestees "were charged with new crimes over the next two years, the same benchmark used by the creators of the [COMPAS] algorithm."[98] *ProPublica* determined that, "when a full range of crimes were taken into account . . . the algorithm was [only] somewhat more accurate than a coin flip. Of those deemed likely to re-offend, 61 percent were arrested for any subsequent crimes within two years."[99] These findings have raised serious questions about the accuracy of at least Northpointe's program.[100]

Additionally, many people commonly understand risk assessment programs as predicting a defendant's risk of future dangerousness; in reality, however, a number of these programs instead only *order* defendants by their risks of future

---

95. *See* Angwin et al., *supra* note 42; *see also* Ferguson, *supra* note 37, at 1144 (stating in reference to predictive policing programs that, "[l]ike an old-school weather forecast, the data can provide localized forecasts—'cloudy with a chance of murder'—with a significant degree of variability and fallibility").

96. *See* Angwin et al., *supra* note 42.

97. *See id.*

98. *Id.*; *see also* NORTHPOINTE, *supra* note 51, at 27 (2015), https://perma.cc/A665-WHGU (PDF) ("The recidivism risk scale was developed to predict new offenses subsequent to the COMPAS assessment date. The outcome used for the original scale construction was a new misdemeanor or felony offense within two years of the COMPAS administration date."), *cited in* Angwin et al., *supra* note 42.

99. Angwin et al., *supra* note 42. A study by the founders of Northpointe concluded that the predictive validity of the algorithm was around seventy to eighty percent and that its reliability hovered around seventy percent. *See* Tim Brennan et al., *Evaluating the Predictive Validity of the COMPAS Risk and Needs Assessment System*, 36 CRIM. JUST. & BEHAV. 21, 31–34 (2009).

100. It seems that there are a number of shortcomings to *ProPublica*'s study, however, including sample size, sample breadth, and potential confounding variables. *See* Angwin et al., *supra* note 42. Further, *ProPublica*'s study focused on just one risk assessment algorithm—Northpointe's COMPAS. Although this system is widely employed, it is not the only algorithm in use and thus cannot alone condemn all risk assessment algorithms.

dangerousness.[101] Imagine that you have one group of defendants who range from a ten percent chance of recidivating to a sixty percent chance of recidivating and another group of defendants who range from a two percent chance of recidivating to a ten percent chance of recidivating. The program would score an equal number of defendants within each group as having a high risk of future dangerousness, and it would score an equal number within each group as having a low risk of future dangerousness.[102] In other words, the scores are curved depending on the other members within the defendant group. This means that the intended "accuracy" in this context relates to the accuracy of the ordering rather than the accuracy of a risk-of-recidivism calculation. Such an approach is generally much less useful if sentencing and parole decisions are to be based on true risks of recidivism rather than on, for example, the availability of resources like empty prison beds.[103]

---

101. *See, e.g.*, NORTHPOINTE, COMPAS RISK & NEED ASSESSMENT SYSTEM: SELECTED QUESTIONS POSED BY INQUIRING AGENCIES, at 5 (2012), https://perma.cc/73A6-2TK7 (PDF) (describing how COMPAS scores and ranks individuals).

102. *See, e.g.*, *id.*; *see also* Sandra G. Mayson, *Bias In, Bias Out*, 128 YALE L.J. 2218, 2246 (2019) (explaining that a popular measure of risk assessment tools' performance is "area under the curve," which "conveys the probability that, for any two people selected at random in the data, the algorithm will correctly *order* them in terms of risk" (emphasis added)); Sandra G. Mayson, *Dangerous Defendants*, 127 YALE L.J. 490, 513 (2018) (explaining that "[a] classification as high risk does not assert that Person A will fail to appear or be rearrested unless restrained" but instead only "purports to . . . rank Person A relative to the rest of the population upon which the instrument was developed"); *cf.* Jessica M. Eaglin, *Constructing Recidivism Risk*, 67 EMORY L.J. 59, 87 (2017) (explaining that "[t]ranslating tool outcomes into risk categories is a highly subjective, policy-oriented process" and that "[t]his decision requires some expertise not only in what the tool is predicting, but also in how society interprets the numerical outcome's meaning": "In short, where developers place cut-off points reflects a normative judgment about how much likelihood of risk is acceptable in society without intervention.").

103. If the availability of resources like empty prison beds is to be a significant factor in these determinations, this might be a reason to find a set number or percentage of low-risk or high-risk defendants regardless of the true risk of the defendant.

In general, there has been little investigation into the accuracy of risk assessment computer programs.[104] The few researchers assessing these programs are generally the programs' developers themselves, who obviously have conflicts of interest; they have financial and reputational interests in the popularity and wide acceptance of the programs.[105] Still, many jurisdictions have already adopted these programs,[106] and many more are considering adopting them in the future.[107] They have often done so without fully understanding or testing the accuracy of the results produced by the programs.

III. Conviction Programs

Critics have been pushing back against prediction programs used for bail, sentencing, and parole, but they have largely overlooked the use of computer programs for obtaining convictions. As courts and parole boards have, over the years, been increasingly relying on computer programs to aid in criminal justice decisionmaking, police officers, forensic scientists, and prosecutors have quietly been relying on computer programs to produce various forms of incriminating evidence.[108] Longstanding examples of this include evidence created by breathalyzers and AFISs.[109] Further, the criminal justice system's reliance on conviction programs has reached into a new era wherein actors rely on evidence produced by, for example, probabilistic genotyping

---

104. *See* Angwin et al., *supra* note 42 ("There have been few independent studies of these criminal risk assessments.").

105. *See id.*

106. *See id.* (noting that "many jurisdictions have adopted Northpointe's software before rigorously testing whether it works").

107. *See, e.g.*, Jolie McCullogh, *Courts Have Called Texas Bail Practices Unconstitutional. Will That Push This Year's Reform Efforts to Success?*, TEX. TRIB. (Feb. 4, 2019), https://perma.cc/8EXT-XSZY (last visited Oct. 3, 2019) ("[Texas] State Sen. John Whitmire, D-Houston, and state Rep. Andrew Murr, R-Junction, announced Monday at the Capitol that they have again filed legislation that would implement a risk-assessment tool for judges to use when making bail decisions, among other proposals.") (on file with the Washington and Lee Law Review).

108. *See infra* Part III.A.

109. Some other examples include radar guns and lidar detectors.

systems (PGSs).[110] Although many of these technologies have escaped effective and arresting criticism, they are actually more pernicious than the prediction programs that are under attack. Conviction programs are different from prediction programs in important ways, including that prosecutors and experts regularly present them as having the imprimatur of science and that more is simply at stake when the question is one of innocence rather than one of temporary pretrial confinement or punishment for those already determined guilty.[111]

A. An Array of Conviction Programs

Prosecutors, judges, and juries today rely on a wide range of evidence to convict criminal defendants. Much of this evidence is produced by scientific and technological research that is captured in generally inaccessible computer programs and their underlying algorithms and source codes. Some of these technologies, like breathalyzers and AFISs, have been around for decades,[112] while others, like PGSs, are new and emerging developments.[113] The criminal justice actors who turn to these technologies for damning evidence of guilt generally blindly rely on these programs and unquestioningly accept their outputs. This may not be surprising considering that the technologies are complicated and are viewed in light of the objectivity and verifiability of science. But it raises the question of whether these programs are quite as accurate as they seem to be.

---

110. *See* Kirchner, *supra* note 42 (noting that TrueAllele, a PGS, was first used in a criminal case in 2009).

111. *See infra* Part III.B.

112. *See infra* Part III.A.1.

113. One might classify these technologies as "[l]itigation-[r]elated [g]adgetry and [s]oftware." Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 2013–20 (2017).

1. Breathalyzers[114] and Automated Fingerprint Identification Systems

Criminal justice actors regularly employ computer programs in carrying out their duties, and, in many areas, they have relied on these same technologies for decades.[115] For example, when a police officer pulls over a suspected drunk driver, he often has the driver blow into a breathalyzer machine to determine the driver's blood or breath alcohol content.[116] In all states, a reading of 0.08 or higher is, alone, a ground for a driving-while-intoxicated conviction, regardless of whether the driver's behavior suggested that he was impaired.[117] The breathalyzer reading is based on an internal algorithm and underlying source code that are generally unknown by both the police officer and the driver. Similarly, when a forensic scientist tries to use an AFIS to match a latent print found at a crime scene to a known print in a law enforcement database, she employs a computer program generally developed by an independent company.[118] As with the breathalyzer operator, the fingerprint examiner is generally unaware of how the algorithm determines whether the prints match and the underlying source code implementing that calculation.[119] Yet, compared to the recent focus on prediction programs, commentators have given relatively little attention to reliance on these technologies within the criminal justice system.[120] This is despite the fact that the same

---

114. Throughout this article, I use the term "breathalyzer" in a generic sense. There have historically been many breathalyzer devices, such as the Drunk-O-Meter, Intoxilyzer, and the Breathalyzer, itself.

115. *See supra* note 109 and accompanying text.

116. Blood alcohol content is calculated by first measuring the breath alcohol content in the provided breath sample.

117. *See Blood Alcohol Concentration Limits for Enforcement of Impaired Driving Laws—U.S. States—2001*, ALCOMETERS, https://perma.cc/G9XL-3HA5 (last visited Mar. 9, 2019) [hereinafter *Blood Alcohol Concentration Limits*] (listing criminalized blood alcohol concentration levels by state) (on file with the Washington and Lee Law Review).

118. *See* Interview with James Loudermilk, Senior Director for Innovation and Customer Solutions, IDEMIA Nat'l Sec. Sol'ns (July 15, 2019).

119. *See id.* The FBI declined to comment on this. *See* E-mail from Jeffrey Heinze, Supervisory Special Agent, Office of Public Affairs, FBI, to author (Feb. 3, 2020, 08:50 CST) (on file with author).

120. *See supra* Part II.C–D.

concerns of accuracy exist in the conviction context as in the prediction context.[121] With respect to conviction programs, the allure of relying on computerized, "scientific" justice is strong, just like in the context of prediction programs.[122] These programs offer an air of fairness, consistency, and accuracy by operating according to set algorithms and source codes that are thought to be built on sound research.[123] In reality, though, there may be insufficient research or validation studies propping up many of these programs or the algorithms and source codes on which they are built.[124] Instead, many of these technologies, have, in a sense, been grandfathered into the current system. The problem is that these technologies are not being seriously questioned. Judges, prosecutors, defense attorneys, and other actors within the criminal justice system often blindly accept these technologies as accurate and reliable evidence supporting convictions. That hardly anyone is seriously questioning these technologies is disquieting.

2. New Technology: Probabilistic Genotyping Systems

Commentators have paid significantly more attention to criminal justice actors' recent use of the cutting-edge technology of PGSs. Today, prosecutors regularly rely on DNA tests and analyses to secure convictions in court.[125] In fact, some prosecutors complain that, because jurors are so used to seeing DNA evidence on television shows like *CSI: Crime Scene Investigation*, they often demand DNA evidence before voting to convict, even if DNA

---

121. *See supra* Part II.D.

122. *See supra* Part II.C.

123. *See* Katherine Kwong, Note, *The Algorithm Says You Did It: The Use of Black Box Algorithms to Analyze Complex DNA Evidence*, 31 HARV. J.L. & TECH. 275, 276 (2018) (explaining there is not enough information released to determine the fairness of these algorithms and source codes).

124. *See infra* notes 206–226 and accompanying text; *cf.* Ryan, *supra* note 14 (discussing the insufficiency of research supporting fingerprint matching).

125. Prosecutors rely on DNA analyses employing complex statistical techniques to secure convictions, but these programs are also sometimes used to exonerate those who have been wrongfully convicted. In fact, TrueAllele—one of these programs—was recently employed to free a wrongfully convicted man. *See* Kirchner, *supra* note 42.

evidence is not available in the case.[126] Even if DNA evidence *is* found at a crime scene, on a victim, or in some other incriminating location, though, it sometimes may be in a state too contaminated or diluted for analysis.[127] Additionally, DNA that has not been properly preserved generally becomes ineligible for analysis after a week, and, depending on where the DNA came from, maybe sooner.[128] More problematic today, a DNA quantity on the order of picograms is ordinarily necessary for examination.[129] Further, a DNA sample that is comprised of multiple contributing DNA samples may not be ripe for analysis because it is difficult to disaggregate which DNA alleles belong to which contributors.[130] In recent years, though, researchers have developed computer programs to run statistical analyses on these types of low-level and mixed samples so that analysts can determine the probability that any particular individual was a contributor to the DNA sample at

---

126. *See* Tom R. Tyler, *Viewing CSI and the Threshold of Guilt: Managing Truth and Justice in Reality and Fiction*, 115 YALE L.J. 1050, 1050 (2006) (explaining that "the 'CSI effect' is a term that legal authorities and the mass media have coined to describe a supposed influence that watching the television show *CSI: Crime Scene Investigation* has on juror behavior" and that the supposed effect is "that jurors who see the high-quality forensic evidence presented on *CSI* raise their standards in real trials, in which actual evidence is typically more flawed and uncertain" and that, "[a]s a result, these CSI-affected jurors are alleged to acquit defendants more frequently").

127. *See* William C. Thompson et al., *Forensic DNA Statistics: Still Controversial in Some Cases*, CHAMPION, Dec. 2012, at 12 ("When labs try to 'type' samples that contain too little DNA, or DNA that is too degraded, the results of the DNA test can be unreliable.").

128. *See* Karl M. McDonald, *DNA Forensic Testing and Use of DNA Rape Kits in Cases of Rape and Sexual Assault*, FORENSIC MAG. (Jan. 26, 2015, 8:21 AM), https://perma.cc/8XT4-6M7G (last visited Oct. 4, 2019) (on file with the Washington and Lee Law Review). DNA from fingernail scrapings is generally viable for two days, as is DNA from skin-to-skin contact. *Id.* DNA from a penis can be viable for about twelve hours. *Id.* And "[f]ibers of anything put on the head can last up to seven days." *Id.*

129. *See* Roland A.H. van Oorschot et al., *Forensic Trace DNA: A Review*, 10 INVESTIGATIVE GENETICS 3 (2010) (stating that "[t]race DNA typically refers to either the very limited and/or invisible biological samples and/or amounts of DNA less than 100 pg" but that "some laboratories use a 200 pg limit as the threshold limit"); *cf.* JOHN M. BUTLER, FUNDAMENTALS OF FORENSIC DNA TYPING 111 (2010) ("Typically 0.5 to 2.10 ng of input human DNA is optimal with current commercial STR kits."). A picogram = 1×10^{-12} grams.

130. *See* William C. Thompson et al., *supra* note 127, at 12, 14.

issue.[131] Forensic analysts in the United States primarily use TrueAllele and STRmix for this purpose, but other programs exist as well.[132]

When DNA analysts cannot discern which "peaks and valleys" produced by their testing should be paired together because they belong to one individual and not to the others whose DNA is also present in the sample, TrueAllele and STRmix have the ability to further the evaluation.[133] These programs run statistical analyses, "calculat[ing] the probability of the peak heights [in the DNA profile] given all the possible genotype combinations for the individual contributors."[134] Accordingly, TrueAllele and STRmix purportedly can assess the probability that the sample contains the DNA of an individual with a known DNA profile.[135] But, because an algorithm embedded in a computer program formulates

---

131. *See* Michael D. Coble & Jo-Anne Bright, *Probabilistic Genotyping Software: An Overview*, 38 FORENSIC SCI. INT'L: GENETICS 219, 221 (2019). TrueAllele was first used for forensic analysis in the late 1990s, *see History*, CYBERGENETICS, https://perma.cc/J2SK-NKHU (last visited May 24, 2017) (on file with the Washington and Lee Law Review), and was first used in a criminal case in 2009, *see* Kirchner, *supra* note 42. Coming onto the scene somewhat later, STRmix was first used for casework in August of 2012. *See What Can STRmix Do?*, STRMIX, https://perma.cc/789D-2AW2 (last visited Oct. 27, 2019) (on file with the Washington and Lee Law Review).

132. These are "probabilistic genotyping" programs. Kirchner, *supra* note 42. Analysts employ these programs when working with evidence that includes DNA mixtures—those containing DNA from multiple individuals. *See* Logan Koepke, *Should Secret Code Help Convict?*, CRIM. JUST., Mar. 24, 2016 ("TrueAllele Casework is a proprietary computer program that parses DNA *mixtures*—samples that include genetic code from more than one person.").

133. *See* Coble & Bright, *supra* note 131, at 220–21; Keopke, *supra* note 132 (explaining that "TrueAllele looks to pick up where most forensic labs would leave off").

134. *See* Coble & Bright, *supra* note 131, at 221 ("These models take the quantitative information from the DNA profile and calculate the probability of the peak heights given all the possible genotype combinations for the individual contributors."); *see* Koepke, *supra* note 132. As Logan Koepke has explained with respect to TrueAllele, these programs "compare the actual DNA data to different statistical models, weighing the probability that the data matches the model," and they "do[] this by examining 100,000 different *combinations* of possible variables and how well each proposed variable might explain the DNA data." Koepke, *supra* note 132.

135. *See* Koepke, *supra* note 132 ("Essentially, algorithms compare the actual DNA data to different statistical models, weighing the probability that the data matches the model.").

the analysis, and because the underlying source code carries out the calculations, the details of the process are largely unknown to the DNA analysts employing the program.[136] Not surprisingly, the criminal defendants involved, as well as their lawyers, are similarly generally unaware of how these PGSs reach their advanced match determinations.

Despite criminal justice actors' lack of understanding about the intricacies of these PGSs, uses of TrueAllele and STRmix analyses to support criminal convictions have skyrocketed.[137] As of April 2015, TrueAllele evidence had been used to convict criminal defendants "in over 500 cases . . . with the majority of those convictions occurring during the previous full year."[138] Prosecutors are also using STRmix to secure convictions,[139] although the numbers are less clear here, as STRmix is relatively new to the field. Although STRmix was first admitted in a U.S. court in only December 2015,[140] some jurisdictions are already switching from

---

136. As Michael Coble and Jo-Anne Bright have stated, the "software should not be treated as a 'black box' where something magical happens to generate the statistic." Coble & Bright, *supra* note 131, at 223. "It is imperative the end user understand the underlying mathematics (at least to a conceptual level), assumptions, models and limitations of the software program to convey how the program works to the trier of fact." *Id.* This is a challenge, though, as many examiners have been trained to analyze DNA using a different framework. *See id.* ("Transitioning to the [Likelihood Ratio] and understanding the nuances of building relevant propositions based upon case scenarios can be challenging to users accustomed to a frequentist view of probability.").

137. *See* Darlene Dang, *DNA Software Claims to Prevent Wrongful Convictions, but Lacks Third-Party Validation*, HUFF. POST (Apr. 7, 2016, 4:40 PM), https://perma.cc/Q7WU-2DB9 (last updated Apr. 7, 2017) (last visited Oct. 4, 2019) ("This groundbreaking technology helped convict criminals in over 500 cases in the past five years, with the majority of those convictions occurring last year.") (on file with the Washington and Lee Law Review).

138. *Id.*

139. *See* Kirchner, *supra* note 42 ("The U.S. Army and the FBI use STRmix . . . as do several public crime labs across the nation.").

140. *See* John S. Hausman, *Michigan Judge's Landmark DNA Ruling Could Revolutionize CSI Work*, MLIVE (Dec. 23, 2015), https://perma.cc/PKN6-SWXQ (last updated Jan. 19, 2019) (last visited Oct. 27, 2019) (referring to STRmix and stating that "a Michigan judge has made the nation's first ruling on a new approach to analyzing DNA results that could revolutionize crime-scene investigation and court cases") (on file with the Washington and Lee Law Review).

TrueAllele to STRmix, so STRmix's numbers are already on the rise.[141]

B. The Especially Troubling Nature of Conviction Programs

Conviction programs like those powering breathalyzers, AFISs, and PGSs are fundamentally different from the prediction programs that critics continue to attack and that have received more significant attention. Prediction programs focus on human behavior—roughly assessing the probability that a particular offender will, for example, recidivate.[142] Conviction programs, on the other hand, do not focus on behavior in this way. Instead, they measure in some approximate sense the probability that the individual in question has a particular biological characteristic. What is the blood or breath alcohol content of the defendant? What are the characteristics—the "minutiae"—of the defendant's fingerprints? Are his alleles the same as the alleles found in the DNA sample found at the crime scene? Whereas prediction programs draw on the social sciences—they are supposedly based on studies about how certain past conditions have affected human behavior[143]—conviction programs at least purportedly draw from the hard sciences. DNA analysis is the best example of this; it is the "gold standard" for modern-day forensic evidence.[144] The study of DNA grew out of the biology, chemistry, and biochemistry departments of universities.[145] And scientists across the globe

---

141. *See* Kirchner, *supra* note 42 ("New York City's Office of the Chief Medical Examiner recently announced that it will switch to STRmix in 2017.").

142. *See supra* Part II.A.

143. *See, e.g.*, NORTHPOINTE, *supra* note 51, at 26–46 (describing the social science underlying the secret prediction algorithm embedded in COMPAS).

144. *See* DONALD E. SHELTON, FORENSIC SCIENCE EVIDENCE: CAN THE LAW KEEP UP WITH SCIENCE? 190 (2012) ("The prosecution use of DNA in criminal cases has become the new 'gold standard' of criminal identification techniques."); NAT'L ACADEMY OF SCI., STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 130 (2009) (stating that DNA is "the standard against which many other forensic individualization techniques are [now] judged"). *But see* ERIN MURPHY, INSIDE THE CELL: THE DARK SIDE OF FORENSIC DNA xii (2015) (explaining that, although DNA offers "innumerable benefits" for the criminal justice system, caution must be used in employing and relying on DNA analysis).

145. *See* NAT'L ACADEMY OF SCI., *supra* note 144, at 130; *see also* Meghan J.

study DNA and related areas. To the average person, however, DNA analysis is cloaked in mystery. With prosecutors' arguments and experts' testimony often providing random match probabilities smaller than one in several billion or trillion,[146] DNA evidence seems almost bullet-proof. But, in the difficult DNA cases—those involving low-level samples or complex mixtures of multiple individuals' DNA and thus requiring PGS analysis—underneath those probabilities are the algorithms and source codes of the computer programs calculating the relevant statistics. And the forensic examiner ordinarily is unaware of the nuances of these algorithms and source codes.

Although it is no secret that there is some uncertainty in prediction, the way that prosecutors present evidence related to conviction is often on the level of certainty.[147] For example, fingerprint examiners, whose conclusions are often based on AFIS outcomes, generally testify as to whether there is a "match" or "no match" rather than testifying about the probability that the fingerprint found at the crime scene came from the criminal defendant in the case.[148] This level of certainty by examiners is rampant in the areas of forensic study.[149] Similarly, onlookers

---

Ryan, Miranda*'s Truth: The Importance of Adversarial Testing and Dignity in Confession Law*, 43 N. KY. L. REV. 413, 428 (2017) ("DNA evidence is thought to be incredibly reliable, due in part to its development from the research culture of universities . . . .").

146. *See* BUTLER, *supra* note 129, at 247, 251.

147. *See* Joseph B. Kadane & Jonathan J. Koehler, *Certainty & Uncertainty in Reporting Fingerprint Evidence*, DAEDALUS, Fall 2018, at 120 ("Although the ACE-V process is subjective, fingerprint examiners have historically claimed that their identifications are 100 percent certain, and that there is virtually no chance that an error has occurred.").

148. *See* NAT'L ACADEMY OF SCI., *supra* note 144, at 141–42 (explaining that "SWGFAST has promulgated three acceptable conclusions resulting from latent print comparison: individualization (or identification), exclusion, or inconclusive" and that, "when a latent print examiner testifies that two impressions 'match,' they are communicating the notion that the prints could not possibly have come from two different individuals"). *But cf. Guideline for the Articulation of the Decision-Making Process Leading to an Expert Opinion of Source Identification in Friction Ridge Examinations (draft)*, ORG. OF SCI. AREA COMMS. FOR FORENSIC SCI., at 9–10, https://perma.cc/F8SX-WGSY (PDF) (providing that the examiner's level of confidence in a fingerprint identification determination "shall not be reported in absolute terms and should not be reported numerically").

149. *See* Danielle Weiss & Gerald Laporte, *Uncertainty Ahead: A Shift in How*

often perceive DNA evidence as iron-clad, indisputable evidence against the accused.[150] Although DNA analysts will testify about the probability that a random individual's DNA would match the sample DNA found at the crime scene or in another potentially incriminating location, these estimates do not take into account the chance that there was a mistake in the lab or that leaving DNA at the crime scene does not necessarily mean guilt.[151] Further, these DNA experts' probability statements are so significant that factfinders regularly consider them conclusive.[152] This is in addition to decisionmakers regularly falling prey to the prosecutor's fallacy, whereby they mistake the random match probability with the probability that the defendant is not guilty.[153]

Federal Scientific Experts Can Testify, 279 NAT'L INST. OF JUST. J. 1, 1 (2018) (explaining that, for decades, scientific experts have asserted that their expert opinions are to a "reasonable degree of scientific certainty").

150. *See* Kadane & Koehler, *supra* note 147, at 120–21.

151. *See* Meghan J. Ryan, *The Privacy, Probability, and Political Pitfalls of Universal DNA Collection*, 20 SMU SCI. & TECH. L. REV. 3, 18 (2017); Meghan J. Ryan, *Remedying Wrongful Execution*, 45 U. MICH. J.L. REFORM 261, 274 n.89 (2012) ("[W]hile DNA evidence can be 'uniquely probative' of a defendant's innocence, it is not conclusive. For example, the defendant may not have left behind any of his DNA, and the trace DNA evidence examined could belong to his partner or an innocent individual." (internal citations omitted)); Ryan & Adams, *supra* note 63, at 1083 ("Errors can still occur with respect to DNA evidence. . . . For example, laboratory tests can be mislabeled or contaminated, and an analyst could make a mistake or even possibly fabricate results."); Ryan, *supra* note 145, at 430 (explaining that "there can be cross-contamination in the laboratory, the forensic scientist may err in running the samples or interpreting the results, or the forensic scientist may lie about the results"). Appropriate testimony on the part of the prosecutor would refer to "the probability of selecting the observed profile from a population of random unrelated individuals . . . based on the alleles present in [the] sample" rather than the "chance that the DNA profile came from someone else" or the "chance that a defendant is not guilty." *See* BUTLER, *supra* note 129, at 251. The latter two approaches are known as the prosecutor's fallacy. *See id.* (providing examples of the prosecutor's fallacy, such as stating that "there is only a 1 in 15,000 chance that the defendant is not guilty").

152. *See* BUTLER, *supra* note 129, at 2 ("Thousands of cases have been closed with guilty suspects punished and innocent ones freed because of the power of a silent biological witness at the crime scene."); Kadane & Koehler, *supra* note 147, at 120–21.

153. *See* James S. Liebman et al., *The Evidence of Things Not Seen: Non-Matches as Evidence of Innocence*, 98 IOWA L. REV. 577, 615 (2013)

Prosecutors' presentations of conviction program evidence as virtually infallible is especially troubling considering that arguably more is at stake with conviction programs. Unlike the prediction programs used to make bail, sentencing, and parole decisions, conviction programs affect determinations of guilt and innocence. In this regard, convicting an innocent person is often considered more concerning than imposing, for example, an inaccurate or unjust sentence.[154] Bail, sentencing, and parole decisions are of course important. They affect who is detained and how severely an offender is punished. In this sense, they potentially affect an individual's liberty and the stigma attached to detention and punishment severity. But they do not go to the heart of conviction. Certainly, unjust sentences are deeply undesirable, but a sentence that is too harsh is arguably not as terrible as wrongly convicting an innocent person.[155] In this sense, decisions about conviction are more important than sentencing decisions.[156] Similarly, a person who has been arrested and denied bail may have a more difficult time preparing for trial than someone who has not been denied bail, and this may negatively affect this individual's probability of being convicted.[157] But the

---

(describing the prosecutor's fallacy).

154. This is debatable, and other commentators do not agree with me on this point. I think that wrongful conviction is a greater wrong than a sentence that is too harsh because, with wrongful conviction, the defendant is completely innocent, whereas, with too harsh of a sentence, the defendant is a wrongdoer and has run afoul of the law in some way. Still, certain defendants will almost certainly disagree with this point. To some defendants, especially guilty repeat offenders, the sentence is the most important aspect of a criminal proceeding. They have already committed the crime, and now they just want to do their time and get out. Regardless of whether wrongful conviction is a worse wrong than imposing too harsh of a punishment, though, wrongful conviction remains a problem and the computer programs that create risks of wrongful convictions are similarly problematic.

155. *See supra* note 154 (explaining this point further and noting that it is debatable).

156. *See supra* note 154 and accompanying text (noting that this is debatable and that acceptance of this proposition is not central to this Article's thesis).

157. *See* Melanie D. Wilson, *The Price of Pretrial Release: Can We Afford to Keep Our Fourth Amendment Rights?*, 92 IOWA L. REV. 159, 194 (2006) ("Because the judge's decision to detain an arrested person has the capacity to alter her ability to prepare her case for trial and, thereby, impair a defendant's fair-trial process, pretrial waivers used to gain pretrial freedom are important.").

denial of bail likely does not have as great of an impact on conviction than, say, DNA evidence implicating the defendant. Indeed, DNA evidence, breathalyzer results, and fingerprint matches are ordinarily particularly damning evidence in a case.[158] One significant reason for this is that each of these types of evidence is often viewed as incredibly reliable and accurate, rooted in science, and providing valid, objective evidence of guilt.[159]

IV. Accuracy and Secrecy Intertwined

Although much is at stake where convictions are involved, and although prosecutors regularly present evidence produced by conviction programs as nearly indisputable, there are real questions about the accuracy of the outputs that these conviction programs produce and that prosecutors rely on so heavily today.

---

158. *See* JOHN BUGLIOSI, THE ART OF PROSECUTION: TRIAL ADVOCACY FUNDAMENTALS FROM CASE PREPARATION THROUGH SUMMATION 12 (2000) ("DNA has surpassed fingerprints as the single most damning evidence in a criminal case."); Aurora J. Wilson, *Discovery of Breathalyzer Source Code in DUI Prosecutions*, 7 WASH. J.L. TECH. & ARTS 121, 122 (2011) ("Breathalyzer test results commonly provide critical evidence in cases involving charges for driving under the influence (DUI) or driving while intoxicated (DWI)."); Michael Specter, *Do Fingerprints Lie?*, NEW YORKER (May 19, 2002), https://perma.cc/CW8D-MS7X (last visited Oct. 17, 2019) (explaining that the current culture is that, if "[y]ou are indicted on the basis of a fingerprint . . . [y]ou are [no longer] innocent till proven guilty" and that, "if the police have a print, you are assumed to be guilty") (on file with the Washington and Lee Law Review).

159. *See* NAT'L ACAD. OF SCI., *supra* note 144, at 130 ("[D]NA typing is now universally recognized as the standard against which many other forensic individualization techniques are judged. DNA enjoys this preeminent position because of its reliability and the fact that, absent fraud or an error in labeling or handling, the probabilities of a false positive are quantifiable and often miniscule."); BUGLIOSI, *supra* note 158, at 12; (describing DNA evidence as "damning evidence in a criminal case"); MURPHY, *supra* note 144, at 85 (stating that, with respect to DNA, "[m]any jurors, and even legal officials, hear the word *match* as synonymous with *case closed*"); SHELTON, *supra* note 144, at 190 (describing DNA evidence as "the new 'gold standard' of criminal identification techniques" because it has "a firm scientific foundation established outside of the context of criminal litigation"); Specter, *supra* note 158 ("For more than a century, the fingerprint has been regarded as an unassailable symbol of truth, particularly in the courtroom. When a trained expert tells a judge and jury that prints found at a crime scene match those of the accused, his testimony often decides the case.").

For the most part, simply more research must be done to determine whether these technologies produce accurate information on which convictions should fairly be based.[160] Even if the developers of these technologies were aware of inaccurate outputs, or of *potential* inaccurate outputs, though, one wonders whether they would be forthcoming about such defects, knowing that such revelations could cause their revenues from these lucrative business products to plummet. In any case, the incredible secrecy surrounding use of these programs currently masks any answers that could be gleaned by more closely examining these technologies. Shielding these conviction programs from public—and even legal and scientific—scrutiny translates into a situation in which criminal defendants are being convicted based on evidence that has not been clearly established as accurate. Burgeoning secrecy in the law generally, and laypersons' misunderstandings and acceptance of evidence presented as science, further exacerbate this concern of unchallenged evidence in criminal cases.

A. The Interconnected Problems of Accuracy and Secrecy

The accuracy of evidence presented at trial—especially that presented as "scientific" evidence—is important for the proper working of, and faith in, our criminal justice system.[161] Where computerized programs used for conviction are concerned, there are significant questions about whether the programs' outputs are accurate and useful figures on which legal decisionmakers should rely in assessing guilt and innocence. These questions about accuracy are difficult to resolve, as the details of the programs—the underlying algorithms and source codes—are generally kept under lock and key by the companies that created them and license them for government use in convicting criminal

160. *See, e.g.*, Ryan, *supra* note 14 (describing how the discipline of fingerprint matching is severely wanting for a scientific foundation and setting forth some necessary research that scientists and lawyers must conduct to shore up the practice).

161. *See id.* ("Avoiding wrongful convictions—based on fingerprint or even other questionable evidence—is critical, but one should not overlook the importance of punishing guilty offenders. The legitimacy of criminal law depends on it.").

defendants. This secrecy, paired with the pending accuracy questions, is incredibly problematic.

1. Breathalyzers

Breathalyzers are a common example of a mainstream technology for which there are real questions about accuracy. And the secrecy surrounding the technology, as well as judicial refusal to carefully examine whether breathalyzers produce valid readings, exacerbate these accuracy questions. In most jurisdictions today, defendants can be convicted of a driving-under-the-influence (DUI) or driving-while-intoxicated (DWI) offense by simply blowing a certain value on a breathalyzer.[162] This would constitute a per se violation of the relevant DUI or DWI statute.[163] Some reasons that jurisdictions have criminalized blowing certain breathalyzer values—rather than just allowing those values to serve as indirect evidence of blood alcohol concentration—relate to the relative ease with which officers can conduct breath tests in the field and the uncertainties surrounding conversions from breath alcohol levels to the blood alcohol levels that might otherwise be criminalized.[164] Such conversions can depend upon a number of factors,[165] making breathalyzer values less accurate at

---

162. *See Blood Alcohol Concentration Limits*, *supra* note 117; *see also* People v. Bransford, 884 P.2d 70, 72 (Cal. 1994) ("[T]he Legislature intended the statute to criminalize the act of driving either with the specified blood-alcohol level or with the specified breath-alcohol level."). For example, California law provides that "[i]t is unlawful for a person who has 0.08 percent or more, by weight, of alcohol in his or her blood to drive a vehicle" and that this value "is based upon grams of alcohol per 100 milliliters of blood or grams of alcohol per 210 liters of breath." CAL. VEH. CODE § 23152(b) (West 2019).

163. *See Blood Alcohol Concentration Limits*, *supra* note 117 ("All 50 states and the District of Columbia have per se laws defining it as a crime to drive with a blood alcohol concentration . . . at or above a proscribed level, 0.08 percent.").

164. *See* People v. Vangelder, 312 P.3d 1045, 1061 (Cal. 2013) (stating that the amendment to the California statute "of the per se offense (§ 23152(b)) was specifically designed to obviate the need for *conversion* of breath results into blood results—and it rendered irrelevant and inadmissible defense expert testimony regarding partition ratio variability among different individuals or at different times for the same individual").

165. *See Bransford*, 884 P.2d at 71 ("Many variables . . . can affect the actual ratio of an individual's breath-alcohol concentration to blood-alcohol

determining whether a particular suspect has a certain blood alcohol concentration. Rather than requiring proof of one's actual blood alcohol concentration in each case, it was a fairly simple legislative solution to criminalize particular breathalyzer readings in addition to blood alcohol concentrations.[166]

Such absolute reliance on breathalyzers naturally makes the accuracy of breathalyzers significant. As a result, some defense lawyers in recent years have sought access to the source codes upon which these machines rely.[167] As one defendant explained, in these types of cases, the only good defense "is to go after the testing method itself."[168] If the source codes contain errors, or the breathalyzer results are based on faulty algorithms, then the resulting alcohol concentrations will likely be inaccurate. And investigators have occasionally uncovered such errors. For example, one expert found defects in breathalyzers regularly used in New Jersey.[169] Because the breathalyzer failed to properly store enough test values, it could report an inaccurate blood alcohol

---

concentration. These variables include body temperature, atmospheric pressure, medical conditions, sex, and the precision of the measuring device.").

166. *See, e.g.*, CAL. VEH. CODE § 23152 (West 2017)(permitting prosecutors to establish illegal blood alcohol content based on "grams of alcohol per 210 liters of breath").

167. *See, e.g.*, State v. Underdahl, 767 N.W.2d 677, 680–81 (Minn. 2009) (recounting the efforts of defense attorneys in two consolidated appeals to obtain source codes for the breathalyzers used in the underlying prosecutions).

168. *Id.* at 685.

169. *See* State v. Chun, 943 A.2d 114, 157 (N.J. 2008) (explaining that one "expert . . . identified a significant flaw in the [breathalyzer] program's source code that, in limited circumstances, can lead to an inaccurate reported BAC test result" and that, although an opposing expert "disputed many of the conclusions proffered by defendants' experts, . . . he acknowledged and explained the buffer overflow defect, admitting that he was responsible for the inclusion of this error in the code"); *see also Underdahl*, 767 N.W.2d at 685 (explaining that one of the appellants submitted a report "analyz[ing] the New Jersey machine's computer source code and uncover[ing] a variety of defects that could impact the test result"). Further, research shows that improper use of breathalyzers can lead to erroneous results. *See* Roth, *supra* 113, at 1999 (citing a report from the American Prosecutors Research Institute and offering the example that "an operator of a breath-alcohol machine who fails to wait long enough after a suspect vomits before commencing the test runs the risk that the machine will mistake residual mouth alcohol for alcohol in deep lung air and inaccurately estimate the suspect's blood-alcohol level").

concentration for a subject.[170] If more information about the algorithms and source codes embedded in breathalyzer programs were released, experts would almost certainly uncover more errors. Such access to the underlying source codes and algorithms of breathalyzers is necessary to secure reliable determinations of guilt and innocence.[171]

Despite this need for the program information that controls breathalyzers, courts have generally refused to grant defendants access to these algorithms and source codes. In many instances, states premise discovery on the government's possession of the requested information.[172] As states often simply license use of the proprietary technology from private companies, they lack this information embedded in the breathalyzer programs.[173] In other states, courts condition discovery on the government having better access to the information than the defendant or on the prosecution making its "best efforts" to obtain the information.[174] Courts have

---

170. *See Chun*, 943 A.2d at 157.

171. A number of states have limited breathalyzer results to those produced by machines that have been previously approved or have put other front-end protocols in place to improve accuracy and reliability. *See* Roth, *supra* note 113, at 2016 ("Many states now limit the type of machines that can be used and enforce operation protocols to ensure accurate results.").

172. *See, e.g.*, MINN. R. CRIM. P. 9.01, subdiv. 2(1) ("On the defendant's motion, the court for good cause must require the prosecutor . . . to assist the defendant in seeking access to specified matters relating to the case that are within the possession or control of an official or employee of any governmental agency, but not within the prosecutor's control."); *see also* Wilson, *supra* note 158, at 129 (explaining that "the Federal Rules of Criminal Procedure treat possession of requested evidence as dispositive for purposes of compliance with a motion for discovery"—that, "[i]n effect, if the prosecution does not possess or control the requested evidence, the government is not mandated to comply with the defendant's discovery motion"—and that "[t]his interpretation of [the] Federal Rule[s] of Criminal Procedure . . . influences state court decisions in states where the rules of criminal procedure are derived from the federal rules").

173. *Cf.* Hills v. State, 663 S.E.2d 265, 266 (Ga. Ct. App. 2008) (affirming the trial court's denial of defendant's discovery request for breathalyzer source code "because the state did not possess or control it"); Fargo v. Levine, 747 N.W.2d 130, 135 (S.D. 2008) ("We affirm the district court's judgment, concluding the district court did not abuse its discretion in denying [defendant's] motion to compel disclosure of the source code because [the defendant] failed to show Fargo had possession, custody or control of the code.").

174. *See* Wilson, *supra* note 158, at 131 (stating that, in Arizona, "the defendant must show that the State has 'better access to the information' and that the defense has made a 'good faith effort to obtain the information without

applied these seemingly more liberal rules narrowly, however, and, again, have generally not allowed for defendants' requested discovery in these cases.[175] In still other states, courts have found the underlying source codes and algorithms either irrelevant to the cases at bar or have determined that defendants' access to this information was outweighed by the program developers' business interests.[176] Accordingly, most defendants have been unsuccessful in obtaining the discovery necessary to effectively challenge breathalyzer results.[177]

Although defendants are generally unsuccessful in obtaining access to information essential to assessing the accuracy of breathalyzers,[178] one noteworthy case in which a defendant was successful in this regard is *State v. Underdahl*,[179] which was litigated in the Minnesota Supreme Court.[180] In that case, two

---

success'" and that "the New York criminal procedure laws require the prosecution to make a 'good faith effort' to obtain material requested by the defendant even if the material is not within the prosecution's possession, custody or control" (internal citations omitted)).

175. *See id.*

176. *See id.*

177. See *id.* at 129–32 (explaining that even "states with seemingly flexible criminal procedure rules invariably arrive at a similar result as the majority: breathalyzer source code is generally not subject to discovery because it is not in the state's possession, custody, or control, and the state is not better-positioned to acquire the proprietary information").

178. *See* Edward J. Imwinkelried, *Computer Source Code: A Source of the Growing Controversy Over the Reliability of Automated Forensic Techniques*, 66 DEPAUL L. REV. 97, 100 (2016) (noting that, "[w]ith few exceptions, the clear majority of courts [have] rejected defendants' requests that a defense expert be granted access to the [breathalyzer's] source code"); Wilson, *supra* note 158, at 123 (explaining that most courts refuse to grant defendants access to breathalyzer source code because this "source code is the proprietary information of the manufacturer and cannot therefore be in the possession, custody, or control of the State").

179. 767 N.W.2d 677 (Minn. 2009).

180. *Underdahl* is part of a morass of Minnesota cases relating to the discovery of breathalyzer source code. A Minnesota district court granted Underdahl discovery on May, 2, 2006, which was the genesis of this litigation, and which eventually resulted in a statewide examination of the accuracy and reliability of breathalyzer evidence in Minnesota. *See In re* Source Code Evidentiary Hearings in Implied Consent Matters, 816 N.W.2d 525, 527 (Minn. 2012) ("This appeal involves a statewide challenge to the reliability of Intoxilyzer 5000EN test results based on alleged defects in the Intoxilyzer 5000EN source code."); *see also In re* Comm'r of Pub. Safety, 735 N.W.2d 706 (Minn. 2007)

defendants were separately charged with driving while intoxicated when their breathalyzer tests indicated blood alcohol concentrations[181] of 0.23 and 0.18.[182] Both defendants separately requested discovery of the breathalyzer's source code.[183] The district courts in both cases granted the defendants' discovery requests, finding the source code relevant to the defendants' guilt or innocence.[184] On appeal, though, the Minnesota Court of Appeals consolidated the cases and reversed the district courts' discovery orders.[185] Finally, the Minnesota Supreme Court recognized that the breathalyzer's source code could very well be relevant in these cases,[186] and it reinstated the district court's order for discovery in one of the defendant's cases.[187] With respect to the other defendant, the court determined that the defendant had not made enough of a showing of relevance to justify the

---

(denying the Commissioner of Public Safety's request for a writ of prohibition to prevent the district court's enforcement of its order to disclose the breathalyzer source code). By this time, "requests for discovery of the source code [had become] part of standard litigation strategy in criminal DWI and implied consent proceedings" in the state. *In re Source* Code Evidentiary Hearings in Implied Consent Matters, 816 N.W.2d at 529. Ultimately, the Minnesota Supreme Court upheld the district court determination that the breathalyzer results were generally reliable. *See id.* at 528, 541–43; *see also In re* Source Code Evidentiary Hearings in Implied Consent Matters, No. 70-CR-09-19749, 2011 WL 803997 (Minn. D. Ct. Mar. 08, 2011) (detailing the district court's order).

181. The relevant statute does not specify whether the "alcohol concentration" measures blood or breath alcohol concentration. MINN. STAT. ANN. § 169A.20 (2017).

182. *Underdahl*, 767 N.W.2d at 680.

183. *See id.*

184. *See id.* at 680–81. The district courts not only granted the discovery requests, but they also ordered that, if the source code were not turned over within thirty days, the breathalyzer evidence would be excluded and, at least in one case, the charge would be dismissed. *See id.*

185. *Id.* at 681.

186. *See id.* at 686 ("[W]e hold that the district court in [one defendant's] case did not abuse its discretion in concluding that the source code may relate to his guilt or innocence.").

187. *See id.* (finding that "the district court in [one of the defendant's] case[s] did not abuse its discretion in concluding that the source code may relate to his guilt or innocence").

discovery order.[188] This is even though the facts of the cases—although not the requests for discovery—were similar.[189]

Underdahl remains an outlier, and defendants generally cannot gain access to the algorithms and source codes underlying the computer program information propping up their convictions.[190] Instead, the breathalyzer developers retain this closely held information. Preserving developers' proprietary interests in the algorithms and source codes is thought to incentivize innovators to develop these types of technologies and support the competitiveness of the industry, but it weakens defendants' abilities to defend themselves in court. Today, despite the opacity of their underlying algorithms and source codes, breathalyzer results remain powerful evidence in court.

2. Automated Fingerprint Identification Systems

Automated fingerprint identification systems constitute another genre of computer programs that helps prosecutors secure criminal convictions. An AFIS relies on its internal algorithms, and the computer source codes implementing those algorithms, to match latent prints from crime scenes to exemplar fingerprints—the known fingerprints on file.[191] Contrary to how

188. *See Underdahl*, 767 N.W.2d at 685–86. Justices Alan Page and Paul Anderson concurred in part and dissented in part, objecting to the Supreme Court's affirmance of the Court of Appeal's reversal of the production order with respect to the second defendant, Dale Lee Underdahl. *See id.* at 687–88 (Page, J., concurring in part and dissenting in part).

189. *See id.* at 680. In contrast to Underdahl's discovery request, where he did not offer any information or exhibits supporting the motion, "Brunner submitted a memorandum and nine exhibits to support his request for the source code." *Id.* at 685. One of Brunner's exhibits "was the written testimony of . . . a computer science professor at the University of California in Berkeley, which explained the source code in voting machines, the source code's importance in finding defects and problems in those machines, and the issues surrounding the source code's disclosure." *Id.* Another exhibit "detailed Brunner's attempts to obtain the source code, both from the State and [the breathalyzer manufacturer]." *Id.* Yet another exhibit "was a copy of a report prepared on behalf of the defendants in New Jersey litigation about the reliability of New Jersey's breath-test machine." *Id.*

190. *See* Wilson, *supra* note 158, at 123.

191. *See generally* NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, THE FINGERPRINT SOURCEBOOK ch. 6, https://perma.cc/JC9T-5H2Z (PDF).

AFISs are depicted on television and in the movies, though, these programs do not actually exactly match prints. In fact, such perfect matches are nearly impossible, as any individual's finger will print differently depending on the mechanics of touch and the properties of the surface touched.[192] Instead, AFISs provide authorities with a number of possible matches, and human fingerprint examiners are the ones to actually declare matches and testify to them in court.[193] The accuracy and reliability of AFISs remain important, however, because, as has recently become apparent, there are real questions about the abilities of fingerprint examiners to discern fingerprint matches from non-matches or inconclusive results.[194] It seems, then, that these examiners rely quite heavily on AFIS results, thus rendering AFIS conviction programs similar to breathalyzers in regularly fortifying criminal convictions.

Despite the important role that AFISs play in the ultimate conviction of criminal defendants, experts know very little about the accuracy of AFISs. Outside of the companies developing these products and the government agencies purchasing or licensing the technology, very few individuals, if any, have raised the concern that these programs may not produce accurate results.[195] In fact,

---

192. *See* NAT'L ACAD. OF SCI., *supra* note 144, at 137. The National Academy of Sciences report explains that a number of factors contribute to fingerprint impressions, including: the "[c]ondition of the skin," "[t]ype of residue," "[m]echanics of touch," "[n]ature of the surface touched," "[d]evelopment technique," "[c]apture technique," and "[s]ize of the latent print or the percentage of the surface that is available for comparison." *Id.* at 137–38.

193. *See* NAT'L INST. OF JUSTICE, *supra* note 191, at 6–27.

194. *See* Specter, *supra* note 158. Notably, over half of the practicing or would-be fingerprint examiners who take the International Association of Identification's certification test fail it. *See* Lyn Haber & Ralph Norman Haber, *Error Rates for Human Latent Fingerprint Examiners*, *in* AUTOMATIC FINGERPRINT RECOGNITION SYSTEMS 354 (Nalina Ratha & Ruud Bolle, eds. 2004) (noting "that about half the applicants for certification fail the test on the basis of poor fingerprint matching skills"); *see also* Andy Newman, *Fingerprinting's Reliability Draws Growing Court Challenges*, N.Y. TIMES (Apr. 7, 2001), https://perma.cc/AUB5-6JSV (last visited Oct. 17, 2019) ("The accuracy of making identifications from dusted or latent prints, which are often smudged, distorted or fragmentary, has never been scientifically tested.") (on file with the Washington and Lee Law Review).

195. *But cf.* NAT'L ACAD. OF SCI., *supra* note 144, at 142–43 ("Although there is limited information about the accuracy and reliability of friction ridge analyses, claims that these analyses have zero error rates are not scientifically plausible.").

it seems that accuracy is not necessarily the goal in AFIS functioning. Take the FBI's current AFIS program, for example. While the FBI requests figures on the validity of these programs, neither its purchasing agents nor its fingerprint examiners are exactly sure how the program produces the possible matches that it generates.[196] The FBI's current program produces a handful of possible matches from the database for each latent fingerprint inputted into the system.[197] It will produce these possible matches regardless of whether there is a 1% or a 99% similarity between the latent print and each of the closest "matches"[198] in the database.[199] The program does not produce any useful data for the user about how similar the internal database exemplar prints are to the inputted latent prints.[200] While researchers have played with "similarity scores," attempting to quantify how close alleged matches are, there is no consensus as to how to measure similarity, so similarity scores are just assessments of similarity according to a particular researcher's, or programmer's, own assessment of similarity.[201]

After AFIS has generated a number of potential matches, the operator then turns over these results to a fingerprint examiner to determine with (alleged) certainty whether one of the program-produced "likely" exemplar prints actually matches the latent print.[202] Again, the fingerprint examiner's ability to do this

---

196. *See* Interview with James Loudermilk, *supra* note 118; *see also supra* note 119 (noting that the FBI declined to comment).

197. *See* Interview with James Loudermilk, *supra* note 118.

198. The determination that these three prints are the closest matches to the latent print are according to the proprietary algorithm, the details of which remain secret. *See id.*

199. *See id.*

200. *See id.*; *see also infra* note 205 (noting that a similarity score is "just 'an artificial construct of the algorithm'").

201. *See* Ryan, *supra* note 14 ("[T]here are multiple ways to assess print *similarity*, depending on how that term is defined. The probability that prints share the same source . . . is a more complicated question.").

202. *See supra* note 193 and accompanying text. It is important to note that there are significant questions about the validity and reliability of fingerprint examiners' determinations of fingerprint matches. Their methods are unscientific, and some studies have shown that their reliability is wanting. *See* Ryan, *supra* note 14; *cf.* 5 DAVID FAIGMAN ET AL., MODERN SCIENTIFIC EVIDENCE: THE LAW AND SCIENCE OF EXPERT TESTIMONY § 32.1 (2018) ("[S]urprisingly little

in an accurate and reliable manner remains questionable.[203] Further, the fingerprint examiner—who is the individual ultimately testifying in court—is generally unfamiliar with the AFIS technology providing him with a persuasive starting point for his analysis.[204] Although AFIS provides the examiner with a limited number of possibilities for a match, the examiner is generally unaware of how the technology has chosen these particular fingerprints as the possible matches from the database, and he is also unaware of how similar the "likely" matches are.[205]

Also like breathalyzers, AFISs are generally shrouded in secrecy. Again, the companies that develop these computer programs often do not want to release the details of their algorithms or underlying source codes because this would nullify their legal monopolies over the programs; it would hurt their business interests.[206] Because this information is generally unavailable to the public, to criminal defendants, and even to the primary users of the program—law enforcement officers and fingerprint examiners—it seems that no defendants have ever challenged the matching programs on which their fingerprint matches are based. This lack of challenges may also result from the fact that, unlike breathalyzer evidence, AFIS matches are a step removed from prosecutors' court cases against these

---

conventional science exists to support the claims of the fingerprint examination community."). Further, fingerprint examiners are generally not blinded from the already-developed facts of the case—from who the suspect is, how gruesome the crime was, the identity of the victim, etc.—making them susceptible to bias, whether conscious or unconscious. *See* Sue Russell, *Bias and the Big Fingerprint Dust-Up*, PAC. STANDARD (June 18, 2009), https://perma.cc/7S3R-D9TY (last updated Oct. 31, 2018) (last visited Oct. 17, 2019) (on file with the Washington and Lee Law Review).

203. *See supra* note 194 and accompanying text.

204. *See, e.g.*, Ryan, *supra* note 14 ("[E]ven the FBI does not have access to the underlying algorithm and source code that produces the closest fingerprint matches . . . .").

205. *See* Interview with James Loudermilk, *supra* note 118; *see also supra* note 119 (noting that the FBI declined to comment). Although the program provides the user with similarity scores, these scores are just "an artificial construct of the algorithm"; similarity is assessed according to the secret algorithm's own definition of "similarity." Interview with James Loudermilk, *supra* note 118; *supra* notes 200–201 and accompanying text.

206. *See* Interview with James Loudermilk, *supra* note 118.

defendants. And even more basic challenges to fingerprint examiners' match conclusions and resulting court testimony have been repeatedly shot down by courts across the nation.[207] Throughout history, not a single criminal defendant in the United States has found success in challenging the art of fingerprinting.[208]

---

207. *See* Ryan, *supra* note 14.

208. In 2002, there was, briefly, a success story of a defendant having a fingerprint examiner's expert testimony against him excluded. *See* Paul C. Giannelli, *Fingerprints Challenged*, 17 CRIM. JUST. 33, 33 (2002). In *United States v. Llera Plaza*, 179 F. Supp. 2d 492 (E.D. Pa. 2002) (withdrawn from bound volume), *vacated and superseded by* United States v. Llera Plaza, 188 F. Supp. 2d 549 (E.D. Pa. 2002), Pennsylvania District Court Judge Louis H. Pollak initially determined that the fingerprint examiner's testimony against the defendant—who was being tried on various "drug and murder charges," *Llera Plaza*, 188 F. Supp. 2d at 550—was inadmissible. *See Llera Plaza*, 179 F. Supp. 2d at 517–18. The district court concluded that:

> The parties will be able to present expert fingerprint testimony (1) describing how any latent and rolled prints at issue in this case were obtained, (2) identifying, and placing before the jury, such fingerprints and any necessary magnifications, and (3) pointing out any observed similarities and differences between a particular latent print and a particular rolled print alleged by the government to be attributable to the same persons. But the parties will not be permitted to present testimony expressing an opinion of an expert witness that a particular latent print matches, or does not match, the rolled print of a particular person and hence is, or is not, the fingerprint of that person.

Id. Judge Pollak reached his singular conclusion by carefully examining the details of this particular forensic science discipline and applying the controlling *Daubert* standard rather than just presuming that fingerprint examiner testimony was admissible because of its long historical pedigree. *See id.* at 494–517. He determined that there was little, if any, scientific testing establishing the "reliability of fingerprints," *id.* at 506–08 ("On the record made in *Mitchell*, the government had little success in identifying scientific testing that tended to establish the reliability of fingerprint identifications."), that fingerprint examination "had not been sufficiently subjected to the peer review [and publication] process," Ryan, *supra* note 14; *see also Llera Plaza*, 179 F. Supp. 2d at 508–09 (noting that any publications had not truly been subjected to scientific scrutiny and stating that "[i]t would . . . be a misnomer to call fingerprint examiners a 'scientific community' in the *Daubert* sense), and that fingerprint identifications further failed the next *Daubert* factor considering "the known or potential rate of error . . . and the existence and maintenance of standards controlling the technique's operation," *see Llera Plaza*, 179 F. Supp. 2d at 509–14. While fingerprint identifications are generally accepted, the district court explained that "the failure of fingerprint identifications fully to satisfy the first three *Daubert* factors militates against heavy reliance on the general acceptance factor," *id.* at 515, and that general acceptance cannot "by itself . . . sustain the government's burden in making the case for the admissibility of fingerprint

3. Probabilistic Genotyping Systems

As with breathalyzers, AFISs, and other technologies, there are real concerns about the accuracy of PGSs like TrueAllele and STRmix. In 2016, the President's Council of Advisors on Science and Technology (PCAST) reviewed the use of forensic sciences in the United States, including PGSs such as TrueAllele and STRmix.[209] Although PCAST recognized that these approaches to

---

testimony under Federal Rule of Evidence 702." *Id.* This radical skeptical view of fingerprint identifications "sent reverberations across the criminal justice community—but not for long." Ryan, *supra* note 14. Judge Pollak reversed his decision just two months later. *See Llera Plaza*, 188 F. Supp. 2d 549, *vacating and superseding Llera Plaza*, 179 F. Supp. 2d 492 (withdrawn from bound volume); Ryan, *supra* note 14. He "explained that, upon reconsideration, it seemed that, although fingerprint examination is not scientific, it is a technical discipline and, in that sense, there has been sufficient peer review and publication and sufficient knowledge of error rate and maintenance of standards under *Daubert*." Ryan, *supra* note 14; *see Llera Plaza*, 188 F. Supp. 2d at 571. "The 'testing' factor of *Daubert* was still not met, but this, the court determined, would not prevent the admissibility of testimony on fingerprint identifications." Ryan, *supra* note 14; *see Llera Plaza*, 188 F. Supp. 2d at 571–72. Judge Pollak explained that, "[t]o postpone present in-court utilization of this 'bedrock forensic identifier' pending such [useful] research would be to make the best the enemy of the good." *Llera Plaza*, 188 F. Supp. 2d at 572. This "was the end of the brief victory by criminal defendants over the questionable practice of admitting 'expert' testimony on fingerprint identifications." Ryan, *supra* note 14. As I have explained elsewhere, "[s]ince Judge Pollak's brave analysis in his initial opinion carefully analyzing the forensic discipline under *Daubert*, there have been no other even slightly successful challenges to this evidence in court." *Id.* Instead, "[j]udges seem to have taken a uniform stance in admitting this evidence despite the questions about the accuracy and reliability of the human fingerprint examiners and the [opaque] AFISs on which they rely as important starting points for their examinations." *Id.* Without much success challenging fingerprint evidence in general, there has been little incentive for defendants to broaden their challenges to include access to the algorithms and source codes underlying AFIS results that contribute to fingerprint examiners' analyses.

209. *See generally* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., FORENSIC SCIENCE IN CRIMINAL COURTS: ENSURING SCIENTIFIC VALIDITY OF FEATURE-COMPARISON METHODS (Sept. 2016), https://perma.cc/A7EF-2NJC (PDF) (reviewing forensic science methods as used in U.S. Courts, including examining the uses of PGSs). This goes hand-in-hand with the FBI's recent notice to laboratories that federal data they had been using in calculating probabilities as related to DNA mixtures was erroneous. *See* Spencer S. Hsu, *FBI Notifies Crime Labs of Errors Used in DNA Match Calculations Since 1999*, WASH. POST (May 29, 2015), https://perma.cc/8FFH-949L (last visited Oct. 12, 2019) (on file with the Washington and Lee Law Review).

analyzing DNA mixtures are an improvement over more subjective methods of analyzing mixtures—methods that require examiners to make assumptions about which alleles to include and exclude in the probability calculations—it also expressed concerns about blindly relying on these computer-based approaches.[210] PCAST explained:

> These probabilistic genotyping software programs clearly represent a major improvement over purely subjective interpretation. However, they still require careful scrutiny to determine (1) whether the methods are scientifically valid, including defining the limitations on their reliability (that is, the circumstances in which they may yield unreliable results) and (2) whether the software correctly implements the methods. This is particularly important because the programs employ different mathematical algorithms and can yield different results for the same mixture profile.[211]

PCAST's concern about accuracy is very real. TrueAllele and STRmix have produced conflicting results in certain cases.[212] In *New York v. Hillary*,[213] for example, TrueAllele results suggested that defendant Hillary was not at the murder scene, whereas STRmix results placed him there.[214] Further, experts found a coding error in the STRmix software in the midst of a criminal trial in New Zealand.[215] This important observation likely would have

---

210. *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 209, at 79.

211. *Id.*

212. *See* Augenstein, *supra* note 9; Kirchner, *supra* note 42.

213. No. 2015-15 (St. Lawrence County Aug. 26, 2016).

214. *See* Augenstein, *supra* note 9.

215. *See* Kirchner, *supra* note 42; David Murray, *Queensland Authorities Confirm 'Miscode' Affects DNA Evidence in Criminal Cases*, THE COURIER-MAIL, (Mar. 20, 2015), https://perma.cc/6RLC-SN72 (last visited Jan. 21, 2020) (on file with the Washington and Lee Law Review); *see also* STATEMENT RELATING TO STRMIX™ MISCODES, FRIDAY, 18 MARCH 2016, https://perma.cc/53X8-PJ4R (PDF) (announcing the coding error); *see also* Roth, *supra* note 113, at 2024–25 (stating that "[STRmix's] creators have had to disclose publicly multiple episodes of miscodes potentially affecting match statistics"). Perhaps suggesting similar problems, "TrueAllele's creator Mark Perlin has executed over twenty-five revisions to its 170,000+ lines of source code, with no published documentation as to what has been revised or why." Andrea Roth, *Trial by Machine*, 104 GEO. L.J. 1245, 1273 (2016); *see also* Natalie Ram, *Innovating Criminal Justice*, 112 NW. U. L. REV. 659, 681 (2018) (suggesting that these changes may have "corrected

gone unnoticed if the underlying source code and algorithm had remained entirely secret. These examples raise the very serious question about which results, if any, should be trusted.

Despite different PGSs producing conflicting results, the creators of these programs still tout the programs' accuracy and usefulness. Cybergenetics founder and creator of TrueAllele, Mark Perlin, boasts about the improved accuracy of his program over traditional DNA analyses[216] and claims that TrueAllele "is validated to [the level of] five [DNA mixture] contributors in various scientific publications."[217] Importantly, though, the studies and reviews justifying this claim of accuracy were conducted by Cybergenetics or its shareholders.[218] As the lead author on one of these studies, for example, Perlin disclosed that he "is a shareholder, officer and employee of Cybergenetics . . . [which] manufactures the patented TrueAllele® Casework system, and provides expert testimony about DNA case results."[219] The second and third authors on the article were also at the time "current or former employees of Cybergenetics."[220] This is a clear conflict of interest. Perlin's claims of program accuracy are not unique,

---

undisclosed errors or inadvertently introduced new ones").

216. *See* Augenstein, *supra* note 9. This is not inconsistent with the PCAST report, which similarly stated that "[t]hese probabilistic genotyping software programs clearly represent a major improvement over purely subjective interpretation." PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 209, at 79.

217. Augenstein, *supra* note 9. According to Perlin, the National Institute of Standards and Technology (NIST) "pretends" that TrueAllele must be further validated or that "there is a problem" with TrueAllele in order to secure funding for the organization. *Id.* He has further argued that NIST is "biased and lack[s] expertise." *Id.* As for PCAST, Perlin has suggested that the "report is well-intentioned, but misguided," and that "[f]orensics needs better science, not more bureaucracy." *Id.*

218. *See id.*; *see also* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 209, at 80 ("[M]ost of the studies evaluating software packages have been undertaken by the software developers themselves."). *But see* Imwinkelried, *supra* note 178, at 121 (suggesting that the number of validation studies demonstrating the accuracy of the TrueAllele software is sufficient, at least when the software is used under certain conditions).

219. Mark W. Perlin et al., *TrueAllele Casework on Virginia DNA Mixture Evidence: Computer and Manual Interpretation in 72 Reported Criminal Cases*, 9 PLOS ONE 3, 1 (2014).

220. *Id.*

though. STRmix developer John Buckleton has similarly argued that his program is well validated and that PCAST reached improper conclusions based on inadequate research.[221] PCAST has explained that, although "[a] number of papers have been published that analyze known mixtures in order to address [accuracy and related concerns]," several points must be made.[222] "First, most of the studies evaluating [these] software packages have been undertaken by the software developers themselves. While 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."[223] PCAST also pointed out that "there have been few comparative studies across the methods to evaluate the differences among them" and the few that have been conducted were not by uninterested, independent groups.[224] "Most importantly," PCAST explained:

> [C]urrent studies have adequately explored only a limited range of mixture types (with respect to number of contributors, ratio of minor contributors, and total amount of DNA). The two most widely used methods (STRMix and TrueAllele) appear to be reliable within a certain range, based on the available evidence and the inherent difficulty of the problem. Specifically, these methods appear to be reliable for three-person mixtures in which the minor contributor constitutes at least 20 percent of the intact DNA in the mixture and in which the DNA amount exceeds the minimum level required for the method. . . . For more complex mixtures (*e.g.* more contributors or lower proportions), there is relatively little published evidence. In human molecular genetics, an experimental validation of an important diagnostic method would typically involve hundreds of distinct samples.[225]

---

221. *See* Augenstein, *supra* note 9. In response to the PCAST report, Buckleton provided PCAST with a list of publications validating STRmix. *See id.* As with TrueAllele, these publications were authored by individuals with a financial interest in the technology.

222. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 209, at 80–81.

223. *Id.* at 80.

224. *Id.*

225. *Id.* at 80–81. The report further stated that "[o]ne forensic scientist told PCAST that many more distinct samples have, in fact, been analyzed, but that

TrueAllele and STRmix continue to maintain, though, that their technologies are validated for analyzing more than three-person mixtures,[226] and forensic scientists regularly use these programs on these more complex mixtures.

One of the primary reasons that experts have not investigated the accuracy of PGSs more thoroughly is that the developers of these programs have vigilantly guarded their programs as trade secrets. As with other creators of conviction programs, PGS developers like Cybergenetics and Buckleton claim that secrecy is necessary to preserve their property rights.[227] Indeed, if the source code or algorithm were made public, the program would become vulnerable to copycats that could purloin market share. Because of this secrecy, researchers have difficulty gaining access to the algorithms and source codes that could inform accuracy determinations.[228] Further, because licensing the programs is expensive, it is difficult for researchers to even engage in validation exercises that could be useful for assessing accuracy.

Not only does this secrecy make it difficult for researchers to examine PGSs, but it makes it nearly impossible for criminal defendants and their attorneys to challenge this evidence when prosecutors present it in court. As commentators have explained, "[w]ithout the programming code, defense attorneys are unable to

---

the data have not yet been collated and published." *Id.* at 81. PCAST then urged forensic scientists and scientific journals to work together "to publish high-quality validation studies that properly establish the range of reliability of methods for the analysis of complex DNA mixtures." *Id.* PCAST explained that this is necessary "[b]ecause empirical evidence is essential for establishing the foundational validity of a method." *Id.*

226. *See* Augenstein, *supra* note 9.

227. *See* Dang, *supra* note 137. Cybergenetics has consistently refused to reveal its source code or details about its algorithm, and judges have also refused to order discovery here. *See* Kirchner, *supra* note 42 ("Defendants' requests to get access to TrueAllele's source code have consistently been denied, leading the Electronic Privacy Information Center, an advocacy group, to kick off a FOIA campaign to obtain whatever information is publicly available from the jurisdictions that use it."). Professor Natalie Ram stated that, at least as of 2018, "no one outside of Perlin's company has seen or examined TrueAllele's source code." Ram, *supra* note 215, at 677.

228. *Cf.* Dang, *supra* note 137 ("[W]ithout the code, there is no way of verifying that True Allele is as accurate as Cybergenetics claims.").

challenge the accuracy of TrueAllele" and other PGSs.[229] "Likewise, prosecutors can't authenticate it."[230] The same is true with respect to the appropriateness of the underlying algorithm.

This concern that secrecy leaves defense attorneys unable to challenge the accuracy of a program like TrueAllele was the claim made by Michael Robinson, a man on trial for murder in Pennsylvania in 2013.[231] Part of the evidence against Robinson was a match to his DNA found on a bandana near the crime scene.[232] Examiners cultivated this DNA evidence by analyzing the complex sample with TrueAllele.[233] The results were staggering and damning: The TrueAllele analysis determined that the DNA found on the bandana "was 5.6 billion times more likely" to have come from Robinson than from another individual.[234] And the punishment facing Robinson if convicted—the death penalty—exacerbated the devastating nature of the probability determination.[235] During the course of Robinson's defense, his counsel requested access to the source code underlying TrueAllele, claiming that, "without production and defense review of the computer instructions, not only will the petitioner be denied his constitutional right to a fair trial—he risks being wrongly executed."[236] Defense counsel explained that having access to the source code was essential for cross-examining Mark Perlin,

---

229. *Id.*

230. *Id.*

231. *See* Seth Augenstein, *Access Denied: Source Code for DNA Software Remains Protected in Pa. Murder Trial*, FORENSIC MAG. (Feb. 5, 2016), https://perma.cc/G8TV-MRBG (last visited Oct. 16, 2019) (on file with the Washington and Lee Law Review).

232. *See id.*; Dang, *supra* note 137.

233. *See* Augenstein, *supra* note 231; Dang, *supra* note 137.

234. Dang, *supra* note 137 ("TrueAllele found that the DNA was 5.6 billion times more likely to belong to Robinson than to another suspect."); Paula Reed Ward, *Attorneys Ask Superior Court to Take Up DNA Issue*, PITTSBURGH POST-GAZETTE, Mar. 8, 2016 ("Dr. Perlin said the DNA was 5.6 billion times more likely to belong to Mr. Robinson."). The TrueAllele analysis actually initially produced a probability of one in 2 billion, but, after a software upgrade to the program, it generated the one in 5.6 billion probability figure. *See id.*

235. *See* Dang, *supra* note 137 ("If Robinson is convicted, he faces the death penalty.").

236. *Id.*

TrueAllele's developer.[237] The district court was unpersuaded by this argument, though, and denied the discovery request.[238] The court stated that "[a]n order requiring Cybergenetics to produce the source code would be unreasonable, as release would have the potential to cause great harm to Cybergenetics."[239] Indeed, Cybergenetics could lose a lot of money to competitors if it made the source code public.

Commercial PGS developers have generally sought to protect their creations through secrecy, and many courts have granted them this sphere of secrecy with respect to the programs' algorithms and source codes.[240] Some courts have granted limited access to this information in some circumstances, although these orders have rarely endured.[241] For example, in March of 2018, a

---

237. *See id.*

238. *See* Augenstein, *supra* note 231; Dang, *supra* note 137.

239. Dang, *supra* note 137.

240. Some non-commercial developers make their source codes publicly available, allowing researchers to modify and use their codes. *See* Kirchner, *supra* note 42. As Lauren Kirchner has reported:

> Some makers of probabilistic genotyping software allow other programmers to use and modify their code. LRmix, software created by a pair of scientists in the Netherlands, EuroForMix, created by a Norwegian team, and Lab Retriever, a non-commercial program available under the Creative Commons license and uploaded to GitHub, are among the free, open-source tools available.
>
> Beyond offering transparency, this approach can help expose problems. A significant bug was discovered and fixed in LikeLTD, an open-source Australian probabilistic genotyping program, because of outside scrutiny.

Id.

241. As Professor Natalie Ram explained, as of 2018, "only one American court ha[d] compelled production of the source code for probabilistic genotyping software in a criminal case." Ram, *supra* note 215, at 678; *see also* Imwinkelried, *supra* note 178, at 101 ("The courts' responses to requests for the source code of TrueAllele has been even more uniformly negative than the previous requests for access to the source codes of infrared breath testing instruments."). And the software at issue in that case was not developed by the commercial sector but was instead created by New York City's crime lab. *See* Lauren Kirchner, *Federal Judge Unseals New York Crime Lab's Software for Analyzing DNA Evidence*, PROPUBLICA (Oct. 20, 2017), https://perma.cc/4JJF-2JZT (last visited Jan. 21, 2020) (on file with the Washington and Lee Law Review). Experts had already questioned the validity of FST's design, but, after a judge ordered disclosure of the software's source code, one reviewing (defense) expert "found that the program dropped valuable data from its calculations, in ways that users wouldn't

San Diego Superior Court judge ruled that prosecutors were required to turn over STRmix's software and source code to defense counsel,[242] but the California Court of Appeals reversed this order just a few months later.[243] Aside from court orders, certain developers like Buckleton have made their source codes available to defense counsel on a limited basis.[244] Such limited access could require defense counsel to sign confidentiality and non-disclosure agreements, though.[245] This could have the effect of limiting counsel from critiquing the workings or accuracy of the program in open court.[246] Less forthcoming, Cybergenetics provides preliminary DNA *results* to law enforcement (as well as to defense counsel) on a complimentary basis, charging the client for only a full report that could be used as evidence at trial.[247]

---

necessarily be aware of, but that could unpredictably affect the likelihood assigned to the defendant's DNA being in the mixture." Lauren Kirchner, *Traces of Crime: How New York's DNA Techniques Became Tainted*, N.Y. TIMES (Sept. 4, 2017), https://perma.cc/DPN6-YMVZ (last visited Jan. 21, 2020) (on file with the Washington and Lee Law Review). The expert concluded: "'I did not leave with the impression that FST was developed by an experienced software development team,'" and that, "[p]ending more rigorous testing, 'the correctness of the behavior of the FST software should be seriously questioned.'" *Id.* Faced with these concerns, the U.S. Attorney's office withdrew the relevant DNA evidence against the defendant prior to the admissibility hearing. *See id.*

242. *See* Greg Moran, *DA Fights Judge's Order to Hand Over Info on How New DNA Test Works*, SAN DIEGO UNION-TRIB. (Apr. 16, 2018, 5:00 AM), https://perma.cc/25GS-8RMP (last visited Jan. 20, 2020) (on file with the Washington and Lee Law Review).

243. *See* People v. Superior Court, 239 Ca. Rptr. 3d 71 (Cal. Ct. App. 2018).

244. *See* Moran, *supra* note 242; Kevin Petroff, *The Changing State of DNA Analysis*, 46 TEX. PROSEC. (July–Aug. 2016), https://perma.cc/6QR7-V8AQ (last visited Jan. 20, 2020) (explaining that, although there are certainly "some differences between [STRmix and TrueAllele], the biggest issue . . . is that the STRmix creator is willing to share the 'source code,' or the ingredients of the program, with the State or the defense if requested in a case," while, "[a]t this time, TrueAllele is refusing to provide that information") (on file with the Washington and Lee Law Review).

245. *See* Moran, *supra* note 242.

246. *See id.*

247. *See* Kirchner, *supra* note 42 ("[Cybergenetics] offers to take on [the] most difficult DNA cases and provides preliminary results for free. . . . [C]ustomers only pay at the point at which they want Cybergenetics to run a complete analysis and write a report about the results that can be used at trial.").

Despite these concerns about accuracy and reliability, and despite regularly being held secret, which heightens the validity concerns, TrueAllele is used by crime labs in Virginia, Baltimore, Kern County (CA), Beaufort County (SC), and Richland County (SC).[248] STRmix is used by the FBI and U.S. Army, as well as labs in New York, California, and Texas.[249]

B. Burgeoning Secrecy in the Law

Secrecy has become a problem throughout the law[250] and is especially troubling in the context of using computer programs in the criminal justice system. Most often, criminal defendants do not have access to the algorithms and source codes that criminal justice system actors rely on in making impactful decisions about these defendants' lives.[251] In fact, it seems that even the individuals wielding these programs—from police officers to prosecutors to judges—do not have access to the details of the programs upon which these important decisions are made.[252] Moreover, even if these actors did have access to the relevant algorithms and source codes, they probably would not understand their nuances,[253] as doing so would ordinarily require an understanding of the applicable database, expertise in computer science, and a background of conducting social or natural science

248. *See id.*

249. *See id.*; Petroff, *supra* note 244.

250. *See, e.g.*, William W. Berry & Meghan J. Ryan, *Cruel Techniques, Unusual Secrets*, 78 OHIO ST. L.J. 403, 405 (2017) (describing the problems of secrecy surrounding lethal injection procedures under the Eighth Amendment's prohibition on cruel and unusual punishments).

251. *See supra* Part III.

252. *See supra* Parts III–IV.

253. *See* Ferguson, *supra* note 37, at 1166 ("The nature of algorithms further obscures the process, except perhaps to technical experts.").

research.[254] As one might imagine, most criminal justice actors lack these proficiencies.[255]

One of the reasons that these algorithms and source codes are kept secret is that outside companies have created them and rely on this secrecy to make profits; the algorithms and source codes are proprietary in nature. Northpointe's COMPAS would not be nearly as lucrative if its algorithm or source code were made public and others could profit off of its research and development investments. The same is true with respect to TrueAllele and other technologies that the government uses to secure convictions. The intricacies of intellectual property law exacerbate what has become a secrecy problem in this arena.[256] In recent years it has become more difficult to obtain effective patents on algorithms, pushing businesses to heighten the secrecy surrounding their inventions and operations rather than disclose information in exchange for a temporary monopoly on the technology by way of patent law.[257] This is one factor that has contributed to the rise of secrecy in the realm of government conviction programs.

But the secrecy surrounding the workings of technologies like breathalyzers, AFISs, and PGSs is not entirely novel within the criminal justice sphere. For example, in the area of lethal injection there has also been a marked increase in secrecy as states have had to experiment with a variety of drug cocktails to carry out executions because European drug manufacturers have refused to sell their drugs to buyers intending to use them to execute

---

254. *Cf. id.* (stating that "the technical complexity of [automated predictive technologies' designs] makes it nearly impossible for outsiders to determine the accuracy, effectiveness, or fairness of the program" and explaining that, in the context of predictive policing algorithms, although government actors "receive the results, . . . due to the complexity of the chosen algorithm they can rarely understand the underlying math").

255. *Cf.* NAT'L ASS'N OF CRIM. DEFENSE LAWYERS, *GIDEON* AT 50: A THREE-PART EXAMINATION OF INDIGENT DEFENSE IN AMERICA 9 (Oct. 2016) (examining the sorry state of indigent defense in the United States today).

256. For a more detailed account of the intersection of intellectual property and secret conviction programs, see Meghan J. Ryan, *Secret Algorithms, IP Rights, and the Public Interest* (unpublished manuscript) (on file with author).

257. *See* Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. 208 (2014) (limiting businesses' abilities to obtain patents on computer software); *see also* Ryan, *supra* note 256 (examining the interaction between intellectual property law and the burgeoning secrecy in public law fields like criminal law and procedure).

individuals.[258] In many instances, they have refused to disclose the combinations of drugs to be used for execution, the dosages to be used, and the drug suppliers.[259] This is in addition to the long history of secrecy about the identity of the executioners and the limitations on the numbers of individuals who may observe executions.[260] Some litigants have objected to this secrecy, but they have generally been unsuccessful due to the limitations of due process and the confines of the particular procedural postures in which these matters are raised.[261] Secrecy is also prevalent in the

---

258. *See* Berry & Ryan, *supra* note 250, at 422 ("[S]ecrecy has increasingly crept into lethal injection executions. Today, state governments shroud modern executions with multiple levels of secrecy, a disturbing notion in an open, democratic society."); *see also* Eric Berger, *Lethal Injection Secrecy and Eighth Amendment Due Process*, 55 B.C. L. REV. 1367, 1380–83 (2014) (chronicling states' "increasingly creative and legally dubious steps to procure drugs for their execution procedures").

259. *See* Berry & Ryan, *supra* note 250, at 423 ("In many cases, states have elected to keep the identity of the new drugs secret, as well as the names of the drug manufacturers.").

260. *See id.* (noting that the recent rise in secrecy around lethal injection protocols "complements states' traditional determinations to keep the identities of executioners secret" and explaining that, "[n]ot only have executions transitioned from the public to the private sphere, leaving most Americans without the experience of watching someone die by lethal injection or firing squad, but also gaining any access to the details of these executions is exceedingly difficult, if not impossible"). There is at least one additional layer of secrecy with respect to lethal injections. *Id.* at 406. This stems from the government's use of a paralytic to hide the corporal writhing that would likely otherwise be observed as the death row offender is being put to death. *See id.* There seems to be no clinical reason for this paralytic, which actually complicates the execution process by making it more difficult to determine whether the offender has been sufficiently sedated before he is killed. *See* Brief for Petitioners at 52, Baze v. Rees, No. 07-5439, 2007 WL 3307732 (Nov. 5, 2007) (stating that "[i]t is undisputed that pancuronium is not a necessary component of the execution procedure" and pointing out that the lower court "concluded that the 'use of pancuronium in Kentucky's lethal injection protocol serves no therapeutic purpose'" (internal alterations omitted)); Gregory D. Curfman et al., *Physicians and Execution*, 358 NEW ENGLAND J. MED. 403, 403 (2008) ("The use of a neuromuscular blocker, pancuronium bromide, as part of the protocol has been especially controversial, since it has no anesthetic properties and only paralyzes the person, which can mask inadequate anesthesia if a sufficient dose of sodium thiopental has not been administered.").

261. *See* Berger, *supra* note 258, at 1392 ("The majority of courts, especially federal appellate courts, have permitted states to keep secret important details from their lethal injection procedures."). In *Sepulvado v. Jindal*, 729 F.3d 413 (5th Cir. 2013), for instance, the Fifth Circuit, rejecting the death row plaintiff's

area of government surveillance. After the terrorist attack on September 11, 2001, and Congress's enactment of the USA Patriot Act, the Foreign Intelligence Surveillance Court (FISA Court) began issuing significantly broader secret subpoenas requiring internet and telecommunications companies to surrender customers' personal data, browsing data, and details of their conversations.[262] It also "began issuing ground-breaking secret legal interpretations that allowed mass surveillance."[263] All of this was done in the name of national security.[264] Further, secrecy abounds in terms of how the government obtains information to be used against any particular defendant. As a result of the "increasingly prevalent doctrine of 'collective knowledge,'" which means that one officer's knowledge is imputed to other officers, individual police officers can possess the necessary "reasonable suspicion" to take actions in an effort to obtain evidence against a suspect.[265] This allows police officers to obtain the information that facilitates "parallel construction" in a case;[266] it enables the police to obtain information from a secret source and then suggest that the information came from another line of investigation.[267] All of

---

request that the state disclose the details of the execution protocol, concluded that "[t]here is no violation of the Due Process Clause from the uncertainty that Louisiana has imposed on Sepulvado by withholding the details of its execution protocol." *Id.* at 420. Provocatively, the court conceded that "[p]erhaps the state's secrecy masks 'a substantial risk of serious harm'" stemming from the protocol, "but," the court furthered, "it does not create one." *Id.* Defending its position, the court pronounced that "[c]ourts are not supposed to function as 'boards of inquiry charged with determining best practices.'" *Id.* at 419 (quoting Baze v. Rees, 553 U.S. 35, 51 (2008) (plurality opinion)).

262. *See US Foreign Intelligence Court Did Not Deny Any Surveillance Requests Last Year*, THE GUARDIAN (Apr. 30, 2016), https://perma.cc/6FMZ-GSVT (last visited Oct. 16, 2019) (discussing developments in government surveillance in the post 9/11 era) (on file with the Washington and Lee Law Review).

263. ELIZABETH GOITEIN, THE NEW ERA OF SECRET LAW 6, 15 (2016), https://perma.cc/HY6K-D3FW (PDF).

264. *See id.*

265. HUMAN RIGHTS WATCH, DARK SIDE: SECRET ORIGINS OF EVIDENCE IN US CRIMINAL CASES 37 (Jan. 9, 2018), https://perma.cc/C5N2-CCYE (last visited Oct. 16, 2019) (on file with the Washington and Lee Law Review).

266. *Id.*

267. *See id.* ("Through a practice known as parallel construction, an official who wishes to keep an investigative activity hidden from courts and defendants—and ultimately from the public—can simply go through the motions

this obscures the true source of information against the defendant. It has been defended as protecting the identities of vulnerable confidential informants, though.

Whereas courts upholding the secrecy in these other contexts have relied on the limitations of constitutional commands, the confines of particular procedural postures, national security, and protecting informants, courts upholding the secrecy in the conviction algorithm context—at least to the extent that they have been faced by these questions—have relied on the business interests of the companies that developed the computer programs. As the judge in the *Robinson* case[268] stated, "[a]n order requiring Cybergenetics to produce the source code would be unreasonable, as release would have the potential to cause great harm to Cybergenetics."[269] This is a questionable position when you reframe the issue as one weighing the importance of accuracy in criminal convictions against the importance of maintaining the secrecy of technologies that the government has licensed to secure convictions. This is not to suggest that the technology companies should necessarily be required to publish the details of their conviction programs, but perhaps there should be limitations on the technologies that the government may use in convicting individuals—especially when there are serious questions about the accuracy and reliability of those technologies. Secrecy poses a significant hurdle with respect to probing these questions of accuracy and reliability.

C. Lay Acceptance and (Mis)Understanding of Science and Technology

Intertwined with the motivations for secrecy is the general lack of understanding of science and technology among lawyers. Many lawyers have little understanding of science and the intricacies of technology.[270] Like many Americans, most lawyers

---

of re-discovering evidence in some other way." (internal quotations omitted)).

268. *See supra* notes 231–239 and accompanying text.

269. Dang, *supra* note 137.

270. *See* Garrett M. Graff, *Government Lawyers Don't Understand the Internet. That's a Problem*, WASH. POST (Sept. 23, 2016, 11:48 AM),

rely heavily on technology in their everyday lives with the use of the internet, smartphones, and other gadgets. And in their law practices, attorneys often rely on technology when working on matters such as electronic discovery and DNA evidence. With this heavy reliance on science and technology, but with little understanding of it, the useful results in some ways seem like magic.[271] Consumers of science and technology generally lack understanding of the limits of science and technology. The same is true with computer programs and their underlying algorithms and source codes. Players within the criminal justice system frequently rely on these programs, but they generally lack enough understanding to fully comprehend the programs' limitations.[272] Instead, like much science and technology that Americans regularly encounter, criminal justice actors blindly trust these products because they are in fact the products of science and technology.[273] This trusted view of science and technology within our system has become pervasive. Indeed, one commentator has

---

https://perma.cc/WMM4-5MUD (last visited Oct. 30, 2019) ("Both federal prosecutors and the attorneys who represent executive agencies in court are bungling lawsuits across the country because they don't understand what they're talking about. Too few lawyers have the skill set or the specialized knowledge to make sense of code, networks and the people who use them . . . .") (on file with the Washington and Lee Law Review); *see also* James Podgers, *Lawyers Still Have a Lot to Learn About Technology, Ethics 20/20 Witnesses Say*, ABA J. (Feb. 3, 2012, 2:12 AM), https://perma.cc/4E2P-46BU (last visited Oct. 30, 2019) ("Lawyers don't fully appreciate how much technology is changing the nature of law practice, several witnesses said today at a public hearing conducted by the ABA Commission on Ethics 20/20.") (on file with the Washington and Lee Law Review); Ryan & Adams, *supra* note 63, at 1080 (stating that "the problems with [reliability in various] areas of forensic science are exacerbated by generally poor scientific understanding within the legal community, which has led many to ascribe undue value to dubious evidence").

271. *See* ARTHUR C. CLARKE, PROFILES OF THE FUTURE: AN INQUIRY INTO THE LIMITS OF THE POSSIBLE 21 n.1 (1962) ("Any sufficiently advanced technology is indistinguishable from magic.").

272. *See* Graff, *supra* note 270 (explaining how a changing world requires greater understanding of technology but how lawyers, who are not sufficiently trained in topics like coding, are troublingly deficient in this knowledge, leading to "bungle[d] lawsuits," "stymie[d] criminal investigations," and "misappl[ied] law").

273. *See* ROBIN FELDMAN, THE ROLE OF SCIENCE IN LAW 1 (2009) ("The allure of science has always captivated members of the legal profession. Its siren's song has followed us throughout much of American legal history.").

suggested that science has become the God of the criminal justice system; judges and lawyers seem to venerate science more than anything else in the system.[274]

Because lawyers generally trust the results of science and technology, and of criminal justice prediction and conviction programs in particular, defense lawyers often do not even consider challenging prosecutors' reliance on these secret programs. There have been some pockets of litigation related to the secrecy of these algorithms and source codes—such as with breathalyzers and PGSs[275]—but not enough. Perhaps such challenges have been stifled by the routine lack of success that challengers experience.[276]

V. A Problem of Constitutional Proportions

The secrecy of the algorithms and source codes underlying today's many conviction programs should spark concern. The dangers of this secrecy go beyond the criticisms levied against the secrecy shrouding the details of the prediction programs used in setting bail, sentencing, and making parole decisions.[277] Those criticisms have generally focused on the programs' reliance on legally questionable and morally repugnant factors that discriminate against minorities, and they have lightly touched on the issues of accuracy and reliability as well.[278] With respect to conviction programs, concerns about accuracy and reliability take center stage, as false positives in this area could amount to fining, incarcerating, or even killing innocent people.[279] Of course concerns about relying on race and its proxies, or other unacceptable factors, remain troubling, but accuracy and reliability are paramount here. And one cannot satisfactorily determine accuracy and reliability when secrecy cloaks the algorithms and source codes underlying these conviction

274. *See id.* at 119 ("Perhaps the greatest irony . . . is the place of honor and worship to which science has ascended.").

275. *See supra* Parts IV.A.1, 3.

276. *See supra* Parts IV.A.1, 3.

277. *See supra* Part II.

278. *See supra* Part II.D.

279. *See supra* notes 154–156 and accompanying text.

programs. However, in many cases, for-profit companies have created the programs prosecutors regularly employ.[280] It is not surprising, then, that these companies want to maintain the secrecy surrounding their products so that they may continue to earn profits off of them. While this makes sense from the company's perspective, it creates problems when prosecutors use these programs within the criminal justice system. If the programs remain secret, how can researchers or defendants independently test them for consistency and accuracy? If judges, prosecutors, or the companies themselves refuse to lift the veil of secrecy, how can defendants effectively challenge these programs, which may very well be the basis not just for a defendant's denial of bail, long sentence, or denial of parole, but for the defendant's conviction? Although defendants generally have access to the results of their computer-based assessments, the details of the algorithm and underlying source code that computed it are generally withheld.[281]

This secrecy poses a problem under the Fifth and Fourteenth Amendments to the Constitution, which provide that criminal defendants are entitled to due process of law prior to conviction and punishment.[282] Defendants' due process rights are in some regards quite broad, but defining the scope of these rights is sometimes difficult and requires a bit of interpretation.[283] In various areas of due process jurisprudence, courts have applied slightly different tests to determine whether there has been a due process violation. For example, in determining whether the prosecution has unfairly withheld exculpatory information, a court

---

280. *See supra* Part IV.A.

281. *See* Angwin et al., *supra* note 42; *see also supra* Part III (describing various conviction algorithms and touching on the secrecy enveloping these various cocoons surrounding the technologies employed to secure convictions).

282. *See* U.S. CONST. amend. V ("No person . . . shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law . . . ."); U.S. CONST. amend. XIV, § 1 ("No State . . . shall . . . deprive any person of life, liberty, or property, without due process of law . . . .").

283. *See* Niki Kuckes, *Civil Due Process, Criminal Due Process*, 25 YALE L. & POL'Y REV. 1, 14 (2006) (explaining that "[t]he body of criminal due process precedents is highly protective of defendants in many regards" but that, "[a]t the same time, due process hearing rights that are routine in the pretrial stages of civil cases can be absent from parallel stages of the criminal process, despite the comparable or greater interests at stake").

assesses whether the withheld information was material—whether there is a reasonable probability that disclosing it would have made a difference in the outcome at trial.[284] In the context of pre-trial publicity, the U.S. Supreme Court has held that a defendant's due process rights have been violated if a media circus may have, or actually did, infect the jury in the charging venue.[285] Common to the Court's due process cases in the criminal justice arena, though, is reliance on several values supported by this constitutional right.[286] The various constitutional values embedded in and at the core of the Court's due process cases include "adversarial testing, truth-finding,

284. *See* United States v. Bagley, 473 U.S. 667, 682 (1985) (plurality opinion) ("The evidence is material only if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different. A 'reasonable probability' is a probability sufficient to undermine confidence in the outcome."); Brady v. Maryland, 373 U.S. 83, 87 (1963) ("We now hold that the suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution.").

285. *See* Skilling v. United States, 561 U.S. 358, 398–99 (2010) (stating that "[j]urors . . . need not enter the box with empty heads in order to determine the facts impartially," explaining that "[i]t is sufficient if the jurors can lay aside their impressions or opinions and render a verdict based on the evidence presented in court," and concluding that "Skilling failed to establish that a presumption of prejudice arose or that actual bias infected the jury that tried him" (internal quotations and alterations omitted)); Sheppard v. Maxwell, 384 U.S. 333, 358 (1966) ("The carnival atmosphere at trial could easily have been avoided since the courtroom and courthouse premises are subject to the control of the court. . . . [T]he presence of the press at judicial proceedings must be limited when it is apparent that the accused might otherwise be prejudiced or disadvantaged."); Rideau v. Louisiana, 373 U.S. 723, 726 (1963) ("[I]t was a denial of due process . . . to refuse the request for a change of venue, after the people of Calcasieu Parish had been exposed repeatedly and in depth to the spectacle of Rideau personally confessing in detail to the crimes with which he was later to be charged."); *see also* Jordan Gross, *If Skilling Can't Get a Change of Venue, Who Can? Salvaging Common Law Implied Bias Principles from the Wreckage of the Constitutional Pretrial Publicity Standard*, 85 TEMP. L. REV. 575, 582–615 (2013) (chronicling the evolution of the Court's pretrial publicity jurisprudence).

286. *See* Ryan, *supra* note 145, at 421 ("Beyond the constitutional provisions themselves, though, the Court regularly relies on at least four important constitutional criminal procedural values. These are the values of adversarial testing, truth-finding, dignity, and equality.").

dignity, and equality."[287] Each of these values is important to preserving criminal defendants' due process rights.[288]

This constitutional right of due process encompasses a number of more specific rights, including the right to a fair trial, the right to be provided with exculpatory evidence known by the government, the right to present a defense, and the right to have access to resources to make out a defense.[289] In its 1973 case of *Chambers v. Mississippi*,[290] the Court explained that "[t]he right of an accused in a criminal trial to due process is, in essence, the right to a fair opportunity to defend against the State's accusations."[291] In *Chambers*, this meant that the state's evidentiary rules preventing the defendant from admitting into evidence the many confessions to the crime made by another individual unconstitutionally deprived the defendant of his due process rights.[292] More recently, in its 2006 case of *Holmes v. South Carolina*,[293] the Court reiterated the principle espoused in *Chambers*, stating that "the Constitution guarantees criminal defendants 'a meaningful opportunity to present a complete defense.'"[294] There, the Court held that the defendant's due process rights were violated when the state court refused to admit evidence that another individual confessed to the crime because, according to the state court, this evidence failed to "raise[] a reasonable

---

287. *Id.*

288. *Id.*

289. *See, e.g.*, Ake v. Oklahoma, 470 U.S. 68, 76, 86–87 (1985) (explaining that the Due Process Clause requires courts to "take steps to assure that the defendant has a fair opportunity to present his defense," which in this case meant providing the defendant with the assistance of a psychiatrist); *see also In re* Oliver, 333 U.S. 257, 273 (1948) (stating that "a person's right to reasonable notice of a charge against him, and an opportunity to be heard in his defense—a right to his day in court—are basic in our system of jurisprudence" and that "these rights include, as a minimum, a right to examine the witnesses against him, to offer testimony, and to be represented by counsel").

290. 410 U.S. 284 (1973).

291. *Id.* at 294.

292. *See id.* at 302 ("We conclude that the exclusion of this critical evidence, coupled with the State's refusal to permit Chambers to cross-examine [the confessor], denied him a trial in accord with traditional and fundamental standards of due process.").

293. 547 U.S. 319 (2006).

294. *Id.* at 324 (quoting Crane v. Kentucky, 476 U.S. 683, 690 (1986)).

inference as to the defendant's own innocence"[295] and instead "merely cast[] a bare suspicion or raise[d] a conjectural inference as to another's guilt."[296] Invoking the constitutional right to present one's defense under the Due Process Clause, the Supreme Court explained that, while states "have broad latitude . . . to establish rules excluding evidence from criminal trials, . . . the Constitution guarantees criminal defendants 'a meaningful opportunity to present a complete defense,'"[297] which limits states' rulemaking powers.[298] When a state promulgates rules that "infringe upon [this] weighty interest of the accused,"[299] it risks depriving the defendant of this important right.[300]

The Court has even extended this right to present a defense to include providing indigent defendants with the resources to do so. In *Ake v. Oklahoma*,[301] the Court explained that the "due process guarantee of fundamental fairness . . . derives from the belief that justice cannot be equal where, simply as a result of his poverty, a defendant is denied the opportunity to participate meaningfully in a judicial proceeding in which his liberty is at stake."[302] Accordingly, if a defendant cannot afford the tools necessary to meaningfully present his defense, the government "must take steps to assure that [he] has a fair opportunity" to do so."[303] The Court has applied this principle to provide defendants with copies of their district court transcripts,[304] waive the fee to file for

---

295. *Id.* at 323.

296. *Id.* at 323–24.

297. *Id.* at 324.

298. *See id.* (stating that states' latitude "to establish rules excluding evidence from criminal trials . . . has limits").

299. *Holmes*, 547 U.S. at 324.

300. *Id.*

301. 470 U.S. 68 (1985).

302. *Id.* at 76.

303. *Id.*

304. *See* Griffin v. Illinois, 351 U.S. 12, 19 (1956); *see also* Ake v. Oklahoma, 470 U.S. 68, 76 (1985) (relying on the *Griffin* case as partial precedent for the decision).

appeal,[305] provide defendants with effective assistance of counsel,[306] and the assistance of a psychiatrist.[307]

The constitutional right to be provided the opportunity to present a complete defense is closely related to the Confrontation Clause right firmly embedded in the Sixth Amendment[308] and recently expounded on by the Court in *Crawford v. Washington*[309] and its progeny. In *Crawford*, the Court clarified that the Confrontation Clause requires that out-of-court statements that are testimonial in nature be inadmissible at trial unless "the declarant was unavailable to testify . . . and the defendant had had a prior opportunity for cross-examination."[310] In *Melendez-Diaz v. Massachusetts*[311] and *Bullcoming v. New Mexico*,[312] the Court built on this groundbreaking case to establish that, even when a party presents forensic testimony at trial, the author of the relevant forensic report must also testify at trial.[313] Referencing these same

---

305. *See* Burns v. Ohio, 360 U.S. 252, 258 (1959); *see also Ake*, 470 U.S. at 76 (relying on *Burns* as partial precedent for the decision).

306. *See* Strickland v. Washington, 466 U.S. 668, 685 (1984); Gideon v. Wainwright, 372 U.S. 335, 339–40 (1963); *see also Ake*, 470 U.S. at 76 (relying on *Burns* as partial precedent for the decision).

307. *See Ake*, 470 U.S. at 86–87 ("We therefore conclude that Ake also was entitled to the assistance of a psychiatrist on this issue and that the denial of that assistance deprived him of due process.").

308. The Sixth Amendment provides that, "[i]n all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him." U.S. CONST. amend. VI.

309. 541 U.S. 36 (2004).

310. *Id.* at 53–54, 68. The Court also noted that this rule "does not bar the use of testimonial statements for purposes other than establishing the truth of the matter asserted . . . ." *Id.* at 59 n.9; *see also* Williams v. Illinois, 567 U.S. 50 (2012) (plurality opinion) (stating that "*Crawford* . . . took pains to reaffirm the proposition that the Confrontation Clause 'does not bar the use of testimonial statements for purposes other than establishing the truth of the matter asserted'").

311. 557 U.S. 305 (2009).

312. 564 U.S. 647 (2011).

313. *See id.* at 651–52 (concluding that live testimony of a forensic analyst who did not perform the relevant forensic testing was insufficient to meet the requirements of the Confrontation Clause); *Melendez-Diaz*, 557 U.S. at 307, 329 (holding that "affidavits reporting the results of forensic analysis which shows that material seized by the police and connected to the defendant was cocaine" constituted testimonial statements, which rendered them inadmissible under the Sixth Amendment Confrontation Clause and *Crawford* because the declarant was

ideas, the *Holmes* Court[314] noted that the right to have a meaningful opportunity to present a complete defense could be rooted in the Confrontation Clause of the Sixth Amendment in addition to the Fifth and Fourteenth Amendment Due Process Clauses.[315] In fact, even in *Chambers*—which the Court decided long before the *Crawford* case—the Court found that "[t]he rights to confront and cross-examine witnesses and to call witnesses in one's own behalf have long been recognized as essential to due process."[316]

Defendants' inabilities to gain access to information that may be essential to presenting a complete defense thus poses a significant constitutional concern under both the Due Process Clauses and the Confrontation Clause. Pursuant to the Due Process Clauses, greater information about the algorithms and source codes underlying the computer programs generating breathalyzer, fingerprint, and DNA evidence against criminal defendants could very well be crucial to these defendants' defenses. Without access to this information, criminal defendants are denied the "fair opportunity to defend against the State's accusations" to

---

not unavailable and the defense had not had the opportunity to cross-examine the declarant). The Court muddied the waters somewhat when it determined in *Williams v. Illinois*, 567 U.S. 50 (2012), that there was no Confrontation Clause defect when the prosecution's expert relied on the report of an outside laboratory—a report that developed a DNA profile of a rapist from the victim's vaginal swabs—to conclude that the defendant's DNA profile matched the DNA profile developed by the outside laboratory. *See generally* Williams v. Illinois, 567 U.S. 50 (2012). Although five Justices voted in favor of not finding a Confrontation Clause problem, they could not agree on the reasoning. As Justice Kagan explained in dissent, the *Williams* case "left significant confusion in [its] wake." *Id.* at 141. It now seems that *Melendez-Diaz* and *Bullcoming* "no longer mean all that they say," but "no one can tell in what way or to what extent they are altered because no proposed limitation commands the support of a majority." *Id.* Justice Kagan (along with Justices Scalia, Ginsburg, and Sotomayor) thus concluded that, "until a majority of th[e] Court reverses or confines those decisions, [one should] understand them as continuing to govern, in every particular, the admission of forensic evidence." *Id.*

314. Holmes v. South Carolina, 547 U.S. 319 (2006).

315. *See id.* at 324 ("Whether rooted directly in the Due Process Clause of the Fourteenth Amendment or in the Compulsory Process or Confrontation Clauses of the Sixth Amendment, the Constitution guarantees criminal defendants 'a meaningful opportunity to present a complete defense.'" (quoting Crane v. Kentucky, 476 U.S. 683, 690 (1986))).

316. Chambers v. Mississippi, 410 U.S. 284, 294 (1973).

which *Chambers* and *Holmes* held they are entitled."[317] At the same time, withholding this information about the underlying algorithms and computer source codes violates the related Confrontation Clause.[318] The State is presenting testimonial information—whether that be in the form of breathalyzer, fingerprint, DNA, or other evidence—against the defendant without allowing the defendant to truly confront the witnesses against him as the Sixth Amendment requires.[319] The forensic examiner in these cases is not the true witness, or at least not the only witness, against the defendant. Instead, the forensic examiner is relying heavily on the conviction program's underlying algorithm and source code in concluding that the defendant's blood or breath alcohol content is at a particular level, that his fingerprint is a match to the one left on the murder weapon, or that his DNA matches the DNA left at the crime scene.[320] Often, the forensic examiner is not even entirely aware of how the algorithm and source code reach their results.[321] Instead, the examiner may understand only how he must set up the test and how to interpret the results reached by the algorithm and source code embedded in the computer program. Cross-examination may thus reveal the examiner's mistakes, incompetency, or even fraud,[322] but the

317. *Id.* at 294; *see also Holmes*, 547 U.S. at 324 (stating that "the Constitution guarantees criminal defendants 'a meaningful opportunity to present a complete defense.'" (quoting Crane v. Kentucky, 476 U.S. 683, 690 (1986))).

318. Professor Andrea Roth has argued that "[a]llowing the state to build or harness machines to render accusations, without also providing the defendant a constitutional right to test the credibility of those machine sources, resembles trial by ex parte affidavit"—one of the primary concerns that animated the drafting and ratification of the Confrontation Clause. *See* Roth, *supra* note 113, at 2041, 2043.

319. *See* U.S. CONST. amend. VI (providing that, "[i]n all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him"); *see also supra* notes 308–316 and accompanying text (explaining how the Court has interpreted the Sixth Amendment in *Crawford v. Washington*, 541 U.S. 36 (2004) and its progeny). Some scholars disagree, though, on whether machines, themselves, are "witnesses" under the language of the Sixth Amendment. *See* Roth, *supra* note 113, at 2040.

320. *See supra* Parts III.A.1–2.

321. *See supra* notes 118–119 and accompanying text.

322. *See Bullcoming*, 564 U.S. 647, 661–62 (2011) (explaining that confrontation was necessary to "expose any lapses or lies on the certifying

examiner would not be able to sufficiently answer any questions the defense might pose related to how the conviction program reached its conclusions. And any answer the examiner might espouse would likely be based on training materials provided to him—statements provided by the creator of the test—which likely would not divulge details about the proprietary algorithm or source code. Such examiner statements would be insufficient to meet the requirements of the Sixth Amendment as explained by *Crawford* and its progeny.[323]

As the Supreme Court acknowledged in *Melendez-Diaz* and *Bullcoming*, requiring additional expert testimony on the part of the prosecution could pose practical problems. In those cases, the Court was addressing the prosecution's concerns that requiring forensic examiners to testify to the results of drug analyses and blood tests would be overly burdensome.[324] The Court, however, explained that constitutional requirements like those imposed by the Confrontation Clause "may not disregard [such constitutional provisions] at our convenience,"[325] and only a small percentage of cases proceed to trial anyway, significantly reducing the burden alleged by the prosecution.[326] Attempting to mitigate such possible

---

analyst's part"); Melendez-Diaz v. Massachusetts, 557 U.S. 305, 319 (2009) ("Confrontation is designed to weed out not only the fraudulent analyst, but the incompetent one as well. Serious deficiencies have been found in the forensic evidence used in criminal trials.").

323. The prosecution could potentially circumvent the Confrontation Clause requirements by calling an expert to testify about a matter and, in doing so, relying on and referring to a secret conviction program's output. *See generally* Williams v. Illinois, 567 U.S. 50 (2012) (plurality opinion) (finding no constitutional defect in a similar circumstance). In *Williams v. Illinois*, the Court found no violation of the Confrontation Clause in a similar situation, either because the expert's reference to the underlying report was not offered to prove the truth of the matter asserted, or because the reference, had it been admitted for that purpose, was not testimonial in nature. *See id.* at 57–59. A majority of the Justices could not agree on the reasoning for the decision, leaving the precedential value of the case unclear. *See id.* at 141 (Kagan, J., dissenting).

324. *See Bullcoming*, 564 U.S. at 665; *Melendez-Diaz*, 557 U.S. at 325.

325. *Melendez-Diaz*, 557 U.S. at 325; *see Bullcoming*, 564 U.S. at 665 (quoting *Melendez-Diaz*, 557 U.S. at 325).

326. *See Bullcoming*, 564 U.S. at 667; *see also Melendez-Diaz*, 557 U.S. at 325. Further, the Court stated that "[p]erhaps the best indication that the sky will not fall [when enforcing the Confrontation Clause] . . . is that it has not done so already. Many States have already adopted the constitutional

inconveniences in the *evidentiary* context, a number of states have addressed the issue of the accuracy and reliability of conviction program software and outputs through statutes and rules concluding that particular tools, and their underlying source codes and algorithms, are admissible at trial without a predicate showing of their validity in each case.[327] In *Underdahl*, for example, a relevant state statute provided that "the results of a breath test, when performed by a person who has been fully trained in the use of an . . . approved breath-testing instrument, . . . are admissible in evidence without antecedent expert testimony that . . . [the] instrument provides a trustworthy and reliable measure of the alcohol in the breath."[328] And pursuant to a state rule, the relevant breathalyzer was approved for use statewide.[329] State procedures authorizing particular instruments, though, are far from transparent, and, as the litigation related to the *Underdahl* case demonstrates, states have approved instruments that do indeed produce inaccurate results, at least in some circumstances.[330] Further, prior authorization via statute or rule does not resolve the Confrontation Clause matter. A defendant is still being tried based on secret algorithms and source codes, and he is not being given the opportunity to ask questions and receive answers from individuals who have knowledge about this secret material; he thus lacks an opportunity to sufficiently confront witnesses against him and defend against this inculpatory evidence. As *Melendez-Diaz* and *Bullcoming* made clear, whether compliance with the constitutional requirements creates burdens for the state does not justify disregarding the constitutional rules.

---

rule . . . announce[d]" in *Melendez-Diaz*. *Melendez Diaz*, 557 U.S. at 325.

327. *See* Imwinkelried, *supra* note 178, at 112 (explaining that, "[u]nless the court invalidates the statute on some constitutional ground, the[se] statute[s] eliminate[] the need for the prosecution to present any foundational testimony about the empirical validity of the technique").

328. MINN. STAT. § 634.16.

329. *See* Minn. R. 7502.0420, subpart 3 (repealed).

330. *See In re* Source Code Evidentiary Hearings in Implied Consent Matters, 816 N.W.2d 525, 536 (Minn. 2012) (referencing "[t]he district court['s] determin[ation] . . . that the source code of the instrument did impact the reliability of Intoxilyzer 5000EN instruments that reported a 'deficient sample' while running the 240 software").

In addition to the primary concerns related to a defendant's opportunity to make a complete defense and to confront witnesses against him, the secrecy surrounding today's secret conviction programs raises some questions under the doctrine flowing from the Supreme Court's case of *Brady v. Maryland*[331] and the disclosure obligations under various jurisdictions' discovery rules. *Brady* and its progeny provide that a defendant's due process rights are violated if the prosecution withholds exculpatory or impeachment evidence favorable to the accused if that evidence was material—if "its suppression undermines confidence in the outcome of the trial."[332] Beyond just the relevant exculpatory material within its own possession or knowledge, though, the prosecution is charged with disclosing exculpatory material within the knowledge of agents acting on its behalf, such as police officers and forensic examiners.[333] Translating this doctrine to the employment of PGSs in criminal cases illustrates the difficulties that these conviction programs create. If a PGS acts on behalf of the prosecution in analyzing a DNA mixture to determine the relative likelihoods that the defendant was a contributor to the

---

331. 373 U.S. 83 (1963).

332. *See* United States v. Bagley, 473 U.S. 667, 674–78 (1985) ("Consistent with 'our overriding concern with the justice of the finding of guilt,' a constitutional error occurs, and the conviction must be reversed, only if the evidence is material in the sense that its suppression undermines confidence in the outcome of the trial."); *Brady*, 373 U.S. at 87 ("We now hold that the suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution.").

333. *See* Kyles v. Whitley, 514 U.S. 419, 437 (1995)

> [T]he prosecution, which alone can know what is undisclosed, must be assigned the consequent responsibility to gauge the likely net effect of all such evidence and make disclosure when the point of "reasonable probability" is reached. This in turn means that the individual prosecutor has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case, including the police.

See also John v. People, S. Ct. Crim. No. 2014-0030, 2015 WL 5622212, at *5 (V.I. Sept. 24, 2015) ("The prosecutor is presumed to have knowledge of all relevant and material information within the actual knowledge and possession of other agencies outside of the prosecutor's office where these agencies have collaborated with the prosecution as . . . part of the investigative team, such as the police department or forensic lab.").

sample versus another individual, then the prosecution should be charged with the potentially exculpatory and impeachment evidence buried in the PGS's algorithms and source codes. But without transparency between at least the PGS developer and the prosecution, the prosecutor is not in a position to fulfill his constitutional and ethical duties with respect to disclosure. Where state discovery rules require the prosecution to maintain an open file,[334] similar logic indicates that the prosecution should provide the accused with information on the conviction programs' algorithms and source codes.

Ultimately, defendants' due process and confrontation rights suggest that the algorithms and source codes underlying secret conviction programs should be disclosed. It is only with access to this information that defendants and their counsel and experts can examine whether the evidence used against them is valid. There are a variety of ways by which transparency could be achieved, and it would not necessarily have to jeopardize the business interests of the companies producing these important technologies.[335] Indeed, the government could provide this information under seal or pursuant to a protective order;[336] or, perhaps more appropriately, the companies could include the value of disclosure in their bargains with the government to use the programs or use

---

334. *See, e.g.*, N.C. GEN. STAT. ANN. § 15A-903 ("Upon motion of the defendant, the court must order . . . [t]he State to make available to the defendant the complete files of all law enforcement agencies, investigatory agencies, and prosecutors' offices involved in the investigation of the crimes committed or the prosecution of the defendant."); TEX. CRIM. PROC. CODE ANN. § 39.14

> Subject to [certain] restrictions . . . as soon as practicable after receiving a timely request from the defendant the state shall produce and permit the inspection of any . . . documents . . . that constitute or contain evidence material to any matter involved in the action and that are in the possession, custody, or control of the state or any person under contract with the state.

335. In fact, as Professor Edward Imwinkelried has explained, a company's exposure risk for the wrongful disclosure of a trade secret is small in the context of disclosure pursuant to a criminal prosecution. *See* Imwinkelried, *supra* note 178, at 127–28. The risk is much higher when a company is ordered to disclose a trade secret to its competitors—those "with economic interests directly adverse to those of the owner of the trade secret." *Id.* at 128.

336. For a discussion of how parties have disclosed trade secrets pursuant to protective orders and other protective measures in different types of cases, see *id.* at 125–28.

the resulting analyses in court. The government could perhaps pay a premium for an exclusive license to the software. Whatever the method, only greater transparency can satisfy defendants' constitutional guarantees.

A courtroom may not be the best crucible in which to determine the accuracy and reliability of these types of technology. Experts, rather than lay judges and jurors, could very likely reach more reliable conclusions on this subject of accuracy. And defense lawyers would most certainly welcome peer review of the various conviction programs. But, while accuracy and reliability are crucial here, they are not the only priority. Rather, the constitutional rights of individual defendants are equally, if not more, important.[337] And courtrooms are the proper venues for jealously guarding these rights. While truth-finding has increasingly become the predominant value in discussions across the criminal justice system, we should not let this goal blind us from other important interests. As William Blackstone once said, it is "better that ten guilty persons escape, than that one innocent suffer."[338] Even in the world of high-powered DNA analysis, absolute certainty of truth—and thus absolute certainty of whether a defendant is guilty—is generally unobtainable.[339] We can achieve probabilities and likelihoods, but absolute certainty is difficult.[340] In wading into the statistics involved in determining the likelihood of a defendant's guilt, it is important to safeguard the principle that the risk of wrongful conviction should weigh heavier than the risk of wrongful exoneration.

---

337. *See* Ryan, *supra* note 145, at 433 ("[T]here are values beyond just truth-finding that should not be forgotten. Just like we sacrifice truth for the sake of privacy when a judge excludes probative evidence that was found in violation of the Fourth Amendment, values such as dignity remain important even aside from their relationship to truth."); *see also supra* notes 286–288 and accompanying text (explaining that the constitutional values of "adversarial testing, truth-finding, dignity, and equality" are "embedded in and at the core of the Court's due process cases").

338. 4 WILLIAM BLACKSTONE, COMMENTARIES *352; *see also* Alexander Volokh, *N Guilty Men*, 146 U. PA. L. REV. 173 (1997) (exploring the "Blackstone ratio" of ten to one).

339. *See* Ryan, *supra* note 145, at 429 ("Despite our advances in science and technology, truth may be difficult to come by. And certainty of truth is generally impossible.").

340. *See id.* at 429.

VI. Conclusion

Commentators have paid significant attention to the algorithms, and maybe even the source codes, underlying computerized prediction programs that judges and parole boards have used to aid in setting bail, sentencing, and determining whether to release offenders from prison. These programs deserve this attention because they are potentially based on illegal or morally repugnant discriminators like race and because there are real, and often overlooked, questions about the accuracy and reliability of these programs. But even more concerning are the secret conviction programs that prosecutors are quietly using to secure convictions in criminal cases. Judges, prosecutors, and the businesses that developed these programs have generally refused to disclose the details of the algorithms and source codes powering these conviction programs, and this secrecy raises real constitutional concerns. Defendants' due process and confrontation rights entitle them to have meaningful opportunities to present full defenses and to confront the witnesses against them. But, without transparency of the algorithms and source codes embedded in the conviction programs, defendants cannot truly probe the evidence presented against them. They lack the opportunity to investigate whether the algorithms are sound, the source codes are error-free, and the programs produce accurate and reliable results. They also lack the opportunity to cross-examine individuals who truly know the inner workings of the programs to again determine accuracy and reliability. Transparency is thus necessary to protect these defendants' constitutional rights.