Georgia State University Law Review

Volume 34
Issue 4 *Summer 2018*

Article 2

8-1-2018

The First Amendment Case for Public Access to Secret Algorithms Used In Criminal Trials

Vera Eidelman
American Civil Liberties Union, vera.eidelman@gmail.com

THE FIRST AMENDMENT CASE FOR PUBLIC ACCESS TO SECRET ALGORITHMS USED IN CRIMINAL TRIALS

Vera Eidelman*

INTRODUCTION

Last year, a New York court convicted a man named Mayer Herskovic of gang assault and sentenced him to four years in prison.[1] A few years earlier, across the country, a California court found another man named Billy Ray Johnson guilty of twenty-four crimes, including multiple counts of rape; the court sentenced Mr. Johnson to life in prison without parole and 300 years to life, plus 123 years.[2] The two cases have little in common—except that both men were convicted on the basis of a new and largely untested method of processing tiny bits of DNA. In Mr. Johnson's case, that was notwithstanding the fact that a witness to one of the alleged crimes reported that the perpetrator was a "light-skinned Hispanic with green eyes," and Mr. Johnson is Black with brown eyes.[3] In both cases, the prosecution relied on DNA statistics generated by proprietary probabilistic genotyping programs—computerized

* William J. Brennan Fellow, American Civil Liberties Union's Speech, Privacy & Technology Project. The Author is counsel for *amici curiae* in a criminal case involving forensic evidence derived from a secret algorithm. *See* Brief of Amici Curiae American Civil Liberties Union et al. at 11, People v. Johnson, No. F071640 (Cal. Ct. App. Sept. 13, 2017). She is indebted to her co-counsel on that brief—Brett Max Kaufman, Brandon Buskey, Rachel Goodman, and Andrea Woods—for their ideas, mentorship, and support. She is also grateful to Esha Bhandari for her thoughtful feedback, and to the staff of the *Georgia State University Law Review* for their diligent editing. The views set forth herein are the Author's personal views and do not reflect those of the ACLU.

1. Lauren Kirchner, *Traces of Crime: How New York's DNA Techniques Became Tainted*, N.Y. TIMES (Sept. 4, 2017), https://www.nytimes.com/2017/09/04/nyregion/dna-analysis-evidence-new-york-disputed-techniques.html [https://perma.cc/K9ZE-Z2AF].

2. Jason Kotowski, '*Eastside Rapist' Billy Ray Johnson to Spend Rest of his Life Behind Bars*, BAKERSFIELD CALIFORNIAN (May 19, 2015), http://www.bakersfield.com/news/eastside-rapist-billy-ray-johnson-to-spend-rest-of-his/article_c1d62989-e01b-5043-8233-9cb7524a4028.html [https://perma.cc/RA4Q-49H9]. As a Fellow at the American Civil Liberties Union, the Author is counsel for *amici curiae* in Mr. Johnson's case. *See* Brief of Amici Curiae American Civil Liberties Union et al. at 11, People v. Johnson, No. F071640 (Cal. Ct. App. Sept. 13, 2017). [hereinafter "ACLU Amicus Brief"].

3. Kotowski, *supra* note 2.

algorithms used to identify a suspect from a tiny, degraded DNA sample swimming in a soup of many individuals' DNA. Both cases are now on appeal, in part based on concerns about those stastics and their underlying algorithms.[4]

In today's world, computerized algorithms impact our lives in crucial ways. Such algorithms can decide whether we get a job interview,[5] go to a particular college,[6] access credit,[7] and receive insurance.[8] They can also inform what news we see[9] and what beliefs we hold.[10] And, as shown by the examples above, it is not only private actors who are using computerized algorithms. Increasingly, the government is too.

In fact, the government now relies on algorithms to make profound decisions about our lives, including what level of health benefits we receive,[11] whether we can work for the government,[12] what risk we

4. California v. Johnson, No. F071640 (Cal. Ct. App. appeal docketed June 1, 2015) (Mr. Johnson's appeal); *see* Lauren Kirchner, *ProPublica Seeks Source Code for New York City's Disputed DNA Software*, PROPUBLICA (Sept. 25, 2017, 7:54 PM), https://www.propublica.org/article/propublica-seeks-source-code-for-new-york-city-disputed-dna-software [https://perma.cc/6G6B-57TU] (discussing Mr. Herskovic's appeal).

5. Gideon Mann & Cathy O'Neil, *Hiring Algorithms Are Not Neutral*, HARV. BUS. REV. (Dec. 9, 2016), https://hbr.org/2016/12/hiring-algorithms-are-not-neutral [https://perma.cc/BHY3-YAVK].

6. Cathy O'Neil, *How Big Data Transformed Applying to College*, SLATE (Sept. 15, 2016, 1:10 PM), http://www.slate.com/articles/business/moneybox/2016/09/how_big_data_made_applying_to_college_tougher_crueler_and_more_expensive.html [https://perma.cc/A2UT-V79T].

7. Kaveh Waddell, *How Algorithms Can Bring Down Minorities' Credit Scores*, ATLANTIC (Dec. 2, 2016), https://www.theatlantic.com/technology/archive/2016/12/how-algorithms-can-bring-down-minorities-credit-scores/509333/ [https://perma.cc/C7S4-PU4P].

8. Oliver Ralph, *Insurance: Robots Learn the Business of Covering Risk*, FIN. TIMES (May 16, 2017), https://www.ft.com/content/e07cee0c-3949-11e7-821a-6027b8a20f23 [https://perma.cc/UH8W-2CHE].

9. Julia Carrie Wong, *Facebook Overhauls News Feed in Favor of 'Meaningful Social Interactions*,*'* GUARDIAN (Jan. 11, 2018, 9:31 PM), https://www.theguardian.com/technology/2018/jan/11/facebook-news-feed-algorithm-overhaul-mark-zuckerberg [https://perma.cc/4RPL-ZEL7].

10. Tom Simonite, *Machines Taught by Photos to Learn Sexist View of Women*, WIRED (Aug. 21, 2017, 9:00 AM), https://www.wired.com/story/machines-taught-by-photos-learn-a-sexist-view-of-women/ [http://perma.cc/Z5C9-LEUG].

11. Across the country, states are relying on proprietary algorithms to allocate Medicaid benefits. A number of courts have expressed skepticisim regarding the constitutionality of such algorithms. *See, e.g.*, Michael T. v. Bowling, No. 2:15-CV-09655, 2016 WL 4870284, at *10 (S.D. W. Va. Sept. 13, 2016) (finding that the proprietary algorithm used by government to set Medicaid benefits "present[s] a serious risk of resulting in erroneous determinations and deprivations"). At least one court has held that such algorithms violate due process. K.W. v. Armstrong, 180 F. Supp. 3d 703, 718 (D. Idaho 2016) (holding that the proprietary tool used to allocate Medicaid benefits "arbitrarily deprives participants of

pose as parents,[13] whether or not we get charged with a crime,[14] and how we should be treated if we do get charged with a crime.[15] Although the government creates and maintains some of these algorithms, many are built by private actors who have a business interest in keeping them secret from competitors.[16] And it is now increasingly common for courts to allow the owners of proprietary algorithms who cry "trade secret!" to keep the details of the algorithms hidden, both from the public and from private litigants (including accused individuals like Mr. Johnson and Mr. Herskovic).[17]

---

their property rights and hence violates due process").

12. Similarly, another court held that the use of an algorithm to determine whether or not to fire teachers could violate their due process rights. Houston Fed'n of Teachers, Local 2415 v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1180 (S.D. Tex. 2017).

13. *See, e.g.*, Virginia Eubanks, *A Child Abuse Prediction Model Fails Poor Families*, WIRED (Jan. 16, 2018), https://www.wired.com/story/excerpt-from-automating-inequality/ [https://perma.cc/J75F-BDUY] (noting that Pittsburgh's "Allegheny Family Screening Tool," which the city uses to identify children at risk of abuse or neglect, unfairly targets low-income and minority families); Dan Hurley, *Can an Algorithm Tell When Kids Are in Danger?*, N.Y. TIMES MAG. (Jan. 2, 2018), https://www.nytimes.com/2018/01/02/magazine/can-an-algorithm-tell-when-kids-are-in-danger.html [https://perma.cc/Q9NS-GFRS] (discussing use of algorithm by Pittsburgh child protective services and noting that the private company's refusal to disclose components of child-welfare alghorithm led Illinois Department of Children and Family Services to stop using the program).

14. *See* discussion of probabilistic genotyping algorithms *infra* Section I.

15. TIM BRENNAN ET AL., ENHANCING PRISON CLASSIFICATION SYSTEMS: THE EMERGING ROLE OF MANAGEMENT INFORMATION SYSTEMS, NAT'L INST. CORRECTIONS 9 (2004), https://info.nicic.gov/nicrp/system/files/019687.pdf [https://perma.cc/77T8-5NRA] (encouraging use of algorithms to classify incarcerated individuals for housing, treatment, and resource allocation).

16. Lauren Kirchner, *Where Traditional DNA Testing Fails, Algorithms Take Over*, PROPUBLICA (Nov. 4, 2016, 8:00 AM), https://www.propublica.org/article/where-traditional-dna-testing-fails-algorithms-take-over [https://perma.cc/B48T-ULCW] (explaining that STRmix was developed by a New Zealand-Australia collaborative and is sold in the United States by a company called Nichevision, and TrueAllele is owned and marketed by a company called Cybergenetics); *see also* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. (forthcoming 2018) (manuscript at 7 n.21) (draft available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2920883) [https://perma.cc/5B2A-X9TG] (noting that "STRmix is sold for profit around the world").

17. *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, 100–01 (2016) (identifying "two primary waves" of criminal cases raising the issue of a trade secret's privilege, including the current wave); Jennifer N. Mellon, *Manufacturing Convictions: Why Defendants Are Entitled to the Data Underlying Forensic DNA Kits*, 51 DUKE L.J. 1097, 1116–19 (2001) (noting that courts have upheld trade secret privilege "in the context of DNA kit testing"); Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CAL. L. REV. 721, 729 (2007) (noting that traditional DNA typing also "weathered a series of challenges related to the reluctance of private companies to divulge claimed proprietary secrets"); Wexler, *supra* note 16, at 14–18, 41–44 (describing recent cases denying defense motions for the disclosure of

But, as this Article sets forth, once a computerized algorithm is used by the government, constitutional rights may attach.[18] And, at the very least, those rights require that algorithms used by the government as evidence in criminal trials be made available—both to litigants and the public.

Scholars have discussed how the government's refusal to disclose such algorithms runs afoul of defendants' constitutional rights,[19] but few have considered the public's interest in these algorithms—or the widespread impact that public disclosure and auditing could have on ensuring their quality.[20]

This Article aims to add to that discussion by setting forth a theory of the public's First Amendment right of access to algorithms used as evidence in criminal trials. This Article uses probabilistic genotyping programs as an illustrative example, largely because the creators of these algorithms have most aggressively pushed to keep them secret.[21] Section I begins by defining the relevant terms, including computerized algorithms, probabilistic genotyping program, machine learning, and source code. Section II describes the roles that humans play in designing, building, operating, and communicating the results of such algorithms—and the variety of errors and mistakes that almost inevitably result. Section III summarizes caselaw articulating the public's First Amendment right of access and suggests how and

---

purported trade secret evidence used to determine guilt at trial, including probabilistic genotyping algorithms and tracing emergence of "the criminal trade secret privilege" in the 1990s, followed by a second wave in mid-2000s regarding the breathalyzer source code, and again now regarding probabilistic genotyping algorithms).

18. *See, e.g.*, Houston Fed'n of Teachers, Local 2415 v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1171 (S.D. Tex. 2017); K.W. v. Armstrong, 180 F. Supp. 3d 703, 715 (D. Idaho 2016); T. v. Bowling, No. 2:15-CV-09655, 2016 WL 4870284, at *7 (S.D. W. Va. Sept. 13, 2016); State v. Loomis, 881 N.W.2d 749, 759–60, 763 (Wis. 2016) (recognizing that use of a risk assessment tool without disclosing its source code involves "potential due process violations").

19. *See* Christian Chessman, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CAL. L. REV. 179, 219–21 (2017); Imwinkelried, *supra* note 17, at 118; Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 2043–45 (2017); *see also* Mellon, *supra* note 17, at 1122–37 (2001) (identifying compulsory process, confrontation clause, and due process arguments for requiring defense access to the data underlying traditional DNA testing); Murphy, *supra* note 17, at 791 (raising due process and assistance of counsel arguments in the context of access to information about traditional DNA testing).

20. *See infra* Section III.A.

21. *See infra* note 34.

why that right should attach to computerized algorithms used as evidence in criminal trials.

I. Computerized Algorithms Explained

A. Algorithms Broadly

At the most elementary level, an algorithm is a series of steps that transforms inputs into an output.[22] It is, essentially, a formula, a manual, a recipe. Something as simple as a blog post explaining how to boil an egg is an algorithm because it directs the transformation of inputs (a saucepan, a stovetop, water, a raw egg, and possibly other inputs) into the desired output (a cooked egg). A probabilistic genotyping program is an example of a more complicated algorithm. It sets forth the steps to transform inputs, described in detail below, into an output: a statistic that establishes the likelihood that a particular suspect is the source of a specific (typically small and often degraded) DNA sample contained in a mixture of multiple peoples' DNA.

Not all algorithms aimed at accomplishing the same goal are identical. Indeed, they often differ in terms of both inputs and steps due to differences in their underlying assumptions. For example, a boiled egg can be made with or without salt or ice water and can be cooked for different amounts of time. Each approach constitutes an egg-making algorithm—but, critically, the quality of the result may differ.

Similarly, the algorithms used to generate a DNA match statistic differ due to differences in underlying assumptions, inputs, and training datasets—and so too must the quality of their output. And, of course, differences in quality of DNA statistics that are introduced at trial to put human beings behind bars or even render them eligible for death are of an entirely different order. Despite that, as discussed further below, the quality of that output is far more difficult to assess than is the quality of a hard boiled egg because of the issue at the

22. *See* THOMAS CORMEN ET AL., INTRODUCTION TO ALGORITHMS 5 (3d ed. 2009).

center of this article: the public lacks access to information about the algorithms.

B. Computerized Algorithms

The phrase computerized algorithms refers to the growing subcategory of algorithms that determine their steps and parameters not only from human assumptions but also machine learning. Machine learning occurs when a computer identifies patterns from a preexisting or training set of data, learns from those patterns, and incorporates the lessons into the algorithm. Probabilistic genotyping programs fall within this subset because they combine human assumptions and machine learning.

As noted above, the desired output for probabilistic genotyping programs is a statistic that expresses the likelihood that a particular suspect is the source of a specific DNA sample—usually a tiny, degraded sample swimming in a larger pool of many individuals' genetic material. These samples can be scraped from, for example, a convenience store counter, a purse strap, a knife handle, or a bike's handlebars.[23] This step is done as it always has been: law enforcement collects the sample and then a lab amplifies it for analysis.[24] From there, however, probabilistic genotyping diverges from traditional forensic DNA analysis.[25]

Although traditional DNA analysis looks for a match to a single person's known genetic profile, probabilistic genotyping must first sketch that profile—based on the algorithms' inputs, discussed below—before searching for a match.[26] Essentially, using traditional DNA analysis is like looking at a photograph, while using a probabilistic genotyping algorithm is like relying on an investigator's composite sketch.[27] Proponents of these programs contend that they

23. Kirchner, *supra* note 16; Liz Robbins, *Helping Decide Guilt or Innocence*, N.Y. TIMES (Dec. 15, 2012), http://www.nytimes.com/2012/12/16/nyregion/a-forensic-tool-helps-decide-guilt-or-innocence.html [https://perma.cc/PL4G-756S].

24. Katherine L. Moss, *The Admissibility of Trueallele: A Computerized DNA Interpretation System*, 72 WASH. & LEE L. REV. 1033, 1059–60 (2015).

25. *Id.*

26. *See* Roth, *supra* note 19, at 2018–19.

27. *See* ACLU Amicus Brief, *supra* note 2.

make it possible to generate matches from precisely the sort of samples that traditional DNA analysis cannot reach, while critics contend that their reliability is uncertain.[28]

Probabilistic genotyping algorithms typically express their output as a likelihood ratio, a statistic that is computed by dividing (1) the estimated probability that the owner of the DNA in the tested sample has the suspect's DNA profile by (2) the probability that a random person of a particular race or ethnicity has the suspect's DNA profile.[29] Or, as one court explained,

> the numerator . . . represents the chance that the prosecution hypothesis is true—that a particular individual was one of the contributors to a mixture. The denominator represents the chance that the defense hypothesis is true—that other random individuals, and not the one of interest to the prosecution, were the contributors. Division of the numerator by the denominator produces the likelihood ratio.[30]

Thus, the goal of probabilistic genotyping programs is the same, but the inputs and precise steps (and therefore, resulting outputs) vary across programs. How they differ is something of a mystery, though, because many are not public. Two of the most popular programs—STRmix, which claims 54% of the U.S. market share,[31] and TrueAllele, which had been used in approximately 500 criminal cases by 2016[32]—are marketed to governments for profit.[33] And the companies behind them refuse to disclose the precise components of

28. Kirchner, *supra* note 16; Robbins, *supra* note 23.

29. *See* William C. Thompson et al., *Forensic DNA Statistics: Still Controversial in Some Cases*, 2012 CHAMPION 12, 23 n.17, http://ssrn.com/abstract=2214459 [https://perma.cc/VU96-BZMN].

30. People v. Collins, 15 N.Y.S.3d 564, 577 (N.Y. Sup. Ct. 2015).

31. Wexler, *supra* note 17, at 66.

32. Imwinkelried, *supra* note 17, at 100–01.

33. *See* Kirchner, *supra* note 16 (explaining that STRmix was developed by a New Zealand-Australia collaborative and is sold in the United States by a company called Nichevision, and TrueAllele is owned and marketed by a company called Cybergenetics); *see also* Wexler, *supra* note 17, at 7 n.21 (noting that "STRmix is sold for profit around the world").

their algorithms, asserting that they are trade secrets.[34] At least one such program, Forensic Statistical Tool (FST), was developed by a government actor, which also asserted a private property interest in the algorithm until the program was shelved in 2017.[35] At the same time, a variety of less popular probabilistic genotyping programs are available for free and are open source.[36]

All of these algorithms are "computerized" because the programs' human designers or operators appear to determine and input most of the baseline assumptions, but the programs also learn from existing datasets of DNA markers and populations. Although the precise inputs of many of these programs are not public, many probabilistic genotyping algorithms appear to include a bevy of assumptions: the number of contributors to a particular DNA sample; the race or ethnicity of the comparison population; the quantity of DNA from each contributor; the degree to which the DNA is degraded; the probability that certain alleles may not be picked up; and more.[37]

---

34. *See* Wexler, *supra* note 17, at 1; *see also* Imwinkelried, *supra* note 17, at 111 (describing second wave of cases regarding "trade secrets" privilege in criminal cases as focused on "probabilistic genotyping programs, notably TrueAllele"); Roth, *supra* note 19, at 2028 ("Creators of proprietary algorithms typically argue that the source code is a trade secret."); Stephanie M. Lee*, People Are Going to Prison Thanks to DNA Software—But How It Works Is Secret*, BUZZFEED (March 18, 2016, 8:46 PM), https://www.buzzfeed.com/stephaniemlee/dna-software-code?utm_term=.ar2No4palG#.ljeLOzEm4j [https://perma.cc/GV3Y-3UMA]; STRmix, *Access to STRmix Software by Defence Legal Teams* (April 2016), https://strmix.esr.cri.nz/assets/Uploads/Defence-Access-to-STRmix-April-2016.pdf [https://perma.cc/ZL5A-2ML5].

35. *See* Robbins, *supra* note 23; Kirchner, *supra* note 1. New York's Office of the Chief Medical Examiner developed FST. Kirchner, *supra* note 1. Prosecutors used FST in New York courts from July 2011 through 2017, and numerous courts recognized a proprietary interest in the government's software. Robbins, *supra* note 23; *see, e.g.*, New York v. Carter, No. 2573/14, slip op. at 7 (N.Y. Sup. Ct. Jan. 12, 2016) (denying the defendant's discovery motion for FST source code because "the source code is proprietary software copyrighted by the city of New York"); *see also* Wexler, *supra* note 17, at 18 n.73 (string cite of New York state cases refusing to disclose FST code because of OCME's ownership interest in the program). A federal court, on the other hand, has questioned "why a public laboratory would need a protective order in this context." Wexler, *supra* note 17, at 47 (citing orders in United States v. Johnson, No. 1:15-cr-00565 (S.D.N.Y. June 7, 2016)).

36. *See* Kirchner, *supra* note 16 (identifying at least four such programs, including LRmix, EuroForMix, Lab Retriever, and LikeLTD—the last of which benefited from public scrutiny that exposed a significant bug).

37. Roth, *supra* note 19, at 1994–97, 1996 n.119; Thompson, *supra* note 29, at 18.

II. Computerized Algorithms Are Human Constructs, Subject to Mistake

Like most other sources of evidence, computerized algorithms are neither inherently good nor inherently bad. As this Section explains, they are merely tools designed, built, and operated by humans to mechanize the analysis of data. And they do so with varying degrees of accuracy. This is not surprising—but, as Section III lays out, it becomes a problem of constitutional magnitude when the algorithms are kept hidden from the public, and their accuracy cannot be assessed or sufficiently questioned.

A. Algorithms Are Not Infallible Oracles

Notwithstanding the complexity of computerized algorithms, when their results are introduced in court, legal experts and prosecutors generally suggest that they are infallible and that their results are foolproof, "overstat[ing] the probative value of their evidence, going far beyond what the relevant science can justify."[38] And juries, frequently deprived of the source code or any countervailing testimony that could expose the algorithm's potential pitfalls, generally do not question the prosecution's results.

This same issue arises when juries consider older and more traditional forensic "science," like bitemark, fingerprint, hair, fiber, and tire tread analysis. According to the Innocence Project, "Misapplication of forensic science is the second most common contributing factor to wrongful convictions, found in nearly half (45%) of DNA exoneration cases."[39] Even with regard to relatively established science like fingerprint analysis, "longstanding claims

38. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., FORENSIC SCIENCE IN CRIMINAL COURTS: ENSURING SCIENTIFIC VALIDITY OF FEATURE-COMPARISON METHODS 29 (2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf [https://perma.cc/GL9N-2TLP] [hereinafter PCAST]; Murphy, *supra* note 17, at 765 (arguing that even defense attorneys may be startstruck by complex forensic evidence).

39. *Misapplication of Forensic Science*, INNOCENCE PROJECT, https://www.innocenceproject.org/causes/misapplication-forensic-science/ [https://perma.cc/GL69-RNRL] (last visited June 17, 2018).

about [its] infallibility" are likely to instill more juror trust in their results than the science warrants.[40] And while traditional DNA analysis, which is limited to searching for matches for single source or "simple mixture" samples (defined as mixtures with no more than two contributors), is a "foundationally valid and reliable method" and is highly trusted by juries, it too "is not infallible in practice."[41]

Subjective interpretation of DNA mixtures with more than two contributors is far less established. In Texas, for example, recalculation of statistics after forensic laboratories changed how they dealt with a common source of missing data in a DNA sample resulted in drastic and material changes in statistics—including "from 1 in 1.4 billion to 1 in 36 in one case, and from 1 in 4,000 to inconclusive in another."[42] According to the President's Council of Advisors on Science and Technology, probabilistic genotyping algorithms offer a more promising approach—but one that has yet to be sufficiently tested by independent groups or evaluated on samples as complex as those it is used for in the real world.[43]

Jurors therefore have a serious propensity to trust the results of probabilistic genotyping more than they should based on the largely untested science, which combines DNA evidence—"powerful new evidence unlike anything known before"[44]—with mechanized data analysis that offers an additional sheen of objectivity, neutrality, and complexity.[45] Moreover, the outputs of these programs can appear

40. PCAST, *supra* note 38, at 9.

41. *Id.* at 73; *see also* Patt Morrison, *Barry Scheck on the O.J. Trial, DNA Evidence and the Innocence Project*, L.A. TIMES (June 17, 2014, 5:24 PM), http://www.latimes.com/opinion/op-ed/la-oe-0618-morrison-scheck-oj-simpson-20140618-column.html [https://perma.cc/PM9N-3GU4].

42. PCAST, *supra* note 38, at 77.

43. *Id.* at 80–82.

44. Dist. Attorney's Office for the Third Judicial Dist. v. Osborne, 557 U.S. 52, 62 (2009); PCAST, *supra* note 38, at 45 (describing finding that mock jurors heavily underestimated the error rates of qualified, experienced forensic scientists); *see also* Murphy, *supra* note 17, at 753 ("It is far easier to imagine that once the government puts the evidence forward, it will be accepted without question as true."); Matthew Shaer, *The False Promise of DNA Testing*, ATLANTIC (June 2016), http://theatln.tc/2xs7XUL [https://perma.cc/6G6B-57TU] (describing the finding that sexual assault cases involving DNA evidence in Australia "were twice as likely to reach trial and 33 times as likely to result in a guilty verdict; homicide cases were 14 times as likely to reach trial and 23 times as likely to end in a guilty verdict").

45. Thompson, *supra* note 29, at 18.

both simple and astronomical with likelihood ratios reaching into the billions and quintillions.[46]

It is, therefore, almost inevitable that "[t]he potential prejudicial impact" of probabilistic genotyping results is "unusually high."[47] Indeed, knowing the power of such evidence, most defendants plead guilty when confronted with "unfavorable [probabilistic genotyping algorithm] results."[48] And algorithms used for evidence can also determine the outcome of a case even if it goes to trial, as the algorithms arguably did in Mr. Herskovic's and Mr. Johnson's cases. This power, especially when compounded with the many potential sources for error discussed below, highlights the constitutional importance of public access to and adversarial testing of such algorithms.

B. Computerized Algorithms Are Designed, Built, and Operated By People

Though computerized algorithms are often presented (and interpreted) as objective, all-knowing oracles, their design combines human assumptions with machine learning—and humans impact both. Algorithmic programs are composites of their underlying model; training data; source code; input parameters and data specific to each case; and the various results from which the final, reported one was chosen. Algorithms are designed, built, and operated by humans, and humans are the ones who translate the outputs into results that factfinders can understand. As a result, algorithms are vulnerable to human bias and mistake at each stage.

---

46. *See* ACLU Amicus Brief, *supra* note 2, at 18 n.4. In Mr. Johnson's case, for example, the ratios introduced into evidence included 34,000; 1 million; 740 million; and 211 quintillion. *Id.* Although these numbers are striking, they do not necessarily translate to accuracy or validity. *See* Thompson, *supra* note 29, at 20. Their size reflects TrueAllele's decision to "consider[] more information when making calculations" than traditional DNA testing does. ACLU Amicus Brief, *supra* note 2, at 18 n.4. While traditional tests "generally consider only whether an allele is present or absent in a sample[,] TrueAllele also considers the height of the underlying peak and the presence or absence of technical artifacts that often accompany actual alleles." Thompson, *supra* note 29, at 19. But its ability to reach higher numbers does not guarantee accuracy any more than a "gasoline gauge that [can tell] you there are 100 gallons in your tank," rather than only 10, is guaranteed to be correct as a result. *Id.* at 20.

47. PCAST, *supra* note 38, at 45.

48. Kirchner, *supra* note 1.

1. Design

At the outset, humans determine the foundational assumptions that undergird algorithms. For probabilistic genotyping programs, these assumptions include whether something identified in a DNA sample constitutes stutter (i.e., random noise that can be ignored) or an actual allele (i.e., a characteristic that the suspect must match). The line between the two can determine whether or not a defendant is considered a statistical match to the sample—and that line is drawn by a human.[49] Other assumptions include "the probability of unusual events—such as small amounts of contamination during testing," which also "directly affect interpretation."[50]

On the machine learning side, humans also impact the algorithm's design by, for example, choosing the training data—another decision that can have significant effects on the algorithm's output and in ways that differentially affect suspects of different races, ethnicities, or ancestral backgrounds.[51]

Recognizing the vast range of assumptions built into a probabilistic genotyping algorithm by design—and the defense's inability to challenge any of them—one court refused to enter FST's results into evidence. The court explained that a defense expert cannot, "for example, obtain a likelihood ratio based on a hypothesis that there were a larger or smaller number of contributors to the mixture than [the algorithm's creator] supposes"; "that contributors are related"; or "how much an individual of a mixed race might differ from a person who is not."[52] But these assumptions are only the start

49. *See* Roberts v. United States, 916 A.2d 922, 933–34 (D.C. 2007); *see also* Roth, *supra* note 19, at 1994–96.

50. Roth, *supra* note 19, at 1996.

51. *See, e.g.*, New York v. Collins, 15 N.Y.S.3d 564, 580–81 (N.Y. Sup. Ct. 2015) (crediting objection of two defense experts to FST because (1) it was trained on data with only "Asian, European, African, and Latino" categories, which is inadequate for identifying other races or ethnicities, and (2) the training data appeared to include only three Asian individuals, which was insufficient to determine false positive rates for people with Asian ancestry); Roth, *supra* note 19, at 1997 (discussing the importance and difficulty of identifying "the appropriate reference population for generating estimates of the rarity of genetic markers"); *see also* Kirchner, *supra* note 4 (noting that Mr. Herskovic, "a Hasidic Jew, . . . is now appealing his conviction . . . because FST was never tested on a population as insulated as the Hasidic Jews of Williamsburg, who very likely share many of the same ancestors, and therefore much of the same DNA").

52. *Collins*, 15 N.Y.S.3d at 578.

of human involvement in—and the creator and prosecution's control of—probabilistic genotyping algorithms.

2. Building Algorithms and Translating Output

Once the design is set, people operationalize the algorithm through source code, which is built from numbers, letters, symbols, and punctuation marks. Source code refers to the human-written instructions that tell a computer how to execute the algorithm.[53] An error or "bug" as simple as a misplaced punctuation mark can materially alter the source code and result in a program that does not reflect the intended algorithm.[54] The more complicated the code and the more difficult the problem the algorithm is attempting to solve, the higher the likelihood of bugs.[55] The source code of probabilistic genotyping algorithms is likely to be affected by both issues: their selling point is the difficulty of the problem they attack, and their source code is complicated, with at least one program's source running for more than 170,000 lines.[56] To use the algorithm once it is designed and built, people must set the input parameters—for example, the assumed number of contributors to a DNA sample—and those choices, too, can make the difference between a conclusive and an inconclusive match.[57]

Finally, at the output stage, people interpret the algorithm's results and translate them into terms that others can understand. For example, they decide what magnitude of likelihood ratio qualifies as

53. *See* Imwinkelried, *supra* note 17, at 102–03.

54. *See* Chessman, *supra* note 19, at 187; Roth, *supra* note 19, at 1994 (quoting Sergey Bratus et al., *Software on the Witness Stand: What Should It Take for Us to Trust It?*, *in* TRUST AND TRUSTWORTHY COMPUTING 396, 397 (Alessandro Acquisti et al. eds., 2010)).

55. Roth, *supra* note 19, at 2024.

56. *Id.* at 2035 (noting that TrueAllele has more than 170,000 lines of source code).

57. *See, e.g.*, Cybergenetics, *TrueAllele Overview Video*, YOUTUBE (May 1, 2013), https://www.youtube.com/watch?v=OU29b5sW88Y [https://perma.cc/8LEL-P485] (showing that TrueAllele allows analysts to set several variables, including the number of contributors to a DNA sample); Letter from Mark W. Perlin, Chief Sci. and Exec. Officer, Cybergenetics, to Jerry D. Varnell, U.S. Dep't of Justice, Procurement Section, at 3 (Apr. 1, 2015), https://www.cybgen.com/information/newsroom/2015/may/Letter_to_FBI.pdf [https://perma.cc/94A4-F5WY] (acknowledging that some probabilistic genotyping algorithms "give different answers based on how an analyst sets their input parameters").

conclusive.[58] And, crucially, people—prosecutors, prosecution experts, and crime lab staff; not the algorithm itself, a computer, or other machine—decide which precise result to disclose to the jury.[59]

C. People Make Mistakes—And So Do Their Computerized Algorithms

1. Potential for Error

At each of these stages, people will almost certainly make mistakes, impose their cognitive biases, and be tempted by perverse incentives. At the design stage, for example, cognitive biases can materially affect which variables people choose to include in an algorithm.[60] Such biases can also affect how they interpret the results—including whether a DNA sample results in a match.[61] And, at the coding stage, even highly experienced programmers have been found to make a mistake "in almost 1% of all expressions contained in [their] source code."[62] Mistakes occur even with tasks as simple as inputting "yes" or "no" to match the program's parameters to a particular case.[63]

And the fact that the people at each stage are different, with different areas of expertise, only compounds the possibility of

58. *See* ACLU Amicus Brief, *supra* note 2, at 14 (noting that, in Mr. Johnson's case, where the prosecution relied upon TrueAllele results, the two different experts who used the program disagreed on what likelihood ratio could be considered conclusive: the company's threshold of exclusion was 1,000, and the state crime lab's threshold was ten times that).

59. *See* Thompson, *supra* note 29, at 20 (describing a case in Northern Ireland in which TrueAllele generated four different likelihood ratios regarding the same defendant—389 million, 1.9 billion, 6.03 billion, and 17.8 billion; the company chose to report the 6.03 billion statistic).

60. *See* discussion of human decisions in design *supra* Section II.B.i.

61. *See* Itiel E. Dror & Greg Hampikian, *Subjectivity and Bias in Forensic DNA Mixture Interpretation*, 51 SCI. & JUST. 204, 205 (2011) (finding that more DNA examiners determined that an individual matched a DNA mixture when they knew that he was a criminal defendant in a gang rape case than when they did not).

62. Chessman, *supra* note 19, at 186.

63. *See* Wexler, *supra* note 16, at 24–25 (describing how the evaluator tasked with calculating an incarcerated individual's risk score mistakenly checked "yes" in response to a question when he should have checked "no"—a mistake that had previously inflated a risk score by a full category); *see also* Murphy, *supra* note 17, at 775 (detailing potential mistakes in traditional DNA analysis—"a manufacturer may contaminate a kit, an analyst may fail to run positive or negative controls, or a technican may erroneously input data into a database"—all of which would also affect the results of a probabilistic genotyping algorithm).

errors.[64] When it comes to an issue as complex as translating probabilistic genotyping concepts into thousands of lines of code—that is, combining the fields of forensic science, genetics, and probabilistic programming—people may simply have conceptual blind spots.[65] While expert in one area, like programming, the purveyors of probabilistic genotyping algorithms may make errors due to an incomplete grasp of another area, like genetics.[66]

Moreover, financial incentives may pervert the goals of the companies that build these algorithms.[67] In the field of probabilistic genotyping, these dynamics are acute because the prosecution, backed by the resources of the state, is the most likely customer—and the prosecution is likely to be most satisfied with an algorithm that delivers a match.[68] As a result, the private purveyors of programs like TrueAllele and STRmix may be incentivized to find a match, rather than the truth, to attract and retain business.[69] Market forces are likely to bias results in this direction, notwithstanding the companies' best intentions. Compounding that problem, private companies are

64. *See* Imwinkelried, *supra* note 17, at 98, 103–04 (identifying various team members involved in drafting the source code and noting that a witness who testifies to present forensic algorithmic DNA evidence is not likely to "be a DNA analyst who personally analyzed" the DNA sample).

65. Chessman, *supra* note 19, at 188 ("Programmers might also be dealing with highly technical subject areas—such as physics, chemistry, and biology—that do not overlap with their training.").

66. *Id.*; *see also* Kirchner, *supra* note 1 (quoting scientist at OCME as stating, "We don't know what's going on in that black box, and that is a legitimate question").

67. *See, e.g.*, CYBERGENETICS, TRUEALLELE CASEWORK TECHNOLOGY 4 (2015) (emphasis added), https://www.cybgen.com/products/casework/forensic_e-brochure.pdf [https://perma.cc/823Q-JB5F] (identifying the algorithm's goal as delivering "a match statistic *strong enough for court*"); *see also* Murphy, *supra* note 17, at 749 (noting differences in incentives for geneticists, who typically look for "areas of the genetic strand that regulate human attributes, diseases, or characteristics" and "the forensic scientist[, who] most commonly studies those places at which genetic material has no demonstrable function or purpose . . . . To suggest that the geneticist's broader interest in genomics validates DNA typing for forensic purposes is like suggesting that the widespread market for electricity somehow ensures the proper functioning of an electric chair.").

68. *See* Murphy, *supra* note 17, at 749 ("Any company that develops a technology for forensic purposes inevitably allies closely with its primary customer, the government."); Wexler, *supra* note 16, at 71 ("An agency that implements these tools and methods has already deemed them valid and reliable according to whatever procurement standards apply, and will have weak incentives to identify information that could prove otherwise.").

69. *See* Melendez-Diaz v. Massachusetts, 557 U.S. 305, 318 (2009) ("A forensic analyst responding to a request from a law enforcement official may feel pressure—or have an incentive—to alter the evidence in a manner favorable to the prosecution.").

also more likely to push for secrecy, which keeps all of these errors hidden from the public.[70]

For these reasons, algorithms are fallible. Although this may surprise laypeople or lawyers, computer scientists have long been acutely aware of this fact. They caution that "the evidence produced by computer programs is no more inherently reliable or truthful than the evidence produced by human witnesses."[71]

2. Documented Error

Experience has borne out this potential for fallibility. For example, in just the last few years, researchers documented a coding error in STRmix that produced incorrect results in sixty criminal cases in Australia, altering likelihood ratios by a factor of ten and forcing prosecutors to replace twenty-four expert statements in criminal cases.[72] In New York, after a trial court ordered FST to release its source code, an expert witness for the defense discovered that "the program dropped valuable data from its calculations, in ways that users wouldn't necessarily be aware of, but that could unpredictably affect the likelihood assigned to the defendant's DNA being in the mixture."[73] In response, the prosecution withdrew the DNA evidence against the defendant.[74] Earlier this year, the New York State Commission on Forensic Science "shelved" two previously-approved probabilistic genotyping algorithms for similar reasons,[75] including one court that declined to admit related evidence because of expert

70. *See* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 101, 106 (2017), http://www.nyulawreview.org/sites/default/files/Joh-FINAL_0.pdf [https://perma.cc/VSN8-7HTP] (noting this phenomenon in the context of policing); *id.* at 125–26 (citing Cybergenetics' secrecy regarding TrueAllele as an example of private companies pushing for secrecy); Murphy, *supra* note 17, at 750; Wexler, *supra* note 16, at 21–23 (discussing same).

71. Chessman, *supra* note 19, at 185.

72. David Murray, *Queensland Authorities Confirm 'Miscode' Affects DNA Evidence in Criminal Cases*, COURIER-MAIL (Mar. 20, 2015, 8:00 AM), http://www.couriermail.com.au/news/queensland/queensland-authorities-confirm-miscode-affects-dna-evidence-in-criminal-cases/news-story/833c580d3f1c59039efd1a2ef55af92b [https://perma.cc/G7G6-ZLBP].

73. Kirchner, *supra* note 1.

74. *Id.*

75. *Id.*

testimony that challenged the assumptions underlying the algorithm and validation studies of it.[76]

Indeed, notwithstanding the fact that each probabilistic genotyping algorithm claims to provide accurate results based on objective scientific principles, competing programs frequently reach meaningfully different results concerning the same forensic sample. For example, in one New York case, after prosecutors shopped around for the program that would generate the strongest match, two programs, TrueAllele and STRmix, reached different results.[77] The judge refused to admit evidence from STRmix because the program had not been internally validated, and the defendant was acquitted.[78] In a Pennsylvania case, TrueAllele calculated a match statistic of 189 billion, compared to a competitor's estimate of 13,000—a more than 14-million–fold difference.[79] In Mr. Johnson's case, two experts—both employed by the prosecution—used TrueAllele to match the same DNA evidence to the same defendant, and yet calculated results that differed by a factor of more than ten.[80] In a Northern Ireland case, TrueAllele analyzed a single forensic sample four times and generated four different likelihood ratios, the highest of which was more than forty-five times the lowest, notwithstanding the fact that the same lab was using the same program to analyze the same data each time.[81]

These examples highlight not only the possibility of error, but also its significance in altering results. A wrong or even murky result is a serious problem, particularly given the level of trust that juries place in computerized alorithms.[82] And it is a problem both for individuals accused of crimes, whose lives are put into jeopardy by faulty coding, and for prosecutors, whose cases can be upended by their introduction of unreliable evidence.[83] Therefore, access to the

76. People v. Collins, 15 N.Y.S.3d 564, 578–82 (N.Y. Sup. Ct. 2015).
77. *See* New York v. Hillary, No. 2015-15 (N.Y. Cty. Ct. Aug. 26, 2016).
78. *Id.*
79. Pennsylvania v. Foley, 38 A.3d 882, 887, 890 (Pa. Super. Ct. 2012).
80. *See* ACLU Amicus Brief, *supra* note 2, at 18.
81. *See* Thompson, *supra* note 29, at 20.
82. *See supra* Section II.A.
83. Shawn Musgrave, *SJC to Decide Whether to Dismiss All Cases Connected to Former Drug Lab*

computerized algorithms—including their underlying model; training data; source code; input parameters and data specific to each case; and the various results from which the final, reported one was chosen—is necessary. This can be achieved through motions for the First Amendment right of access, as Section III discusses.

III. The Public's First Amendment Right of Access Attaches to Computerized Algorithms Used as Evidence in Criminal Trials

The Sixth and Fourteenth Amendments to the U.S. Constitution require that accused persons have access to the particular algorithm, datasets, and other parameters used for their trial, and such access may uncover issues specific to their particular case.[84] But other widespread problems—whether in the algorithm's design, its operationalization through source code, or the algorithm owner's approach to delivering results—may be best addressed by recognizing the public's right of access to the algorithms and enabling efficient auditing by independent experts.

The First Amendment was designed to "assure [the] unfettered interchange of ideas for the bringing about of political and social changes desired by the people."[85] As the architects of the Constitution explained, First Amendment protections are necessary not only for "the advancement of truth, science, morality, and arts in general" but also for the "diffusion of liberal sentiments on the administration of Government . . . whereby oppressive officers are

Chemist, BOS. GLOBE (Jan. 30, 2018), https://www.bostonglobe.com/metro/2018/01/30/sjc-decide-whether-dismiss-all-cases-connected-former-drug-lab-chemist/74FLWu9e12lNFA3rfkM9ZO/story.html [https://perma.cc/ZA9E-K34C] (explaining that district attorneys have dismissed approximately 8,000 cases affected by misconduct by a drug lab chemist in Massachusetts and may dismiss more); *see, e.g.*, Shaer, *supra* note 44 (describing man who was exonerated after retesting).

84. The Fourteenth Amendment right to due process and the Sixth Amendment right to a fair trial work in tandem to guarantee accused persons a fundamentally fair process. *See* Holmes v. South Carolina, 547 U.S. 319, 319 (2006). In addition, the Sixth Amendment protects the right of a defendant to confront "the witnesses against him." U.S. CONST. amend. VI. The Confrontation Clause's animating concern is "to ensure the reliability of the evidence . . . by subjecting it to rigorous testing." Maryland v. Craig, 497 U.S. 836, 845 (1990).

85. Roth v. United States, 354 U.S. 476, 484 (1957) (finding that the Continental Congress made "[t]his objective . . . explicit as early as 1774").

shamed or intimidated[] into more honourable and just modes of conducting affairs."[86]

In other words, public oversight and robust debate is foundational to democracy. Such oversight processes depend upon the government respecting the First Amendment "right to 'receive information and ideas'"[87] and not "limiting the stock of information from which members of the public may draw."[88]

The need for such oversight is perhaps strongest in the criminal justice system where the state wields its greatest power against individual liberty. As the Supreme Court of the United States has explained, "the criminal justice system exists in a larger context of a government ultimately of the people, who wish to be informed about happenings in the criminal justice system, and, if sufficiently informed about those happenings, might wish to make changes to the system."[89] For those reasons, "the right to attend criminal trials is implicit in the guarantees of the First Amendment."[90]

This right of access is broad: indeed, the Supreme Court has cautioned that the right "must be taken as a command of the broadest scope that explicit language, read in the context of a liberty-loving society, will allow." [91] And algorithms used to produce evidence introduced by the prosecution in a criminal trial fit within this broad scope—especially if defense counsel has succeeded in making the algorithms part of the record of the case in order to rebut the resulting evidence. As noted above, other scholarship has explored arguments available to defense counsel to make the source code part of the record.[92] The public's First Amendment right to access that

86. *Id.* (quoting 1 JOURNALS OF THE CONTINENTAL CONGRESS 108 (1774)).

87. Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 576 (1980) (quoting Kleindienst v. Mandel, 408 U.S. 753, 762 (1972)).

88. *Id.* (quoting First Nat'l Bank of Bos. v. Bellotti, 435 U.S. 765, 783 (1978)).

89. Gentile v. State Bar of Nev., 501 U.S. 1030, 1070 (1991).

90. *Richmond Newspapers*, 448 U.S. at 580.

91. *Id.*

92. *See, e.g.*, Chessman, *supra* note 19, at 219–21. In addition to constitutional arguments, scholars have suggested challenges to the secrecy based in evidentiary law. *See* Imwinkelried, *supra* note 17, at 121–24, 128–30; Wexler, *supra* note 16, at 14–18, 41–44 (challenging idea of a "criminal trade secret privilege").

information, described more fully below, should in turn bolster the defendant's arguments for making the algorithm part of the record.[93]

A. The Right of Access Attaches to Such Computerized Algorithms

Nearly forty years ago, the Supreme Court recognized that the First Amendment exists to enable democratic discourse; includes the right to "receive information and ideas"; and protects the right to access judicial proceedings and documents.[94] This right of access is premised on "the common understanding that 'a major purpose of [the First] Amendment was to protect the free discussion of governmental affairs'" and that self-government is most effective and productive when the "constitutionally protected 'discussion of governmental affairs' is an informed one."[95] In other words, the right of access is "necessary to the enjoyment of other First Amendment rights."[96]

The right of access is most clearly established for access to, and information about, criminal trials.[97] Indeed, the seminal case squarely recognizing a First Amendment right of access held that "a presumption of openness inheres in the very nature of a criminal trial under our system of justice."[98] As previously noted, the Supreme Court has explained that the people have the ultimate say in how the criminal justice system operates; they "might wish to make changes to the system,"[99] and the need for public oversight of government

93. Indeed, the Supreme Court has suggested that a defendant's Sixth Amendment right to a public trial may go even further than the First Amendment right in certain cases. *See* Presley v. Georgia, 558 U.S. 209, 213 (2010); Waller v. Georgia, 467 U.S. 39, 46 (1984) ("Nevertheless, there can be little doubt that the explicit Sixth Amendment right of the accused is no less protective of a public trial than the implicit First Amendment right of the press and public."). This suggests that each of the arguments made in this Section could equally be levied by a defendant in the context of a Sixth Amendment challenge.

94. *Richmond Newspapers*, 448 U.S. at 576 (quoting Kleindienst v. Mandel, 408 U.S. 753, 762 (1972)).

95. Globe Newspaper Co. v. Superior Court of Norfolk, 457 U.S. 596, 604–05 (1982) (quoting Mills v. Alabama, 384 U.S. 214, 218 (1966)).

96. *Id.* at 604.

97. *See Richmond Newspapers*, 448 U.S. at 572.

98. *Id.* at 573.

99. *Gentile*, 501 U.S. at 1070.

process is strongest in criminal trials, where the state wields its greatest power to affect individual liberty.[100]

The prevailing test for deciding when the right attaches is the "experience and logic test," which states that the right of public access attaches to any type of judicial process or record that (a) has historically been open to the public and (b) would benefit from public access and oversight.[101] Criminal trials easily meet the history prong of the test given this country's "unbroken, uncontradicted history" of access to criminal trials.[102] And they also meet the logic prong because, as the Supreme Court has explained, public access improves criminal justice by "enhanc[ing the] quality and safeguard[ing] the integrity," "heightening public respect for," and "permit[ting] the public to participate in and serve as a check upon the judicial process."[103]

1. Algorithms As Part of Record

For the right of access to criminal trials to have meaning and bear fruit, the presumption of access must apply broadly to all materials essential to the criminal proceeding—including algorithmic source code used as evidence in a criminal case. Appellate courts around the country have recognized that the right of access to criminal proceedings attaches to materials in the full record of a criminal case. This includes records—like motions, memorandum, affidavits, trancripts, and exhibits—from hearings before, during, and after the proceedings and access to the hearings themselves, including suppression hearings, pretrial release hearings, and closed hearings.[104] Thus, where the defense or prosecution has made an

100. The importance of public access to criminal trials is also embedded in the common law. *See, e.g.*, Lugosch v. Pyramid Co. of Onondaga, 435 F.3d 110, 119 (2d Cir. 2006). The Sixth Amendment, which guarantees a criminal defendant the right to a public trial, is embedded in the common law as well. *See, e.g.*, *In re* Oliver, 333 U.S. 257, 268–69 (1948); Waller, 467 U.S. at 46 ("[T]here can be little doubt that the explicit Sixth Amendment right of the accused is no less protective of a public trial than the implicit First Amendment right of the press and public.").

101. Press-Enter. Co. v. Superior Court of California, 478 U.S. 1, 8–9 (1986).

102. *Richmond Newspapers*, 448 U.S. at 572–73.

103. *Globe Newspaper*, 457 U.S. at 606.

104. *See, e.g.*, Doe v. Pub. Citizen, 749 F.3d 246, 267 (4th Cir. 2014) ("[T]he First Amendment right of access extends to materials submitted in conjunction with judicial proceedings that themselves would

algorithm's source code part of the record, the argument for the public's right to access that source code is clear.[105]

Indeed, one scholar, Rebecca Wexler, has found that "[e]arly historical sources suggest that the [trade secrets] privilege"—precisely the tool companies are now using to keep algorithms out of the record of criminal cases—"was unavailable in criminal proceedings" until the 1990s.[106] This suggests that existing caselaw that has allowed companies to keep their source code hidden on the basis of that privilege is blocking from view information that would historically have been public.[107]

And the "logic" case for access to such information is perhaps even clearer. Openness in the context of algorithms used to produce evidence of guilt has immense public value. This country has a long

---

trigger the right to access."); California First Amendment Coal. v. Woodford, 299 F.3d 868, 874 (9th Cir. 2002) (listing cases identifying "pretrial suppression hearings," "pretrial release proceedings and documents," "transcripts of closed hearings that occurred during the course of jury deliberations," and "plea agreements and related documents" as covered by the First Amendment right of access); *In re* New York Times Co., 828 F.2d 110, 114 (2d Cir. 1987) (right of access attaches to suppression motions and exhibits); *In re* Washington Post Co., 807 F.2d 383, 390 (4th Cir. 1986) (same for plea agreements); United States v. Peters, 754 F.2d 753, 763 (7th Cir. 1985) (same for trial exhibits); *In re* Globe Newspaper Co., 729 F.2d 47, 47 (1st Cir. 1984) (same for memorandum, affidavits and transcripts in criminal case).

105. Some courts have (erroneously) applied a narrower test to determine when the First Amendment right-of-access attaches, looking only to the nature of a particular document rather than the proceedings themselves. *See In re* Boston Herald, 321 F.3d 174, 182–84 (1st Cir. 2003) (reviewing this case law). Algorithmic source code used to produce evidence of guilt in a criminal case should fall within even this too-narrow reading, as the right of access has historically attached to materials essential to the government's case-in-chief and such access has improved the process of assessing that evidence. *See, e.g.*, Valley Broad. Co. v. U.S. Dist. Court, 798 F.2d 1289, 1292–93 (9th Cir. 1986) (transcripts of exhibits); United States v. Posner, 594 F. Supp. 930, 934–36 (S.D. Fla. 1984) (tax returns admitted into evidence); *In re* Application of WFMJ Broad. Co., 566 F. Supp. 1040, 1040 (N.D. Ohio 1983) (tapes played to jury in open court); United States v. Scott, 48 M.J. 663, 666, 667 (A. Ct. Crim. App. 1998) (materials entered into evidence at trial); *In re* Times-World Co., 488 S.E.2d 677, 684 (Va. 1997) (documents submitted into evidence).

106. Wexler, *supra* note 16, at 41–45 (identifying only two pre-1900 cases that considered whether trade secrets must be disclosed in criminal trials: *R v. Maha Rajah Nundocomar*, 20 Howell State Trials 923, 1057 (1775) and *R v. Webb*, 174 Eng. Rep. 140 (1834), both of which held that the secrets must be disclosed).

107. While the trade secrets at issue in *Maha Rajah Nundocomar* and *Webb* (for example, the ingredients of a pill), see Wexler, *supra* note 16, at 41, are not equivalent to algorithmic source code, the "experience" prong "is not meant . . . to be construed so narrowly" as to exclude from First Amendment coverage proceedings or documents that are of "relatively recent vintage." *In re* Boston Herald, 321 F.3d at 184. Rather, in such cases, courts look to analogous proceedings and documents of the same "type or kind." Rivera–Puig v. Garcia–Rosario, 983 F.2d 311, 323 (1st Cir. 1992). Here, the relevant category is material evidence based on purported trade secrets.

history of junk science being used as evidence in criminal cases under the guise of technological advance and of public access to and analysis of such evidence debunking it.[108] Indeed, courts—including the Supreme Court, state supreme courts, and federal appellate courts—look to work done by the *public*, rather than either party or its experts in a criminal case, to determine what rights and standards attach to evidence based on specific technologies.[109] At least one court has already recognized that, when it comes to proprietary algorithms specifically, "[i]t is incumbent upon the criminal justice system to recognize that in the coming months and years, additional research data will become available . . . . The justice system must keep up with the research and continuously assess the use of these tools."[110] Moreover, the system should enable the access necessary for that research.

Public scrutiny has had substantial benefits outside of the courtroom as well, leading to important improvements in investigative fields. For example, after a *New Yorker* article exposed a flawed case based on fire-science evidence, Texas not only "reconsider[ed] old cases that had been improperly handled by the original investigators" but also "reinvented itself as a leader in arson science and investigation" by "revamp[ing] the state's training and investigative standards."[111]

All of this is true of DNA evidence as well. In the DNA field, "[b]oth the initial recognition of serious problems and the subsequent development of reliable procedures were aided by the existence of a

108. *See, e.g.*, Murphy, *supra* note 17, at 724 (describing the "shocking degree to which the criminal justice system has historically failed to prevent the government from deploying spurious sciences and faulty or fraudulent evidence," including "evidentiary stalwarts like handwriting, voice exemplars, hair and fiber, bite and tool marks, and even fingerprints"); Shaer, *supra* note 44 (same).

109. *See* Melendez-Diaz v. Massachusetts, 557 U.S. 305, 319–321 (2009); Han Tak Lee v. Houtzdale SCI, 798 F.3d 159, 166–67 (3d Cir. 2015) (discussing changes in "fire science"); Michigan v. Davis, 72 N.W.2d 269, 282 (Mich. 1955) ("The testimony of Dr. Snyder shows that it is of the greatest value and is quite generally used with very good results. It seems, however, that it has not as yet reached the dignity of positive evidence."); New York v. Leone, 255 N.E.2d 696, 698 (N.Y. 1969) (relying on commentary of outside experts to hold that evidence derived from polygraph tests was not fit for admission).

110. Wisconsin v. Loomis, 881 N.W.2d 749, 753 (Wis. 2016).

111. Jeremy Stahl, *The Trials of Ed Graf*, SLATE (Aug. 15, 2015, 9:02 PM), http://slate.me/2wdpTUA [https://perma.cc/5MYK-9R53]; *see also* David Grann, *Trial By Fire*, NEW YORKER (Sept. 7, 2009), https://www.newyorker.com/magazine/2009/09/07/trial-by-fire [https://perma.cc/U8FX-R977].

robust community of molecular biologists" and by "judges who recognized that this powerful forensic method should only be admitted as courtroom evidence once its reliability was properly established."[112] This is also true of algorithmic evidence. Indeed, public review of the source code at issue here has already proven its worth. In a 2008 case, public review of breathalyzer source code led the New Jersey Supreme Court to require modifications to prevent misleadingly high readings.[113]

In 2017, *United States v. Kevin Johnson* became the first case to make the benefit of public access to probabilistic genotyping algorithms specifically clear. The judge in that case ordered the prosecution to disclose the source code of a probabilistic genotyping algorithm to the defense—after FST calculated that DNA scraped from two guns found in his ex-girlfriend's apartment were 156 times and 66 million times more likely, respectively, to contain Mr. Johnson's DNA than that of a random individual.[114] Mr. Johnson pled guilty to illegal gun possession and was sentenced to 28 months in prison.[115]

Although the judge ordered that the prosecution disclose the source code to the defense, she also issued a protective order that kept the source code, as well as key portions of the defense's expert report challenging the validity of the algorithm, secret from the public.[116] As one of Mr. Johnson's defense attorneys explained, keeping that information secret was against the public's interest because the expert's critique of FST "affects every result that has ever been produced by that software."[117] After ProPublica and Yale's Media Freedom and Information Access Clinic intervened to seek

112. PCAST, *supra* note 38, at 26; *see also* Murphy, *supra* note 17, at 754 (detailing "scandals [that] have revealed systemic problems in a number of 'flagship' DNA laboratories and horrific tales of false-positive DNA matches").

113. New Jersey v. Chun, 943 A.2d 114, 120–21 (N.J. 2008).

114. Lauren Kirchner, *Federal Judge Unseals New York Crime Lab's Software for Analyzing DNA Evidence*, PROPUBLICA (Oct. 20, 2017), https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence [https://perma.cc/4WNV-BLPX].

115. Kirchner, *supra* note 4.

116. *Id.*

117. *Id.*

public access to the code and defense expert's affidavits,[118] the state did not oppose the motion, and the court lifted the protective order.[119] The expert reports are now publicly available,[120] and FST's source code is on GitHub.[121]

As the state recognized, the secrecy surrounding FST had "exacerbated the substantial misunderstanding of fundamental aspects of the FST source code."[122] In other words, the secrecy hurts the criminal justice system on all sides, impeding the process not only for the defense but for the prosecution as well. The public's ability to scrutinize FST is likely to inure to its benefit, but defense counsel and lawyers focused on public access have more work to do to ensure that other courts follow this example—particularly because FST has now been phased out in favor of STRmix and other proprietary algorithms continue to gain customers.

2. Algorithms Not in the Record

The argument for the public's right to access probabilistic genotyping algorithms' source code, training data, input parameters, and other auditing data is more complicated when that information is not explicitly part of the record—for example, in the many cases where defense counsel has sought and been denied access to source code.[123] But because, as discussed in Section II.A above, the algorithm is so central to the functioning of the criminal trial, advocates nevertheless have a colorable argument for public access in such cases.

As the Ninth Circuit recognized in holding that the public has a right to witness a lethal injection from start to finish, meaningful

118. Motion to Lift the Protective Order and Unseal Judicial Records, Exhibit C: Memorandum in Support of Application by ProPublica for Leave to Intervene, United States v. Johnson, No. 1:15-cr-00565-VEC (S.D.N.Y. Aug. 29, 2017).

119. Kirchner, *supra* note 114.

120. The affidavits are unsealed on the case docket. Motion to Lift the Protective Order and Unseal Judicial Records, *supra* note 116, nos. 153-1, 153-2.

121. ProPublica, *New York City's Forensic Statistical Tool*, https://github.com/propublica/nyc-dna-software [https://perma.cc/M93E-GUBD] (last visited Oct. 19, 2017).

122. Kirchner, *supra* note 4.

123. *See supra* note 17.

access to a proceeding means access to its nuts and bolts. In the Ninth Circuit case, that meant the public has a right to view "executions from the moment the condemned is escorted into the execution chamber," including the "initial procedures" when "the condemned . . . is forcibly restrained and fitted with the apparatus of death."[124] The court explained that, for the right of access to accomplish its many goals—ensuring that government processes are fair and humane, heightening public respect for the judicial process, and offering the public a sense of catharsis—"citizens must have reliable information about the 'initial procedures,' which are invasive, possibly painful and may give rise to serious complications."[125] The same must be true for the secret algorithms that produce the prosecution's material evidence in a criminal trial—which, as discussed above, also have the potential for serious complications and inaccuracies. Just as, without access to the initial procedures of an execution, "the public will be forced to rely on the same prison officials who are responsible for administering the execution to disclose and provide information about any difficulties with the procedure," without access to the algorithms that create material evidence, the public will be forced to rely on the same government officials responsible for introducing the evidence and convincing the judge and jurors that they should trust it.[126] But, much like prison officials, these government officials "do not have the same incentives to describe fully the potential shortcomings of" their evidence.[127] Thus, in criminal trials where material evidence is produced by secret algorithms, this principle about access to the nuts-and-bolts of the process must mean access to information about the algorithm's accuracy and reliability.

Indeed, courts have recognized that access to pretrial records and proceedings is "as important as [access to] the trial itself" because those proceedings are, in effect, the "only trial," given that often

124. California First Amendment Coal. v. Woodford, 299 F.3d 868, 877 (9th Cir. 2002).
125. *Id.* at 877.
126. *Id.* at 883.
127. *Id.* at 884.

"defendants thereafter plead[] guilty pursuant to a plea bargain."[128] As noted in Section II.A above, the same is true of algorithms that calculate DNA likelihood ratios—once their results are presented, defendants often plead guilty and no further criminal process occurs.[129] Access to the algorithmic code is necessary to know if the program—and the criminal justice process—works as claimed. The government cannot artificially cabin the record of a proceeding to deny public access to all but the ultimate result.

Moreover, allowing the public, including academics and other experts, to examine DNA typing evidence would markedly improve the reliability and fairness of such evidence in criminal trials. As one scholar, Erin Murphy, has explained, numerous factors that plague the defense—including "structural asymmetry[,] . . . scarcity of resources, weak discovery practices, and high rate of plea bargaining"—make the "adversarial process an inadequate safeguard of the integrity of forensic science."[130] But experts reviewing publicly disclosed information about algorithms, including the source code, should be free of these obstacles and should have the time, resources, and expertise to effectively and efficiently audit the algorithmic programs. Moreover, allowing the public to view the information would avoid the potential "devastating effect" of protective orders that prevent expert findings in one case from spreading to others, where they would be equally relevant and useful.[131] And independent review of documents across cases may catch errors or mistakes that would not be identifiable in one case alone.[132]

This is particularly true of technologies that, like many probabilistic genotyping algorithms, have been minimally tested in the field. Most existing validation studies of probabilistic genotyping have been "conducted under idealized conditions unrepresentative of

128. Georgia v. Waller, 467 U.S. 39, 46–47 (1984) (recognizing the importance of public access to pretrial aspects of a criminal proceeding in the Sixth Amendment context).

129. *See supra* text accompanying note 44.

130. *See* Murphy, *supra* note 17, at 757.

131. Wexler, *supra* note 16, at 57–58.

132. Murphy, *supra* note 17, at 773.

the challenges of real casework."[133] Moreover, "most of the studies evaluating software packages have been undertaken by the software developers themselves."[134] Public access to algorithmic evidence would improve the role such evidence plays in criminal trials—including by preventing the jury from giving it undue weight, where necessary—and increase the public's confidence in the justice system more generally.

B. Private Intellectual Property Claims Cannot Defeat Public Access

Because the public's First Amendment right of access is a qualified one, the issue does not end with whether or not the right *attaches* to algorithmic source code. That inquiry establishes a presumption of openness to the code, and it may be overcome—but "only by an overriding interest," which must be "based on findings" both "that closure is essential to preserve higher values" and that the closure is "narrowly tailored to serve that interest."[135]

In the words of the Supreme Court, the "circumstances" in which "the right to an open trial may give way . . . to other rights or interests . . . will be rare."[136] And the case of algorithmic source code rarely, if ever, presents such circumstances. First, the government's

133. Roth, *supra* note 19, at 2033; *see also* PCAST, *supra* note 38, at 80–81 (noting that although TrueAllele "appear[s] to be reliable for three-person mixtures in which the minor contributor constitutes at least 20 percent of the intact DNA in the mixture and in which the DNA amount exceeds the minimum level required for the method[,] . . . there is relatively little published evidence" for "more complex mixtures"—precisely the sort of mixtures for which it is used in actual cases).

134. PCAST, *supra* note 38, at 80.

135. Press-Enter. Co. v. Superior Court of California (*Press-Enter. II*), 478 U.S. 1, 9 (1986) (quoting Press-Enter. Co. v. Superior Court of California (*Press-Enter. I*), 464 U.S. 501, 510 (1984)); Globe Newspaper Co. v. Superior Court of Norfolk, 457 U.S. 596, 606–07 (1982); N.Y. Civil Liberties Union v. N.Y.C. Transit Auth., 684 F.3d 286, 296 (2d Cir. 2012); *see also* Waller v. Georgia, 467 U.S. 39, 48 (1984) (applying *Press-Enter. II* to the Sixth Amendment context and holding that "the party seeking to close the hearing must advance an overriding interest that is likely to be prejudiced, the closure must be no broader than necessary to protect that interest, the trial court must consider reasonable alternatives to closing the proceeding and it must make findings adequate to support the closure").

136. *Waller*, 467 U.S. at 45 (identifying sufficiently weighty rights and interests as "the defendant's right to a fair trial or the government's interest in inhibiting disclosure of sensitive information"). Here, the defendant's right to a fair trial dovetails—rather than conflicts—with the public's right of access to algorithmic source code, and the "sensitive information" the Supreme Court was contemplating in *Waller* belonged to the government, not a private party. *Id.*

only interest appears to be derivative of a private company's intellectual property interest in purported trade secrets. Companies are concerned that such exposure could lead to copycat competitors and argue that the concern itself might chill innovation. But this private interest, on its own, will likely fail strict scrutiny.[137] In fact, because the private "makers are under a scientific obligation to release this information for peer review," the validity of the interest is questionable.[138] As one commentator, William Thompson, put it, "If scientific evidence is not yet ready for both scientific scrutiny and public re-evaluation by others, it is not yet ready for court."[139]

Indeed, recognizing this private property interest as a sufficiently weighty government interest to defeat the public's right of access could do serious damage to more compelling government interests, including the defendant's right to a fair trial.[140] Similarly, it would "offend[] procedural justice by signaling that the government values trade secrets holders as a group more than those directly affected by criminal justice outcomes."[141]

Even if a court found this interest sufficiently compelling, it would additionally have to find that the government's request for secrecy was narrowly tailored to that interest to overcome the presumption of openness. A blanket ban on disclosure that extends not only to the algorithmic source code but also to material pieces of defense experts' reports challenging the validity of the algorithm simply cannot meet that standard.[142] Such a complete denial of access to a

137. *See* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 759 (1985); DVD Copy Control Ass'n v. Bunner, 75 P.3d 1, 15 (Cal. 2003) (citing Bartnicki v. Vopper, 532 U.S. 514, 533 (2001)) (explaining that the U.S. Supreme Court has "recognized that the First Amendment interests served by the disclosure of purely private information like trade secrets are not as significant as the interests served by the disclosure of information concerning a matter of public importance"); *see also* California First Amendment Coal. v. Woodford, 299 F.3d 868, 883 (9th Cir. 2002) (explaining that narrow tailoring does not comport with "forc[ing the public] to rely on the same prison officials who are responsible for administering the execution to disclose and provide information about any difficulties with the procedure").

138. Mellon, *supra* note 17, at 1119.

139. *Id.* (quoting William C. Thompson, *Evaluating the Admissibility of New Genetic Identification Tests: Lessons from the "DNA War,"* 84 J. CRIM. L. & CRIMINOLOGY 22, 100 (1993)).

140. *See Waller*, 467 U.S. at 45.

141. Wexler, *supra* note 16, at 12, 49–50.

142. *See, e.g.*, ACLU Amicus Brief, *supra* note 2, at 18, 40.

tool used on the public's behalf to convict an accused person would surely be an exaggerated response to private interest concerns.[143] Private concerns like trade secret rights cannot win when balanced against the momentous and bedrock constitutional rights held by the public.[144]

CONCLUSION

Individuals like Mr. Johnson and Mr. Herskovic have been imprisoned on the basis of evidence produced by proprietary algorithms that neither they nor independent experts have had the opportunity to confront and audit. This is the wrong result.

Where a criminal case involves a proprietary algorithm that produced material evidence, the strength of the public's right of access should favor disclosure. This should mean disclosure of source code, which reveals the programmers' intent, assumptions, biases, and mistakes in ways that no other form of the program can as easily reveal. But if a court disagrees, at a minimum, the public should have access to other information that could enable auditing by the public, such as assumptions underlying the source code, defense experts' reports, and the spectrum of results the algorithm calculated. Such disclosure is essential to ensure that justice is occurring in our courtrooms, and where possible, defense counsel and access lawyers should work together to achieve it.

143. California First Amendment Coal. v. Woodford, 299 F.3d 868, 880 (9th Cir. 2002).
144. *See* Mellon, *supra* note 17, at 1119.