Michigan Law Review

Volume 120 | Issue 1

2021

The Missing Algorithm: Safeguarding *Brady* Against the Rise of Trade Secrecy in Policing

Deborah Won
University of Michigan Law School

https://doi.org/10.36644/mlr.120.3.missing

NOTE

THE MISSING ALGORITHM: SAFEGUARDING *BRADY* AGAINST THE RISE OF TRADE SECRECY IN POLICING

Deborah Won[*]

Trade secrecy, a form of intellectual property protection, serves the important societal function of promoting innovation. But as police departments across the country increasingly rely on proprietary technologies like facial recognition and predictive policing tools, an uneasy tension between due process and trade secrecy has developed: to fulfill Brady*'s constitutional promise of a fair trial, defendants must have access to the technologies accusing them, access that trade secrecy inhibits. Thus far, this tension is being resolved too far in favor of the trade secret holder—and at too great an expense to the defendant. The wrong balance has been struck.*

This Note offers three contributions. First, it explains the use of algorithms in law enforcement and the intertwined role of trade secrecy protections. Second, it shows how trade secrecy clashes with the Due Process Clause—the Constitution's mechanism for correcting the power asymmetry between the state and the defendant—and argues that due process should not waver simply because a source of evidence is digital, not human. Third, it proposes a solution that better balances a defendant's due process rights with intellectual property protections.

TABLE OF CONTENTS

[*] J.D., May 2021, University of Michigan Law School. Thank you to Professor Sherman Clark, Nate Wessler, and the Michigan Law Review Notes Office for their feedback and contributions. I am also grateful to Steve Kane and Professors Vivek Sankaran and Bridgette Carr for their mentorship. Finally, I thank my family—including my friends—for their unconditional support.

doi:10.36644/mlr.120.3.missing

INTRODUCTION

Algorithmic policing is on the rise. Investigative tools like facial recognition, DNA genotyping, and predictive policing systems are increasingly—and effectively—being marketed by private technology companies as the best way to police efficiently under tight budget constraints.[1] But because algorithmic systems are built by humans, they exhibit human fallibilities, including racial and gender bias, inconsistency, and error.[2] Despite their similarities, algorithmic systems and humans are treated differently when used against a criminal defendant in court. Humans are subject to adversarial scrutiny; algorithmic systems are not.[3] The difference is attributable to trade secrecy, a form of intellectual property protection designed to maintain "standards of commercial

[1] *See, e.g.*, Beth Pearsall, *Predictive Policing: The Future of Law Enforcement?*, NIJ J., June 2010, at 16, 17 (noting one police chief's belief that predictive policing was "the perfect tool to help departments become more efficient as budgets continue to be reduced"); Ellen Huet, *Server and Protect: Predictive Policing Firm PredPol Promises to Map Crime Before It Happens*, FORBES (Feb. 11, 2015, 6:00 AM), https://www.forbes.com/sites/ellenhuet/2015/02/11/predpol-predictive-policing [perma.cc/7WNJ-KS2A] ("It's impossible to know if PredPol prevents crime, since crime rates fluctuate, or to know the details of the software's black-box algorithm, but budget-strapped police chiefs don't care.").

[2] Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. ONLINE 15, 31–33 (2019).

[3] *See* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 1992 (2017). For example, human witnesses are subject to cross-examination and information about their credibility—or lack thereof—must be shared with the defendant. Boyd v. United States, 908 A.2d 39, 57 (D.C. 2006). Algorithms that serve similar testimonial functions, however, are shielded from inspection. *Compare* Jamison v. Collins, 291 F.3d 380, 389 (6th Cir. 2002) (finding a *Brady* violation where prosecutor failed to disclose evidence about a human eyewitness's "positive identification of different suspects"), *with* Lynch v. State, 260 So. 3d 1166, 1169–70 (Fla. Dist. Ct. App. 2018)

ethics" and "encourage[] invention."[4] When invoked in the criminal context, however, trade secrecy shields algorithmic systems from adversarial scrutiny—even when the Constitution mandates it.[5]

It is perplexing that algorithmic systems receive heightened protection as intellectual property given that defendants' due process rights do not change simply because the investigatory source is digital, not human. This is particularly troubling given the government's affirmative duty under *Brady v. Maryland* to disclose helpful evidence to the criminal defendant.[6] The *Brady* obligation, established by the Supreme Court to ensure that the defendant receives a full and fair trial under the Due Process Clause, requires that the prosecutor turn over any information "favorable" to the defendant that is in the prosecutor's constructive "possession," so long as that evidence is "material" to the defendant's case.[7] Favorable information includes both impeachment[8] and exculpatory[9] evidence. The prosecutor must actively search for favorable evidence not just in their own possession, but also in the possession of any member of the "prosecution team."[10] The prosecutor's duty to search and disclose is "ongoing."[11]

However, prosecutors need only disclose favorable evidence that is "material." The standard for determining materiality may differ depending on whether a prosecutor's *Brady* compliance is evaluated before or after the trial's conclusion. The post-trial materiality standard is well established. A defendant that raises a *Brady* challenge after trial must show prejudice—that there is a "reasonable probability" disclosure of the evidence would have resulted in a

(declining to find a *Brady* violation where the prosecutor failed to disclose evidence about an algorithmic witness's identification of different possible matches).

[4] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481 (1974).

[5] *E.g.*, Brady v. Maryland, 373 U.S. 83, 87 (1963).

[6] *Id.*

[7] *Id.*; Pennsylvania v. Ritchie, 480 U.S. 39, 57 (1987).

[8] Impeachment evidence includes information that would cast doubt on the prosecution's witnesses or expose cracks in its case. Cynthia E. Jones, *A Reason to Doubt: The Suppression of Evidence and the Inference of Innocence*, 100 J. CRIM. L. & CRIMINOLOGY 415, 425 (2010).

[9] Exculpatory evidence includes evidence that tends to negate guilt, reduce culpability, support an affirmative defense, or potentially reduce the severity of a sentence. *Id.* at 423–24.

[10] An individual or entity is a part of the "prosecution team" if their role in the case was to assist the prosecution, evaluated based on "what the person did, not who the person is." United States v. Stewart, 433 F.3d 273, 298 (2d Cir. 2006) (emphasis omitted). The prosecution team, for example, may include law enforcement, crime labs, and expert witnesses. Youngblood v. West Virginia, 547 U.S. 867, 870 (2006); *In re* Brown, 952 P.2d 715, 719–20 (Cal. 1998); *see* State v. Farris, 656 S.E.2d 121, 128–29 (W. Va. 2007).

[11] *Ritchie*, 480 U.S. at 60 ("[T]he duty to disclose is ongoing; information that may be deemed immaterial upon original examination may become important as the proceedings progress.").

different verdict.[12] The *pretrial* materiality standard, however, lacks uniformity. Some courts have imported the post-trial prejudice requirement into the pretrial standard, while others have rejected it and require only that the evidence be favorable.[13] Those courts with a mirrored pretrial standard therefore allow prosecutors to determine whether evidence is *Brady* material based on their own predictions of the eventual trial's outcome. The pretrial prejudice requirement thus makes it easy for prosecutors to manipulate *Brady*'s materiality threshold; prosecutors can cobble together any number of arguments that disclosing evidence would not affect the ultimate verdict. Thus, to maintain the central tenet of *Brady*—that defendants be treated fairly as they face the machinery of the state—defendants should not be required to show prejudice before trial to obtain favorable evidence.[14]

This Note argues that for purposes of *Brady* disclosures, courts should view law enforcement algorithms as analogous to human witnesses and should accordingly implement an at-trial "missing algorithm" remedy when trade secrecy is invoked. Part I provides the factual and legal background of law enforcement algorithms and trade secrecy protections to place the question in context. Part II analyzes *Brady* and its progeny and concludes that algorithmic information falls within a prosecutor's duty to disclose favorable material to the defendant. Part III proposes that courts adopt a missing algorithm rule, allowing juries to draw reasonable and limited inferences to safeguard defendants' due process rights when their access is limited by intellectual property protections.

I. LAW ENFORCEMENT ALGORITHMIC SYSTEMS AND TRADE SECRECY

Machine-learning algorithms are increasingly executing government functions. One context in which algorithmic systems are proliferating is law enforcement and prosecution.[15] As public attention to automated decisionmaking has increased, terms like "algorithm," "machine learning," and

[12] United States v. Bagley, 473 U.S. 667, 682 (1985) (holding that exculpatory evidence is not "material" unless there is a "reasonable probability that . . . the result of the proceeding would have been different" had the evidence been disclosed).

[13] *Compare* United States v. Sudikoff, 36 F. Supp. 2d 1196, 1198–99 (C.D. Cal. 1999) ("This [materiality] standard is only appropriate, and thus applicable, in the context of appellate review. Whether disclosure would have influenced the outcome of a trial can only be determined after the trial is completed and the total effect of all the inculpatory evidence can be weighed against the presumed effect of the undisclosed *Brady* material."), *with* Boyd v. United States, 908 A.2d 39, 59 (D.C. 2006) (interpreting *Bagley* and *Kyles v. Whitley*, 514 U.S. 419, 437 (1995), to require a pretrial "materiality," not "favorable," standard).

[14] For a more comprehensive discussion and argument that courts should reject a pretrial prejudice requirement, see Jones, *supra* note 8.

[15] For example, from 2010 through 2016, over 2,800 arrests were made as a result of facial recognition technology. In 2018 alone, facial recognition was used as an investigative tool in over 8,000 cases. Julie Bosman & Serge F. Kovaleski, *Facial Recognition: Dawn of Dystopia, or Just the New Fingerprint?*, N.Y. TIMES (May 18, 2019), https://www.nytimes.com/2019/05/18/us/facial-recognition-police.html [perma.cc/HU83-Z65H].

"predictive policing" have become buzzwords, often used loosely and interchangeably.[16] Section I.A provides definitions of those terms and a high-level explanation of how an "algorithmic system" works. Section I.B summarizes U.S. trade secrecy law and explains which components of an algorithmic system can be shielded under trade secret protections.

A. *What Are Algorithmic Systems?*

To understand what a *law enforcement* algorithmic system is, it is necessary to first unpack what an algorithmic system is. An algorithmic system involves several separate technical components. As the term suggests, the foundation of the system is the "algorithm," a specified series of logical steps used to accomplish some task.[17] The algorithm is operationalized by source code. Source code is a series of letters, numbers, and punctuation that give the computer instructions on how to act in accordance with the algorithm.[18] Systems vary greatly in how many lines of source code they contain.

A "machine-learning" algorithm is an algorithm that is "taught" on training data to perceive patterns and to subsequently become better at discerning new patterns when exposed to new information.[19] Training data is a collection of examples from which the algorithm is instructed to extract logical rules.[20] "Verification" and "test" data sets are then used to score and refine the performance of the algorithm.[21]

In addition, an algorithmic system requires inputs to produce a desired output. The input is the information fed into the algorithm, and the output is the information created by applying the algorithm to the input data—for example, whether a person's picture has a match in a facial recognition database. Though every algorithmic system requires some kind of input and produces an output, they vary widely depending on the purpose or design of the system and can also vary over time.[22]

These technical components—the algorithm, training data, input, and output—are limited by policy decisions implemented by the designer or the

[16] *See* AI NOW INST., ALGORITHMIC ACCOUNTABILITY POLICY TOOLKIT 2–3 (2018), https://ainowinstitute.org/aap-toolkit.pdf [perma.cc/X2C6-FPD7].

[17] AARON RIEKE, MIRANDA BOGEN & DAVID G. ROBINSON, UPTURN, PUBLIC SCRUTINY OF AUTOMATED DECISIONS 9 (2018), https://omidyar.com/wp-content/uploads/2020/09/Public-Scrutiny-of-Automated-Decisions.pdf [perma.cc/9A9K-JKBN].

[18] Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183, 1193–94 (2019).

[19] Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 881 (2016) (providing a general definition of "machine learning" but noting the inconsistent usage of the phrase); SOLON BAROCAS ET AL., DATA & CIVIL RIGHTS: TECHNOLOGY PRIMER 4 (2014), https://www.datacivilrights.org/pubs/2014-1030/Technology.pdf [perma.cc/NNS7-FS4C].

[20] RIEKE ET AL., *supra* note 17, at 12; BAROCAS ET AL., *supra* note 19, at 4.

[21] Rich, *supra* note 19, at 882.

[22] *See id.* at 921; RIEKE ET AL., *supra* note 17, at 11.

user.[23] Indeed, policies, which are the result of human choices, "govern how both technical and human components of th[e] system should behave."[24] These policy limits might take the form of certain prohibitions built into the algorithm, or they might instruct the user on how to act upon or interpret an algorithm's output.[25]

A "law enforcement algorithmic system," as used in this Note, is an algorithmic system that is used by government entities like police departments for surveillance, investigation, or prosecution purposes.[26] One increasingly common example of a law enforcement algorithmic system is facial recognition technology.[27] A facial recognition algorithm, broadly speaking, is trained to identify faces by analyzing images in a historical dataset.[28] A police officer or analyst can then input an image into the algorithm.[29] The output is a series of similar photos, usually with a probability ranking to denote the likelihood of a "match."[30] Depending on the policies in place, the police officer may or may not act upon the similar photos by finding and detaining any identified individuals.

Each technical component of an algorithmic system involves human judgment. The sequential logical steps embodied by the algorithm and operationalized by the source code are written and designed by humans.[31] The training data is selected by humans. The input is chosen and the output is interpreted by humans. Thus, each component risks human error and human bias.[32]

For example, the historical datasets on which facial recognition and other machine-learning algorithms are trained are often skewed by race and gender.[33] One dataset, deemed the "gold standard benchmark for face recognition," was found to be approximately 83.5 percent white and 77.5 percent

[23] *See* RIEKE ET AL., *supra* note 17, at 11.

[24] *Id.*

[25] *Id.*

[26] While there are law enforcement algorithmic systems that are not "machine learning," this Note focuses on machine-learning systems because they are at the forefront of criminal-justice-technology innovation—the inventions most likely to be declared as trade secrets by developers. However, the thesis and proposed solution of this Note applies to both machine-learning and non-machine-learning technologies alike.

[27] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. CTR. ON PRIV. & TECH. (May 16, 2019), https://www.flawedfacedata.com [perma.cc/S5EY-2X58].

[28] *Amici Curiae* Brief of ACLU et al. in Support of Petitioner at 6, Lynch v. State, No. SC2019-298 (Fla. July 19, 2019) [hereinafter *Lynch* ACLU Amicus Brief], https://www.aclu.org/sites/default/files/field_document/florida_face_recognition_amici_brief.pdf [perma.cc/Y97V-LGEY].

[29] Garvie, *supra* note 27.

[30] RIEKE ET AL., *supra* note 17, at 11.

[31] *See infra* Part II.

[32] *See infra* Part II.

[33] *See* Richardson et al., *supra* note 2, at 18–20; *see also* A.R. LANGE, CTR. FOR DEMOCRACY & TECH., DIGITAL DECISIONS: POLICY TOOLS IN AUTOMATED DECISION-MAKING

male.[34] Unsurprisingly, researchers have found that algorithmic systems are one hundred times more likely to misidentify African and Asian Americans than white individuals,[35] and are also more likely to misidentify women than men.[36] Illustrating this problem, one study tested Rekognition, Amazon's facial recognition tool, and found that it incorrectly identified twenty-eight members of Congress as people from a criminal database.[37] Nonwhite members of Congress were disproportionately misidentified, at about 40 percent of false positives, despite making up only about 20 percent of Congress. That false positives are much higher for racial minorities is particularly concerning given that minorities are also more likely to be subjected to facial recognition searches for law enforcement purposes.[38]

Training data may also be racially skewed because of past discriminatory police practices. When Black men are disproportionately targeted and arrested by police for drug crimes, or when predominantly Black neighborhoods are disproportionately targeted for unjustified police scrutiny and intrusion—to list just a few of the multitude of examples—those racially biased arrests and police contacts create skewed historical data in which Black men are overrepresented.[39] That overrepresentation, often interpreted as indicating

11 (2016), https://cdt.org/wp-content/uploads/2016/01/2016-01-14-Digital-Decisions_Policy-Tools-in-Auto2.pdf [perma.cc/WX9E-JHHL].

[34] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 77, 77, 79 (2018).

[35] Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019, 6:43 PM), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use [perma.cc/WWL9-FEM7].

[36] Buolamwini & Gebru, *supra* note 34, at 2–3.

[37] Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018, 8:00 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [perma.cc/X7QE-Z44N].

[38] Buolamwini & Gebru, *supra* note 34, at 2. In a "striking change" for the prominent supplier of law enforcement technologies, Amazon announced in 2020 that it was placing a temporary, one-year moratorium on the use of Rekognition. The announcement came on the heels of nationwide protest over racism and biased policing and after two years of advocacy by the ACLU to stop Amazon from selling the technology to law enforcement. Karen Weise & Natasha Singer, *Amazon Pauses Police Use of Its Facial Recognition Software*, N.Y. TIMES (June 10, 2020) https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html [perma.cc/KVJ5-E42C].

[39] Richardson et al., *supra* note 2, at 41–46. In addition to the examples discussed, there are many other ways in which training data may be skewed. For example, certain types of crimes, like property theft, may be overrepresented because other types, like white-collar crime, are underenforced or underreported. *Id.* at 41–42, 41 n.119. Concern about flawed training data has likewise been raised in a variety of contexts outside of policing. *E.g.*, Rachel Goodman, *Why Amazon's Automated Hiring Tool Discriminated Against Women*, ACLU (Oct. 12, 2018, 1:00 PM), https://www.aclu.org/blog/womens-rights/womens-rights-workplace/why-amazons-automated-hiring-tool-discriminated-against [perma.cc/VB6H-MZEY] (describing employee hiring algorithm that consistently scored women as less successful job candidates than men due to skewed training data); Angela Lashbrook, *AI-Driven Dermatology Could Leave Dark-Skinned Patients Behind*, ATLANTIC (Aug. 16, 2018), https://www.theatlantic.com/health/archive/2018

greater criminality, may reinforce the biases underlying the discriminatory practices and produce a flawed, circular justification for increasing the policing of already overpoliced communities.[40] Then, when that biased historical data is used to train algorithms, the discrimination becomes "baked in" and can perpetuate and exacerbate the bias—a "garbage in, garbage out" problem.[41]

For instance, in 2012 Chicago deployed the Strategic Subject List (SSL), an algorithmic tool that ranked individuals at risk of becoming either victims or offenders in a shooting or homicide.[42] The tool assigned individuals a risk tier, ranging from "very low" to "very high," but did *not* differentiate between potential "victims" and "offenders."[43] The tool was problematic not only because it weighed arrests rather than convictions as a factor—meaning that the list likely reflected the Chicago Police Department's discriminatory practices of targeting nonwhite individuals and communities—[44] but also because the factor that most affected a person's risk score was *age*.[45] Indeed, *56 percent* of all Black men under thirty in Chicago were listed and assigned risk scores by the SSL.[46] Notably, Black men under thirty were exactly the same demographic targeted by the Chicago Police Department's unlawful stop-and-frisk practices.[47] From these facts, researchers concluded that the tool likely ingested racially skewed data.[48]

Inclusion on the list had serious consequences—two-thirds of the individuals on the list were flagged to receive heightened police scrutiny and were

/08/machine-learning-dermatology-skin-color/567619 [perma.cc/H53U-XQCT] (noting that skin-cancer diagnostic algorithms risk misdiagnosing patients with darker skin because algorithms are trained primarily on data about white patients).

[40] Richardson et al., *supra* note 2, at 41–42.

[41] LANGE, *supra* note 33, at 4.

[42] Richardson et al., *supra* note 2, at 31–32.

[43] *Id.* at 31.

[44] *Id.* at 31 & n.68.

[45] Because the Chicago Police Department refused to release the algorithm, citing proprietary concerns, researchers worked backwards from an available dataset of scores (obtained only after a lengthy legal dispute) to determine how the SSL calculated scores. Jeff Asher & Rob Arthur, *Inside the Algorithm That Tries to Predict Gun Violence in Chicago*, N.Y. TIMES (June 13, 2017), https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html [perma.cc/KCF2-B8TN]; Brianna Posadas, *How Strategic Is Chicago's "Strategic Subjects List"? Upturn Investigates.*, MEDIUM (June 22, 2017), https:/medium.com/equal-future/how-strategic-is-chicagos-strategic-subjects-list-upturn-investigates-9e5b4b235a7c [perma.cc/Y3HW-H3XY]. Two independent analyses by the *New York Times* and *Upturn* confirmed that age was the most important factor in SSL's score assessment. *Id.*

[46] Richardson et al., *supra* note 2, at 32.

[47] These practices were the subject of a 2015 settlement agreement. *See Investigatory Stop and Protective Pat Down Settlement Agreement*, ACLU ILL. 2–8 (Aug. 6, 2015), https://www.aclu-il.org/sites/default/files/wp-content/uploads/2015/08/2015-08-06-Investigatory-Stop-and-Protective-Pat-Down-Settlement-Agreeme....pdf [perma.cc/7MEP-FSNC].

[48] Richardson et al., *supra* note 2, at 15.

more likely to be arrested as a direct result of being included on the list.[49] While it is unclear how officers actually used SSL predictions in the field,[50] one Chicago Police Department directive encouraged "[t]he highest possible charges" for all individuals on the list, regardless of their risk score, so long as they had received notice about being on the list and were subsequently arrested.[51] The SSL is thus a cautionary example of how a tool trained on "dirty data" risks "perpetuating additional harm via feedback loops"[52]—harm laden with grave privacy and civil rights implications for those targeted individuals.[53]

Furthermore, even a simple "accident" in the source code, such as a mistaken ampersand, can result in substantive differences.[54] One study found that 33 percent of "highly experienced" programmers failed to properly use parentheses, which in complex programs could result in "tens of thousands of errors."[55] For example, source code errors in STRmix, a probabilistic DNA genotyping program,[56] produced incorrect results—stating a percentage likelihood that the defendant's DNA matched a sample at the crime scene when that percentage was off by a factor of ten—in sixty criminal cases.[57] Prosecutors were forced to replace twenty-four expert statements after that coding-

[49] *Id.* at 31 n.65, 32; *see also* Jessica Saunders, Priscilla Hunt & John S. Hollywood, *Predictions Put Into Practice: A Quasi-experimental Evaluation of Chicago's Predictive Policing Pilot*, 12 J. EXPERIMENTAL CRIMINOLOGY 347, 366–67 (2016).

[50] Posadas, *supra* note 45; *see also* Saunders et al., *supra* note 49, at 347 ("One potential reason why being placed on the list resulted in an increased chance of being arrested for a shooting is that some officers may have used the list as leads to closing shooting cases.").

[51] Richardson et al., *supra* note 2, at 32–33.

[52] *Id.* at 15.

[53] After eight years of employing the SSL, the Chicago Police Department quietly decommissioned the tool in early 2020 following an investigation by the Office of the Inspector General. Kathleen Foody, *Chicago Police End Effort to Predict Gun Offenders, Victims*, AP NEWS (Jan. 23, 2020), https://apnews.com/article/41f75b783d796b80815609e737211cc6 [perma.cc/X2EL-T5DU]. While the SSL is now out of commission, the Chicago Police Department plans to deploy other predictive policing tools in the future. *Advisory Concerning the Chicago Police Department's Predictive Risk Models*, CITY OF CHI. OFF. OF INSPECTOR GEN. (Jan. 23, 2020), https://igchicago.org/2020/01/23/advisory-concerning-the-chicago-police-departments-predictive-risk-models [perma.cc/MCF6-RCWB].

[54] Christian Chessman, Note, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CALIF. L. REV. 179, 186–95 (2017).

[55] *Id.* at 186–87.

[56] Probabilistic DNA genotyping programs use algorithms to analyze "complex" DNA mixtures, samples which contain the DNA of multiple unknown individuals. In contrast to the analysis of "simple" DNA samples (involving the DNA of just one or perhaps two persons), complex-mixture analysis involves subjective interpretation and thus does not produce objective results, nor has it been thoroughly tested for reliability. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFF. OF THE PRESIDENT, FORENSIC SCIENCE IN CRIMINAL COURTS: ENSURING SCIENTIFIC VALIDITY OF FEATURE-COMPARISON METHODS 7–8 (2016); PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFF. OF THE PRESIDENT, AN ADDENDUM TO THE PCAST REPORT ON FORENSIC SCIENCE IN CRIMINAL COURTS 8 (2017).

[57] Katyal, *supra* note 18, at 1244; Amicus Curiae Brief of Elec. Frontier Found. in Support of Defendant & Appellant Billy Ray Johnson at 13, People v. Johnson, No. F071640 (Cal. Ct. App. July 11, 2019), 2017 WL 10320827, at *13 [hereinafter *Johnson* EFF Amicus Brief]; Brief

error discovery.[58] In one New York trial involving a different DNA genotyping program, the judge granted the defense access to the program despite the government's objections to access on "proprietary" grounds.[59] Review of the source code uncovered that the program had dropped essential data from its calculations in ways that would have unpredictably changed the program's DNA probability results.[60] Once the defense expert witness testified to that effect, the prosecution withdrew the DNA evidence against the defendant.[61]

Additionally, inputs are selected by humans, who may feed nonsensical data to the algorithm.[62] Yet another variation of the garbage in, garbage out problem, such inputs would only produce nonsensical outputs.[63] For example, when the New York Police Department (NYPD) was investigating a beer theft, it first fed the facial recognition tool a store surveillance image of the actual culprit.[64] But when that input produced no match, NYPD decided to input an image of celebrity Woody Harrelson because one officer remarked that the culprit resembled a Woody Harrelson with long hair.[65] Based on the Woody Harrelson "matches," the police arrested the defendant (who was *not* Woody Harrelson).[66] While NYPD declined to admit what happened to the non-Woody Harrelson after the arrest,[67] the incident illustrates how prone to human error, and thus how fallible, algorithms can be. In addition to celebrity images, records show that police departments use other concerning inputs such as artist sketches and graphically modified images.[68]

Similarly, outputs may also be selectively chosen by humans in problematic ways. For example, Willie Lynch was convicted in Florida for selling fifty

of *Amici Curiae* ACLU & ACLU of San Diego & Imperial Cntys. in Support of Real Party in Int. Seeking Dismissal at 25, People v. Superior Ct., 239 Cal. Rptr. 3d 71 (Ct. App. 2018) [hereinafter *Superior Court* ACLU Amicus Brief].

[58] *Superior Court* ACLU Amicus Brief, *supra* note 57, at 25.

[59] 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 [perma.cc/KD4R-Q4S8].

[60] *Id.*

[61] *Id.*

[62] While a specific input is not itself a trade secret, the user manuals that may tell police officers what inputs should or should not be used may be claimed as a trade secret to prevent defendants from reviewing them. *See* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1367 (2018) ("Police departments have cited trade secrets as reason to deny open records requests for face recognition user manuals and audit information.").

[63] Garvie, *supra* note 27.

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] Bosman & Kovaleski, *supra* note 15 ("The New York Police Department declined to say whether the [Woody Harrelson "match"] had been convicted, but defended its use of [facial recognition] technology, saying that . . . [it] had led to arrests in homicides, rapes and robberies and had even helped identify a woman with Alzheimer's.").

[68] Garvie, *supra* note 27.

dollars' worth of drugs based on a facial recognition database called Face Analysis Comparison Examination System (FACES).[69] During a drug sale, police officers surreptitiously photographed the seller with a cell phone camera. The photos were blurry in places and taken at an oblique angle.[70] The officers, not knowing who the individual was, did not make an arrest on the scene.[71] Instead, they sent the cell phone photos to an analyst.[72] That analyst fed the low-quality photos into FACES, which produced five possible African American suspects, including Lynch.[73] FACES only designated Lynch at a one-star level of confidence—the lowest number of stars for "likelihood" that the match was accurate.[74] Despite the low rating, the analyst selected Lynch and submitted his identification information to the officers. No other matches were submitted. The officers promptly arrested Lynch. At trial, Lynch raised just one defense—that he was mistakenly identified as the seller.[75] Lynch was convicted, and on appeal he asked to see the other matches produced by FACES because it would help his defense.[76] The Florida appeals court denied Lynch's request. The court reasoned that because Lynch could not show that the other algorithm-produced matches resembled him, he could not show that access to those photos would support his argument that he was mistakenly identified.[77] Of course, the court did not address how Lynch would have been able to show that those photos resembled him without any access to the photos in the first place.[78] Willie Lynch was sentenced to eight years of incarceration and is currently in prison.

This Section has shown that the potential for error—the same flaws, biases, and lapses in judgment that humans exhibit—is embedded in every component of algorithmic systems. However, while that commonality would urge the same scrutiny for both human and algorithmic error in criminal cases, trade secrecy shrouds the latter.

[69] Lynch v. State, 260 So. 3d 1166, 1168–69 (Fla. Dist. Ct. App. 2018).

[70] *Lynch* ACLU Amicus Brief, *supra* note 28, at 2.

[71] *Id.* at 2–3.

[72] *Lynch*, 260 So. 3d at 1169.

[73] Aaron Mak, *Facing Facts*, SLATE: FUTURE TENSE (Jan. 25, 2019, 12:49 PM), https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html [perma.cc/7DSC-D5NW].

[74] *Lynch* ACLU Amicus Brief, *supra* note 28, at 14.

[75] *Id.* at 1.

[76] Mak, *supra* note 73.

[77] *Lynch*, 260 So. 3d at 1170.

[78] Further, as Lynch's public defender stated in his motion for rehearing, it "strains credulity" to say that none of the other potential matches resembled Lynch. Motion for Rehearing & Written Op. at 2, *Lynch*, 260 So. 3d. 1166 (No. 1D16-3290).

B. *What Are Trade Secrets and What Can They Shield from Disclosure?*

There are four forms of intellectual property: copyright, patents, trademarks, and trade secrets.[79] One central purpose of intellectual property protection is to promote innovation by ensuring the creator has the financial incentives to innovate given the significant investment of resources required to do so.[80] All four forms of intellectual property thus provide some legal mechanism that protects the innovator's ability to reap the financial benefits of their investment.[81]

Trade secrecy's mechanism targets misappropriation: the improper use, acquisition, or disclosure of a trade secret.[82] A trade secret designation offers "powerful legal protections to companies that want to keep their business practices a secret."[83] Trade secret holders receive two types of protection. First, substantive trade secret protection allows proprietors to recover monetary damages for trade secret misappropriation and to secure injunctive relief against future misappropriation.[84] Second, evidentiary trade secret protection allows proprietors to shield their trade secret when in court, preventing business competitors from exploiting court proceedings to obtain commercially valuable information.[85]

Trade secrets are the youngest and least restrained form of intellectual property protection.[86] For example, while patent protection requires one to undergo a formal application and approval process and has a set expiration

[79] *See* Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 315 (2008). Intellectual property is defined as, broadly speaking, "creations of the mind." WORLD INTELL. PROP. ORG., WHAT IS INTELLECTUAL PROPERTY? 1 (2020), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_450_2020.pdf [perma.cc/BLP3-K2GR].

[80] WORLD INTELL. PROP. ORG., *supra* note 79, at 2; *see also* Lemley, *supra* note 79, at 329–30; Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241, 262 (1998) (explaining that the "incentives to create" justification is "well-established as the principal economic justification for intellectual property rights in general" and is the "most frequently invoked" justification for trade secrecy).

[81] Lemley, *supra* note 79, at 329–30; Bone, *supra* note 80, at 262–63.

[82] Jessica M. Meyers, *Artificial Intelligence and Trade Secrets*, LANDSLIDE, Jan./Feb. 2019, at 17, https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2018-19/january-february/artificial-intelligence-trade-secrets-webinar [perma.cc/D9VY-9X4L]. In contrast, other forms of intellectual property like patents and copyright provide proprietors with a monopoly over the property's use. *Id.*

[83] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 17 (2014).

[84] Wexler, *supra* note 62, at 1382.

[85] *Id.* at 1382–83.

[86] *See* David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 BERKELEY TECH. L.J. 1091, 1095 (2012).

date,[87] trade secret protection requires no formal process and can extend indefinitely.[88] There is no uniform definition of trade secrets, but they are generally described as "confidential, commercially valuable information."[89] To procure protection, the purported trade secret needs to meet just two requirements: (1) it derives independent economic value from being generally not known and (2) reasonable efforts have been made by the trade secret holder to maintain its secrecy.[90]

The trade secret evidentiary privilege raises the defendant's burden for discovery. When it is invoked, the defendant must make a "particularized showing" that what they seek is "necessary to the defense."[91] If the defendant cannot show necessity, then the proprietor can shield the algorithmic information entirely; the defendant is not allowed access even with a protective order.[92]

Thus, trade secrecy can be invoked to shield algorithmic systems from scrutiny at all stages of a case or proceeding.[93] Specifically, the algorithm and source code, training data, user manuals, and audit information can be claimed as proprietary under the expansive definition of trade secrets.[94] Law enforcement technology proprietors and prosecutors have already begun to invoke trade secrecy to avoid disclosure and scrutiny of their algorithmic systems.[95]

The invocation of trade secrecy to shield law enforcement algorithmic systems is likely to increase. In 2014, the Supreme Court made it more difficult

[87] *See* Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (codified as amended in scattered sections of 35 U.S.C.).

[88] United States v. Dubilier Condenser Corp., 289 U.S. 178, 186 (1933) (explaining that an inventor "may keep his invention secret and reap its fruits indefinitely").

[89] BRIAN T. YEH, CONG. RSCH. SERV., R43714, PROTECTION OF TRADE SECRETS: OVERVIEW OF CURRENT LAW AND LEGISLATION 2 (2016).

[90] UNIF. TRADE SECRETS ACT § 1(4) (UNIF. L. COMM'N 1985).

[91] People v. Superior Ct. (*Chubbs*), No. B258569, 2015 WL 139069, at *6 (Cal. Ct. App. Jan. 9, 2015). While the California evidence code does not expressly require a showing of particularity or necessity, the court of appeals in *Chubbs* read those requirements into the statutory text. *See* Wexler, *supra* note 62, at 1352 & n.39. *Chubbs* "is now being cited . . . across the country," and other state courts are adopting a similar interpretation. *Id.* at 1360–61 (collecting cases).

[92] Wexler, *supra* note 62, at 1359.

[93] *E.g.*, FED. R. EVID. 1101(c) (providing that "[t]he rules on privilege," including trade secret privilege, "apply to all stages of a case or proceeding.").

[94] *E.g.*, Wexler, *supra* note 62, at 1367, 1370.

[95] *See* Citron & Pasquale, *supra* note 83, at 5 (explaining that vendors selling technology have fought to ensure that their algorithms are "shrouded in secrecy," often by invoking trade secret protections); *see also* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 19, 23–26 (2017) (noting that vendors will also often require nondisclosure agreements from their public agency customers); Wexler, *supra* note 62, at 1360 & n.71 (reviewing cases where prosecutors and developers have cited *Chubbs* to justify withholding trade secret information).

to patent software in *Alice Corp. v. CLS Bank International*,[96] thereby encouraging developers to use trade secrecy rather than patents to protect their intellectual property.[97] And in 2016, Congress established the first federal cause of action for trade secret misappropriation by passing the Defend Trade Secrets Act.[98] The availability of a federal cause of action enables proprietors to more easily and efficiently pursue out-of-state and out-of-country infringers, making trade secrecy an appealing choice.[99]

Additionally, state courts are increasingly adopting a criminal trade secret evidentiary privilege.[100] At least twenty-one states have a codified trade secret privilege in their evidence code, and many states recognize a common law privilege.[101] While the trade secret privilege was often invoked in civil cases, it was not until 2015 that the evidentiary privilege was first extended to a criminal case.[102] Since that first case, courts across the country are beginning to expressly allow the privilege to withhold evidence from defendants.[103] Indeed, in a span of just five years, from 2013 to 2018, courts in no fewer than five states denied access to algorithmic information due to trade secrecy.[104] These developments, alongside the lack of any formal claim requirements or expiration date,[105] heavily incentivize algorithm developers to rely more on trade secret protections than on other branches of intellectual property.[106]

Because evidentiary privileges "apply to all stages of a case or proceeding,"[107] trade secrecy protections can be invoked before trial, at trial, and after trial.[108] Before trial, proprietors can invoke the privilege against defendants

[96] 573 U.S. 208 (2014).

[97] Katyal, *supra* note 18, at 1214 ("[T]he uncertainty of patent protection, especially in a post-*Alice* world, can push inventors toward the rational belief that the code is much more valuable as a secret than as a patented invention.").

[98] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, § 2, 130 Stat. 376, 376–82 (codified at 18 U.S.C. § 1836).

[99] Meyers, *supra* note 82 (noting that before the Defend Trade Secrets Act, trade secrets lagged behind the other three forms of intellectual property, which were all covered by federal statute).

[100] *See* Wexler, *supra* note 62, at 1350.

[101] The states that have codified a trade secret privilege include Alabama, Alaska, Arkansas, California, Delaware, Florida, Hawaii, Kansas, Louisiana, Maine, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Dakota, Oklahoma, South Carolina, South Dakota, Texas, and Wisconsin. Wexler, *supra* note 62, at 1352 & n.39.

[102] Wexler, *supra* note 62, at 1358–59.

[103] *Id.* at 1361–62, 1361 n.80.

[104] *Id.* at 1362 n.80 (California, New York, Ohio, Pennsylvania, and Washington). Some courts have denied access based expressly on a trade secret privilege, while others have instead incorporated the evidence's trade secret status into their evaluations of defendants' requests for access. *Id.*

[105] *See supra* text accompanying notes 87–88.

[106] Wexler, *supra* note 62, at 1350; *see* Alice Corp. v. CLS Bank Int'l, 573 U.S. 208, 217–26 (2014).

[107] FED. R. EVID. 1101(c).

[108] Wexler, *supra* note 62, at 1357.

seeking information about the algorithmic systems used in the law enforcement investigation—information that the defendant could have used in suppression hearings.[109] At trial, the proprietor (or the prosecutor on behalf of the proprietor) can invoke the privilege to shield an algorithmic system used as evidence.[110] After trial, the proprietor can invoke the privilege in bail or sentencing proceedings if the defendant seeks access to a risk-assessment algorithmic tool.[111] In addition, proprietors may invoke the privilege if a convicted defendant seeks an appeal.[112]

Law enforcement algorithmic tools are increasingly being used across the country. Surveillance technology companies like Palantir and PredPol that market to government entities and police departments claim that their machine-learning technology is the best way to efficiently police under tight budget constraints.[113] Thus, products like facial recognition technology have proliferated. For example, from 2010 through 2016, facial recognition technology resulted in approximately 2,800 arrests.[114] In 2018 alone, over 8,000 cases used facial recognition as an investigative tool.[115] And companies are developing new uses and new tools to capture the lucrative law enforcement market.[116] Because law enforcement algorithmic tools are becoming more prevalent and the incentives for proprietors to choose trade secrecy over other intellectual property protections are increasing, courts will have to grapple more and more with the invocation of trade secrets in criminal proceedings.

[109] *Id.* at 1365.

[110] People v. Superior Ct. (*Chubbs*), No. B258569, 2015 WL 139069, at *1 (Cal. Ct. App. Jan. 9, 2015).

[111] Wexler, *supra* note 62, at 1368–70.

[112] *E.g.*, People v. Superior Ct., 239 Cal. Rptr. 3d 71 (Ct. App. 2018).

[113] *See supra* note 1 and accompanying text.

[114] Bosman & Kovaleski, *supra* note 15.

[115] *Id.* However, some municipalities have recently moved to ban facial recognition tools. *E.g.*, Kate Conger, Richard Fausset & Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [perma.cc/D7PD-NYEN]; Ally Jarmanning, *Boston Lawmakers Vote to Ban Use of Facial Recognition Technology by the City*, NPR (June 24, 2020, 7:05 PM), https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/06/24/883107627/boston-lawmakers-vote-to-ban-use-of-facial-recognition-technology-by-the-city [perma.cc/85EJ-LB56].

[116] Drew Harwell, *Facial Recognition May Be Coming to a Police Body Camera Near You*, WASH. POST (Apr. 26, 2018, 11:30 AM), https://www.washingtonpost.com/news/the-switch/wp/2018/04/26/facial-recognition-may-be-coming-to-a-police-body-camera-near-you [perma.cc/B5DP-DT25] (facial recognition tools incorporated into body cameras); Maura Dolan, *'Rapid DNA' Promises Breakthroughs in Solving Crimes. So Why Does It Face a Backlash?*, L.A. TIMES (Sept. 25, 2019, 5:00 AM), https://www.latimes.com/california/story/2019-09-24/rapid-dna-forensics-crime-police [perma.cc/6JSV-SZST] (rapid complex DNA tests).

II. WHEN DUE PROCESS AND TRADE SECRETS CLASH

Trade secrets can be invoked to shield from disclosure significant parts of a law enforcement algorithmic tool, including the algorithm, the implementing source code, and the training data (collectively shorthanded here as "algorithmic information"). In the criminal context, trade secrecy protections allow law enforcement and prosecutors to shirk their *Brady* disclosure responsibilities when they use algorithms to identify, investigate, and prosecute a suspect. This Part discusses the constitutional tension between intellectual property and a defendant's due process rights and explains why the principles of *Brady* require that the latter, not the former, prevail.

A. *The* Brady *Doctrine: Human Witnesses and Their Algorithmic Counterparts*

In *Brady v. Maryland*, the Supreme Court held that a prosecutor cannot withhold evidence "favorable to an accused" because such suppression violates the defendant's due process rights under the Fifth and Fourteenth Amendments.[117] The *Brady* doctrine thus imposes upon prosecutors a duty to learn of and disclose to the defendant any information in their possession that is "favorable" and "material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution."[118]

The *Brady* doctrine represents a limited and necessary departure from the pure adversarial model of the United States legal system.[119] Such a departure is warranted because the prosecutor represents not an ordinary party but a sovereignty; as such, the prosecutor's purpose is "not that it shall win a case, but that justice shall be done."[120] The Supreme Court created this duty to disclose because "[s]ociety wins not only when the guilty are convicted but when criminal trials are fair; our system of the administration of justice suffers when any accused is treated unfairly."[121] Ultimately, the *Brady* requirement is a "rule of fairness"—an essential tenet of our criminal justice system.[122] The *Brady*

[117] 373 U.S. 83, 87 (1963).

[118] *Brady*, 373 U.S. at 87; *see also* Kyles v. Whitley, 514 U.S. 419, 437 (1995) ("[T]he 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.").

[119] United States v. Bagley, 473 U.S. 667, 675 n.6 (1985) ("By requiring the prosecutor to assist the defense in making its case, the *Brady* rule represents a limited departure from a pure adversary model.")

[120] *Id.* (quoting Berger v. United States, 295 U.S. 78, 88 (1935)).

[121] *Brady*, 373 U.S. at 87.

[122] Boyd v. United States, 908 A.2d 39, 61 (D.C. 2006) (quoting Curry v. United States, 658 A.2d 193, 197 (D.C. 1995)).

doctrine also serves to safeguard against the inherent power asymmetry between the state and defendant, helping to equalize an otherwise deeply skewed system.[123]

1. The Rise of Trade Secrecy in Policing

Despite the necessity of the *Brady* requirement for a fair criminal system, trade secret protections directly clash with, and pose a threat to, the constitutional defenses erected by *Brady*. While research in this area is limited by barriers to access,[124] researchers have been able to identify flaws in proprietary algorithms. These flaws, discussed in Part I, are pervasive in law enforcement algorithmic tools. For example, law enforcement algorithms have been found to be systematically biased based on race and gender due to the use of data skewed by past discriminatory police practices in algorithm development.[125] Because the systems are built and trained upon biased data, they allow police departments to recast past discriminatory practices as infallible new technology, thereby deepening and perpetuating those discriminatory practices.[126] Law enforcement algorithms can also have mistakes in their source code: even

[123] *See* Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CALIF. L. REV. 721, 757 (2007).

[124] Trade secrecy and other forms of intellectual property protection are one such barrier. For example, police departments have denied researchers' requests for even the *user manuals* for their facial recognition tools, citing trade secret exemptions. Wexler, *supra* note 62, at 1367. Trade secret protections are an especially difficult barrier for researchers since trade secrets are also exempt from federal and state open-records laws, which researchers often rely on to obtain records from public entities. *Id.* at 1366, 1367 n.113; *see* Freedom of Information Act, 5 U.S.C. § 552b(c)(4). Other barriers include efforts by law enforcement to conceal their deployment of new technologies, Joh, *supra* note 95, at 29 (describing how two police departments shielded their use of stingray devices (cell-site simulators) for nearly a decade by calling the devices "confidential informants"); other privileges raised to prevent disclosure, such as the "law enforcement privilege," *see, e.g.*, Puerto Rico v. United States, 490 F.3d 50, 64 (1st Cir. 2007) (describing how the law enforcement privilege intends to prevent interference with law enforcement investigations, techniques, and protocols); efforts by proprietors to keep their government contracts a secret, April Glaser, *Thousands of Contracts Highlight Quiet Ties Between Big Tech and U.S. Military*, NBC (July 8, 2020, 4:58 PM), https://www.nbcnews.com/tech/tech-news/thousands-contracts-highlight-quiet-ties-between-big-tech-u-s-n1233171 [perma.cc/P9VR-VXR9]; and logistical hurdles raised by the complicated nature of algorithms, Rob Kitchin, *Thinking Critically About and Researching Algorithms*, 20 INFO. COMMC'N & SOC'Y 14, 20–21 (2017) (explaining why algorithms' "heterogeneous and embedded" nature makes them difficult to fully deconstruct and understand).

[125] Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (July 22, 2019, 7:00 AM), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally [perma.cc/F5D4-KTLH]; Rich, *supra* note 19, at 909, 922 n.357; *see also* Sahil Chinoy, Opinion, *The Racist History Behind Facial Recognition*, N.Y. TIMES (July 10, 2019), https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html [perma.cc/68YD-WZH5]; Buolamwini & Gebru, *supra* note 34.

[126] Richardson et al., *supra* note 2, at 40–46; Karen Hao, *Police Across the US Are Training Crime-Predicting AIs on Falsified Data*, MIT TECH. REV. (Feb. 13, 2019), https://www.technologyreview.com/2019/02/13/137444/predictive-policing-algorithms-ai-crime-dirty-data [perma.cc/HC9Y-J977].

an error as simple as a misplaced ampersand can significantly alter the algorithm's operation.[127] Despite mounting evidence of their fallibility, police departments across the country continue to acquire and implement proprietary algorithmic tools—often in secret.[128]

Prosecutors and proprietors are already resisting disclosure of information pertaining to law enforcement algorithms in criminal cases. For example, the New York Police Department (NYPD) used facial recognition technology to find a man who stole a pair of socks in a department store using an image from the store's surveillance camera.[129] Multiple potential matches were generated.[130] From those matches, the NYPD detective selected a photo of Andre[131] and texted an officer who had witnessed the incident, "Is this the guy?"[132] The officer texted back in the affirmative. Andre's attorneys argued that the single photograph and text-message confirmation was the "sole basis" for the arrest. When Andre tried to obtain information about NYPD's use of the facial recognition program, NYPD and prosecutors resisted, claiming that disclosure would violate the trade secrecy of the program's owner, a third-party vendor. Before the disclosure issue was resolved, Andre took a plea deal.[133]

Had the other suspect matches come from a human eyewitness rather than from a facial recognition program, the prosecutors would not have been able to shield the eyewitness from scrutiny.[134] *Brady* would have required the prosecutors to disclose that the eyewitness had identified multiple possible

[127] *See* Chessman, *supra* note 54, at 187; Wexler, *supra* note 62, at 1368.

[128] *See* Mick Dumke & Frank Main, *A Look Inside the Watch List Chicago Police Fought to Keep Secret*, CHI. SUN-TIMES (May 18, 2017, 9:26 AM), https://chicago.suntimes.com/2017/5/18/18386116/a-look-inside-the-watch-list-chicago-police-fought-to-keep-secret [perma.cc/E8VF-AAY9]; JAKE LAPERRUQUE, PROJECT ON GOV'T OVERSIGHT, FACING THE FUTURE OF SURVEILLANCE (2019), https://s3.amazonaws.com/docs.pogo.org/report/2019/Facing-the-Future-of-Surveillance_2019.pdf [perma.cc/K6PM-6JUN].

[129] Mike Hayes, *"Is This the Guy?*," APPEAL (Aug. 20, 2019), https://theappeal.org/is-this-the-guy [perma.cc/CX6S-4VJX].

[130] *Id.*

[131] "Andre" is the pseudonym *The Appeal* gave the defendant at his attorneys' behest. *Id.*

[132] *Id.*

[133] *Id.*

[134] *E.g.*, People v. Robinson, 37 Cal. Rptr. 2d 183, 186 (Ct. App. 1995) ("When exculpatory evidence involves an eyewitness to the crime, what must be disclosed is not just the witness's identity 'but all pertinent information which might assist the defense to locate him.' " (quoting Eleazer v. Superior Ct., 464 P.2d 42, 44 (Cal. 1970))).

suspects *other* than the defendant,[135] as well as the eyewitness's level of certainty (or uncertainty) about each identification.[136] This would be true even if the eyewitness's testimony were not introduced by the prosecutor at trial and only the witnessing police officer were to testify.[137] That the prosecutor declined to use the eyewitness at trial does not negate the *Brady* value of the eyewitness's uncertainty or unreliability. Further, had the prosecutor introduced the eyewitness at trial (or had the testifying police officer improperly or sloppily relied on such an unreliable investigative lead, as seems likely in Andre's case),[138] the prosecutor would be required to disclose information challenging the credibility of the eyewitness—including evidence that the witness was racially biased[139] or had previously given inconsistent statements.[140] Thus, had the NYPD relied on a human eyewitness in its investigation, *Brady* would have afforded Andre the evidence he needed to present a full defense. But since the NYPD relied on a proprietary tool and could therefore invoke trade secrecy, Andre was denied that same evidence.[141]

[135] *See* Carrillo v. County of Los Angeles, 798 F.3d 1210, 1227–28 (9th Cir. 2015) (allowing suit for *Brady* violation to proceed because the officer failed to disclose, among other things, that the eyewitness had selected several other photos before identifying the defendant's photo from a line-up).

[136] *See, e.g.*, Boyette v. Lefevre, 246 F.3d 76, 91 (2d Cir. 2001) (noting that a witness's statement about uncertainty of her identification of defendant was "classic *Brady* material"); Jacobs v. Singletary, 952 F.2d 1282, 1287–89 (11th Cir. 1992) (finding a *Brady* violation when the state withheld a polygraph report about an eyewitness's lack of certainty about what he saw).

[137] Police departments often defend their use of law enforcement algorithms by stating that such tools merely provide investigative leads and are not used at trial. *Compare* Hayes, *supra* note 129 ("Like eye-witness testimony, . . . a facial recognition match serves as one piece of a larger investigation. It is a lead, not probable cause . . . ."), *with* Garvie, *supra* note 27 ("[T]he reality is that suspects are being apprehended almost entirely on the basis of face recognition [matches].").

[138] *See* Kyles v. Whitley, 514 U.S. 419, 446 n.15 (1995) (emphasizing that jurors must be able to weigh "the sloppiness of the investigation against the probative force of the State's evidence"); *see also* Bowen v. Maynard, 799 F.2d 593, 613 (10th Cir. 1986) ("A common trial tactic of defense lawyers is to discredit the caliber of the investigation or the decision to charge the defendant, and we may consider such use in assessing a possible *Brady* violation.").

[139] *See, e.g.*, State v. Williams, 956 A.2d 375, 380 (N.J. Super. Ct. App. Div. 2008) (emphasizing that "there is no room for racial bias in any law enforcement investigation" and requiring prosecutor to turn over information relating to officer's racial animus and use of racial epithet in referring to defendant under *Brady*); Gonzales v. State, 929 S.W.2d 546, 550 (Tex. Ct. App. 1996) (stating that "[r]acial prejudice is a prototypical form of bias" and thus must be disclosed as impeachment evidence under Texas criminal-procedure rules); *cf.* United States v. Jernigan, 492 F.3d 1050, 1054 (9th Cir. 2007) (stating that since cross-racial eyewitness identifications are already "particularly suspect," suppression of evidence calling those identifications into question was a *Brady* violation).

[140] *See* White v. Helling, 194 F.3d 937, 943–46 (8th Cir. 1999) (finding a *Brady* violation where prosecutor failed to disclose that its key eyewitness had originally identified another individual and only identified the defendant after meetings with the police).

[141] Another defendant who was denied access to algorithmic information is Billy Ray Johnson. Johnson was convicted of twenty-four crimes based on DNA evidence generated by

Cases like Andre's illustrate the costs of weakening *Brady* protections in the face of new law enforcement technology.[142] The costs will continue to mount as trade secret protections are increasingly raised by prosecutors and faced by defendants.[143]

Technological advances will also accelerate the rate of trade secret invocations in criminal proceedings. Law enforcement algorithm tools, the components of which can be claimed as trade secrets,[144] are proliferating.[145] These tools are being marketed as a cost-effective investigation solution to law enforcement agencies, who are among the biggest consumers of algorithmic technologies like facial recognition programs.[146] Thus, trade secret protections are likely to be increasingly invoked against defendants' requests for law enforcement algorithmic information.

As more proprietary tools are adopted by law enforcement, more criminal defendants will need—and more proprietors will resist—access to algorithmic systems. Indeed, a similar trend can be traced with tools that have had more time to be challenged in courts.[147] For example, the use of probabilistic DNA

TrueAllele, a proprietary probabilistic DNA genotyping tool. Before and during his trial, Johnson requested access to the tool's source code. The trial court denied Johnson access under California's codified trade secret privilege. Johnson was sentenced to life in prison without parole. On appeal, the California Court of Appeal recognized that Johnson and amici had made a "strong showing" that TrueAllele produced inconsistent results but declined to evaluate the trial court's denial because "any error was harmless." People v. Johnson, No. F071640, 2019 WL 3025299, at *1, *8, *10 (Cal. Ct. App. July 11, 2019).

[142] *See* Boyd v. United States, 908 A.2d 39, 61 (D.C. 2006).

[143] *See* Hayes, *supra* note 129; RASHIDA RICHARDSON, JASON M. SCHULTZ & VINCENT M. SOUTHERLAND, AI NOW INST., LITIGATING ALGORITHMS 2019 US REPORT: NEW CHALLENGES TO GOVERNMENT USE OF ALGORITHMIC DECISION SYSTEMS 17 (2019), https://ainowinstitute.org/litigatingalgorithms-2019-us.pdf [perma.cc/DNR2-Q5C9] (explaining that a "common justification[] for nondisclosure" of algorithmic information is that "trade secrecy protections limit[] disclosure"); *see also* Wexler, *supra* note 62, at 1360 (discussing a trade-secret-privilege case "now being cited in criminal proceedings across the country to justify withholding trade secret evidence from the accused").

[144] *See supra* Part I.

[145] *See, e.g.*, *supra* notes 113–116 and accompanying text; RICHARDSON ET AL., *supra* note 143, at 17; Harwell, *supra* note 116 (reporting that the largest seller of police body cameras—now used by most major-city police departments—is developing facial recognition analysis for live body-camera footage, which may "lead to police misidentifying innocent people as suspects or wanted criminals").

[146] *See Facial Recognition: Top 7 Trends*, THALES, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition [perma.cc/8Q43-J5VZ] (last updated June 6, 2021) ("The two most significant drivers of this growth are surveillance in the public sector and numerous other applications in diverse market segments."); Julia Horowitz, *Tech Companies Are Still Helping Police Scan Your Face*, CNN BUS. (July 3, 2020, 8:36 AM), https://www.cnn.com/2020/07/03/tech/facial-recognition-police/index.html [perma.cc/4T35-HC75].

[147] *See, e.g.*, Brief of *Amici Curiae* ACLU & ACLU of S. Cal. in Support of Defendant–Appellant Seeking Reversal at 41, People v. Johnson, No. F071640 (Cal. Ct. App. July 11, 2019),

genotyping programs has rapidly expanded in the last ten years.[148] Defendants across the country have requested access to those programs used against them; proprietors have routinely resisted disclosure, citing trade secrecy and commercial concerns.[149] Courts have consistently denied defendants' access requests.[150]

2. The Need to Treat Algorithmic and Human Sources Alike

That algorithmic information enjoys heightened protection as a trade secret is perplexing given that a defendant's due process rights remain the same regardless of the source of evidence against them—whether that source is digital or human. Developers argue that the disclosure of trade secrets to criminal defendants would jeopardize innovation in criminal justice technology.[151] However, while those innovation concerns have merit,[152] procedural mechanisms like protective orders can ensure that trade secrets remain shielded

2017 WL 10320829, at *41 [hereinafter *Johnson* ACLU Amicus Brief] (contending that the government's interest in secrecy of DNA testing software TrueAllele's source code is "derivative of a private company's intellectual-property interest in purported trade-secrets information").

[148] STRmix, one brand of probabilistic DNA genotyping program, was first introduced in 2012. By 2020, STRmix had been used in over 65,000 investigations in North America and provided evidence in more than 1,300 cases. *Arguing the Case for Probabilistic Genotyping*, ISHI (July 9, 2020), https://www.ishinews.com/arguing-the-case-for-probabilistic-genotyping [perma.cc/M3YY-SLLP]; *see also Survey Shows STRmix Has Been Used in 220,000 Cases Worldwide*, STRMIX (Nov. 19, 2020, 9:00 AM), https://www.strmix.com/news/survey-shows-strmix-has-been-used-in-220000-cases-worldwide [perma.cc/8P3N-99HY].

[149] Illustrative of proprietors' insistence on trade secrecy, Cybergenetics warns on its website that "los[ing] trade secret protection" would "abolish[] software that finds truth" and that defense "[l]awyers could destroy innovative companies and put them out of business." *The Government Wants to Take Away Your Right to Use Independent Forensic Software*, CYBERGENETICS (June 23, 2020), https://www.cybgen.com/information/newsroom/2020/jun/Government-wants-to-take-away-your-right-to-use-independent-forensic-software.shtml [perma.cc/T4VH-6N3R]; *see also, e.g.*, Commonwealth v. Robinson, No. CC 201307777 (Pa. Ct. Com. Pl. Feb. 4, 2016), http://online.wsj.com/public/resources/documents/Michael_Robinson_Opinion.pdf [perma.cc/M5BW-ZVZZ] (barring defendant access because of the "potential to cause great harm to Cybergenetics"); Brief of Appellant at 25, State v. Simmer, 935 N.W.2d 167 (Neb. 2019) (No. S-18-000500) (noting that Cybergenetics' founder resisted disclosing source code because it was a trade secret, though he had a change of heart at the "eleventh hour").

[150] Edward J. Imwinkelried, *Computer Source Code: A Source of the Growing Controversy over the Reliability of Automated Forensic Techniques*, 66 DEPAUL L. REV. 97, 101 (2016); Michelle Taylor, *Bill Questions Proprietary Algorithms Used in Probabilistic Genotyping Software*, FORENSIC MAG. (July 27, 2020), https://www.forensicmag.com/566619-Bill-Questions-Proprietary-Algorithms-Used-in-Probabilistic-Genotyping-Software [perma.cc/XKZ2-X77V] (stating that Cybergenetics "has yet to lose" when invoking trade secrecy in cases in which TrueAllele's findings were submitted as evidence).

[151] *See, e.g.*, Commonwealth v. Foley, 38 A.3d 882, 889 (Pa. Super. Ct. 2012) (expressing concern that "it would not be possible to market [the software] if it were available for free").

[152] *See* Wexler, *supra* note 62, at 1421–22.

from the public while still allowing access by the defendant.[153] In fact, protective orders are routinely granted to shield proprietary technology in civil proceedings, showing that such orders are effective.[154] And there are other ways to incentivize innovation of law enforcement algorithms: alternate forms of intellectual property, such as patents; exclusive government contracts contingent on transparency; tax incentives; and prize competitions.[155] Ultimately, the stakes for criminal defendants are far too great to prioritize intellectual property concerns at the expense of constitutional protections. As shown in the remainder of this Section, barring defendant access to algorithmic information on the basis of trade secret protections is in tension with the *Brady* doctrine. Differentiation between algorithmic and nonalgorithmic material is unwarranted in light of the principles and rationale underlying *Brady* and its progeny.

Defendants' inability to access favorable information[156] about law enforcement algorithms is detrimental to due process for the *same reasons* that defendants' inability to access that information about nonalgorithmic sources is detrimental. For example, courts have held that an eyewitness's inconsistent descriptions of the perpetrator must be disclosed under *Brady*.[157] Similarly, algorithms used in criminal proceedings produce inconsistent results, even when conducted by the same program.[158] Courts have also required disclosure of information that links someone other than the defendant to the crime, as

[153] Protection orders, while one solution to due-process concerns, do not alleviate the tension between trade secret protections and the First Amendment or the right to access criminal trials. Those constitutional tensions, however, are not within the scope of this Note.

[154] Fed. Open Mkt. Comm. of the Fed. Rsrv. Sys. v. Merrill, 443 U.S. 340, 362 n.24 (1979) ("[O]rders forbidding any disclosure of trade secrets or confidential commercial information are rare [in the civil context]. More commonly, the trial court will enter a protective order restricting disclosure to counsel."). However, *overly* protective orders that essentially render defense access to the algorithm meaningless raise the same *Brady* concerns; courts should thus be cautious in crafting protective orders. *See* Lydia Pallas Loren & Andy Johnson-Laird, *Computer Software-Related Litigation: Discovery and the Overly-Protective Order*, 6 FED. CTS. L. REV. 75, 115–23 (2012) (criticizing protective orders with proprietor-imposed conditions like "only handwritten notes" or no "compiling the source code" for rendering any review ineffective and extremely burdensome).

[155] Natalie Ram, *Innovating Criminal Justice*, 112 NW. U. L. REV. 659, 714–24 (2018); Wexler, *supra* note 62, at 1423.

[156] Information favorable to the defendant includes both exculpatory and impeachment evidence. United States v. Bagley, 473 U.S. 667, 676 (1985) (citing Giglio v. United States, 405 U.S. 150, 154–55 (1972)).

[157] Kyles v. Whitley, 514 U.S. 419, 441–44, 45 (1995) (finding a *Brady* violation because prosecution failed to disclose multiple inconsistent statements by key witness); *see also* Mackabee v. United States, 29 A.3d 952, 956–59 (D.C. 2011) (acknowledging that inconsistent descriptions were exculpatory).

[158] *Johnson* ACLU Amicus Brief, *supra* note 147, at 14 (stating that DNA genotyping system TrueAllele gave four significantly different likelihood ratios for one defendant).

when a witness identifies different suspects.[159] Like in Willie Lynch's case, facial recognition programs can also produce multiple suspects other than the defendant.[160]

Courts also emphasize that the prosecution must disclose any information relating to potential witness bias pursuant to *Brady*. This includes whether the witness received any benefits (such as monetary or sentence-reduction benefits)[161] or whether the witness has shown animosity towards the defendant's race or other characteristics.[162] Likewise, the proprietors who contract algorithmic systems to law enforcement agencies have financial incentives to meet law enforcement expectations that the tools they pay for will help maximize the number of successful prosecutions. Thus, proprietor incentives to design overbroad tools (or to ignore errors that create overbreadth)[163] pose the same risk to algorithms' credibility that human witnesses' incentives pose. Law enforcement algorithms have also been shown to produce racially biased and gendered results.[164] It is important for defendants to understand how eyewitness identifications were made because unconscious racial and gender bias may have influenced eyewitnesses' recollections, and police officers' own racial, gender, and confirmation biases may have led them to overly rely on biased eyewitnesses' leads. The same is true for law enforcement algorithms.

These parallels show that algorithmic information has the same underlying flaws as human witnesses or statements that raise due process concerns and must likewise be subject to *Brady*. As this Section has shown, analogizing algorithmic systems to human witnesses—particularly in the *Brady* context—is an apt conceptual framework. Indeed, practitioners and scholars have compared algorithmic systems to their human counterparts in a variety of contexts. One scholar, likening algorithmic systems' outputs to "machine testimony," argues that defendants should be able to cross-examine machine witnesses under the Confrontation Clause.[165]

[159] *E.g.*, Jamison v. Collins, 291 F.3d 380, 389, 391 (6th Cir. 2002) (finding a *Brady* violation because prosecution failed to disclose "positive identification of different suspects by an eyewitness to the crime").

[160] *See supra* notes 69–78 and accompanying text.

[161] Banks v. Dretke, 540 U.S. 668, 698, 702–03 (2004) (finding a *Brady* violation when prosecution failed to disclose that the witness was a paid informant); Giglio v. United States, 405 U.S. 150, 154–55 (1972) (finding a *Brady* violation when prosecution failed to disclose nonprosecution agreement with witness).

[162] *See, e.g.*, State v. Williams, 956 A.2d 375, 379–80 (N.J. Super. Ct. App. Div. 2008).

[163] Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 398–400 (2015) (arguing that surveillance technology companies have little incentive to fix errors in their programs); Jeanna Neefe Matthews et al., *When Trusted Black Boxes Don't Agree: Incentivizing Iterative Improvement and Accountability in Critical Software Systems*, 2020 PROC. AAAI/ACM CONF. ON AI ETHICS & SOC'Y 102 (describing how proprietors might "avoid costly debugging" by using intellectual property claims to keep knowledge about errors unknown); Stephanie J. Lacambra, Jeanna Matthews & Kit Walsh, *Opening the Black Box: Defendants' Rights to Confront Forensic Software*, CHAMPION, May 2018, at 28, 28, 38.

[164] *See supra* text accompanying notes 35–36.

[165] Roth, *supra* note 3, at 2039–48.

If courts allow prosecutors to invoke trade secret protections for law enforcement algorithms in criminal proceedings, the constitutional safeguards promised by *Brady* will be undermined. This *Brady* carveout could incentivize law enforcement and prosecutors to increasingly exploit algorithmic tools to circumvent the duty to investigate and disclose favorable material. Allowing such leeway will not only diminish defendants' due process protections but also cause expressive harm by signaling that the innovation incentives of trade secret protections outweigh defendants' constitutional rights.[166] The choice to protect a proprietor's intellectual property right at the expense of a defendant's due process right conveys to defendants and the broader public that their government values commercial interests over the accused's interest in a full and fair trial.[167] That message of inferiority, in addition to inflicting psychological trauma on the specific defendant,[168] in and of itself creates expressive harm by indicating disregard for defendants and by forcing them into a disvalued relationship with their government.[169]

B. *Additional Forms of Resistance to* Brady *Disclosure of Algorithmic Systems*

Despite the similarities between human and algorithmic witnesses, the latter have proven particularly resistant to *Brady* disclosure. In addition to the trade secret privilege discussed above, resistance generally comes in two other forms: (1) that the algorithm is not "in possession" of the prosecutor and (2) that the algorithm is not "material."[170] While resistance through trade secrets is the primary focus of this Note, these additional two challenges are worth discussing here because they are often raised in conjunction with or as alternatives to the trade secret privilege.[171] As a result, courts sometimes are not clear whether or to what extent their rulings are based on trade secret grounds

[166] Expressive harm, while difficult to capture in one definition, *id.* at 494, generally exists where a person is "treated according to principles that express negative or inappropriate attitudes toward her." *See* Elizabeth S. Anderson & Richard H. Pildes, *Expressive Theories of Law: A General Restatement*, 148 U. PA. L. REV. 1503, 1528 (2000).

[167] *See* Anderson & Pildes, *supra* note 166, at 1542–44 (explaining how discriminatory laws inflict expressive harm by branding the discriminated individuals as inferior and that such "legal communications of status inferiority constitute their targets as second-class citizens"); *see also* Craig Konnoth, *An Expressive Theory of Privacy Intrusions*, 102 IOWA L. REV. 1533, 1536 (2017) (showing how state privacy intrusions, i.e., departures from the baseline privacy protections afforded to individuals, signal the government's disrespect to the harmed and signals to the public that the harmed "lacks social standing and regard relative to other groups and institutions in society").

[168] *See* Alan Strudler, *The Power of Expressive Theories of Law*, 60 MD. L. REV. 492, 492–93 (2001) (describing the difference between "expressive harm" and "consequentialist harm" like psychological trauma).

[169] *See* Anderson & Pildes, *supra* note 166, at 1527–29.

[170] *See* People v. Superior Ct., 239 Cal. Rptr. 3d 71, 77 (Ct. App. 2018).

[171] *See id.*

or on more traditional *Brady* grounds.[172] This issue is exacerbated by the relative newness of the trade secret privilege.[173]

1. Prosecutor's Knowledge or Possession

Prosecutors may argue that an algorithm is not *Brady* material because it is not in the prosecutor's "know[ledge]" or "possession,"[174] but rather possessed by a third-party proprietor.[175] However, this element of *Brady* is construed permissively—constructive knowledge or possession is sufficient.[176] Information is constructively within the prosecutor's knowledge or possession if the "prosecution team," which includes "others acting on the government's behalf,"[177] knows or possesses it.[178] In other words, even if the prosecutor does not actually know or possess the exculpatory information, knowledge or possession is imputed to the prosecutor if any entity assisting them does know or possess it.[179]

Courts have imputed information known or possessed by law enforcement witnesses and investigators,[180] crime labs,[181] crime lab technicians,[182] nurse examiners,[183] and expert witnesses[184] to prosecutors. While the law is quite unsettled as to the scope of the prosecution team,[185] courts largely agree

[172] Wexler, *supra* note 62, at 1393–94 (tracing the "wave" of criminal cases in the mid-2000s in which defendants sought source code for breath test devices as well as courts' rationales for denying defense access, including that the code was not in the prosecutor's "possession" or that the code was not "relevant or material"); *id.* at 1360–61 (noting that though some courts have adopted an explicit trade secret privilege, others have instead "more loosely" incorporated trade secrecy as a consideration when evaluating defendants' requests for access).

[173] *Id.* at 1395 (citing People v. Superior Ct. (*Chubbs*), No. B258569, 2015 WL 139069, at *6, *9 (Cal. Ct. App. Jan. 9, 2015)) (stating that the first explicit application of a trade secret evidentiary privilege in a criminal case by any appeals court in the country was likely in 2015).

[174] *See* Strickler v. Greene, 527 U.S. 263, 263 (1999).

[175] *See Superior Ct.*, 239 Cal. Rptr. 3d. at 76.

[176] *See, e.g.*, United States v. Linder, No. 12 CR 22, 2013 WL 812382, at *33 (N.D. Ill. Mar. 5, 2013) (noting that the prosecutor's constructive knowledge or possession has been "broadly construed").

[177] Kyles v. Whitley, 514 U.S. 419, 437 (1995).

[178] Avila v. Quarterman, 560 F.3d 299, 308 (5th Cir. 2009).

[179] *In re* Brown, 952 P.2d 715, 720 (Cal. 1998) ("[T]hose assisting the government's case are . . . its agents. By necessary implication, the duty is nondelegable at least to the extent the prosecution remains responsible for any lapse in compliance." (citations omitted)).

[180] Youngblood v. West Virginia, 547 U.S. 867, 869–70 (2006); *Kyles*, 514 U.S. at 438.

[181] Bracamontes v. Superior Ct., 255 Cal. Rptr. 3d 53, 64 (Ct. App. 2019).

[182] *Brown*, 952 P.2d at 719.

[183] McCormick v. Parker, 821 F.3d 1240, 1246–48 (10th Cir. 2016); People v. Uribe, 76 Cal. Rptr. 3d 829, 846–47 (Ct. App. 2008).

[184] State v. Farris, 656 S.E.2d 121, 126 (W. Va. 2007); *see also Bracamontes*, 255 Cal. Rptr. 3d at 63 (discussing *Farris*).

[185] *See* United States v. Rosenschein, No. 16-4571, 2019 WL 2298810, at *5 (D.N.M. May 30, 2019) ("Unfortunately, there are few cases in which the Tenth Circuit has analyzed whether

that whether a witness or source "constitutes a state actor for purposes of *Brady*" requires an inquiry into "what the person *did*, not who the person is."[186] Thus, even if the entity is privately owned or employed, the function served by the entity remains the primary focus.[187]

For example, in *Bracamontes v. Superior Court*, a California state court held that two private forensic labs were part of the prosecution team for *Brady* purposes because the lab had "assisted in the government's investigation" by conducting DNA testing "in an effort to identify or exclude suspects."[188] The court emphasized that the lab received monetary payment from the government for its services.[189] Further, the court expressly disagreed with the prosecutor's attempt to distinguish between private and government-run crime labs. In "both cases," the work was "conducted on behalf of the government." The private labs thus bore "the same relationship to the prosecution" as government labs, making it "reasonable to impute the private party's knowledge to the prosecution."[190] Similarly, in *State v. Farris*, the West Virginia Supreme Court held that a private, out-of-state forensic psychologist was part of the prosecution team because the psychologist had conducted her examinations "at the request" of the prosecutor's investigation team.[191] Thus, the knowledge she obtained was imputed to the prosecutors.[192]

Algorithmic systems should likewise be evaluated based on what they *do*, not who their proprietors are.[193] If the algorithmic system directly assists in the investigation of a specific case, it is, like its human counterparts, "acting on the government's behalf." For example, an algorithmic system that examines DNA evidence "in an effort to identify or exclude suspects"[194] is part of the prosecution team even if the system is privately owned, just like the lab in

a person or entity is part of the prosecution team. . . . Outside the Tenth Circuit, there are few cases that have set forth a framework for analyzing who is part of the prosecution team.").

[186] *See, e.g.*, United States v. Stewart, 433 F.3d 273, 298 (2d Cir. 2006); State v. Mullen, 259 P.3d 158, 169 (Wash. 2011) (en banc) (citing Avila v. Quarterman, 560 F.3d 299, 308 (5th Cir. 2009)).

[187] *Bracamontes*, 255 Cal. Rptr. 3d at 64 (private crime labs); *McCormick*, 821 F.3d at 1246–48 (nurse examiner at a privately owned hospital); *Uribe*, 76 Cal. Rptr. 3d at 846–47 (same).

[188] *Bracamontes*, 255 Cal. Rptr. 3d at 64.

[189] *Id.*

[190] *Id.* at 64–65.

[191] State v. Farris, 656 S.E.2d 121, 126 (W. Va. 2007); *see also Bracamontes*, 255 Cal. Rptr. 3d at 63 (discussing *Farris*).

[192] *Farris*, 656 S.E.2d at 126.

[193] This analogy is further bolstered by the fact that some proprietary algorithms are developed and owned by the government itself. *E.g.*, Lauren Kirchner, *Federal Judge Unseals New York Crime Lab's Software for Analyzing DNA Evidence* (Oct. 20, 2017, 8:00 AM), https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence [perma.cc/Q4CX-CM6J] (describing New York City's discontinued probabilistic DNA genotyping tool).

[194] *Bracamontes*, 255 Cal. Rptr. 3d at 64.

Bracamontes.[195] A predictive system used to determine the scope of a criminal conspiracy that examines a party "at the request" of investigators and provides an "expert opinion," as the forensic psychologist did in *Farris*, is part of the prosecution team.[196] A facial recognition system that searches and identifies a primary suspect is part of the prosecution team because it not only assists but "effectively commence[s] the prosecution of th[e] case."[197] On the other hand, systems that are not directly "involved in the investigation of the case"[198] or are used merely at trial for "perceptual content,"[199] as with content used to prove a physical fact rather than the truth of the substance contained within,[200] may be less likely to constitute part of the prosecution team. But law enforcement algorithms deployed to assist in a specific criminal investigation should largely be considered as "acting on the government's behalf." Ultimately, a "case-by-case analysis" is required, algorithmic source or not.[201]

Like the forensic psychologist in *Farris* and the crime labs in *Bracamontes*, both of which were private entities, that an algorithmic system is owned by a private company should not obviate the necessary inquiry into the algorithm's role in the investigation. This extension makes sense for two related reasons. First, the underlying question of the "knowledge or possession" requirement is "whether the [g]overnment should be held responsible for the actions" of the entity.[202] When the government has affirmatively "instructed" or "contracted" the entity to conduct an investigative task, it is reasonable that the government be held responsible, at least as to the scope of its request.[203] Sec-

[195] *Cf.* People v. Wakefield, 107 N.Y.S.3d 487, 496–97 (App. Div. 2019) ("[A]lthough [DNA tool proprietor] Cybergenetics is independent from law enforcement, at the time the [DNA] report was generated, Cybergenetics was 'acting in the role of assisting the police and prosecutors in developing evidence for use at trial.' " (quoting People v. Rodriguez, 59 N.Y.S.3d 337, 345 (App. Div. 2017))).

[196] *Farris*, 656 S.E.2d at 126.

[197] United States v. Rosenschein, No. 16-4571, 2019 WL 2298810, at *6–7 (D.N.M. May 30, 2019) (holding that a government agency, even if it merely "forwarded [the defendant's location] to law enforcement," was still part of the prosecution team because it was "involved in the investigation of the case[] and has provided information to the government in aid of the prosecution" (emphasis omitted)).

[198] *Id.* at *7 (emphasis omitted).

[199] Roth, *supra* note 3, at 2005 (describing how FBI malware outputs would be probative not for their "communicable content" but for their "perceptual content" because they would be "offered not for their truth but to show that the computers then sent information back to the FBI").

[200] One scholar's example is that of a machine and its printout: the printout's "perceptual content" is that the machine and its ink toner were functioning at the time of printing. In contrast, the printout's "communicable content" is the substance of the printout, the machine's output or prediction used to prove the truth of a claim. Roth, *supra* note 3, at 2005.

[201] *See* Avila v. Quarterman, 560 F.3d 299, 308 (5th Cir. 2009).

[202] United States v. Meregildo, 920 F. Supp. 2d 434, 445 (S.D.N.Y. 2013); *see also* Bracamontes v. Superior Ct., 255 Cal. Rptr. 3d 53, 65 (Ct. App. 2019).

[203] *Meregildo*, 920 F. Supp. 2d at 445; *Bracamontes*, 255 Cal. Rptr. 3d at 64.

ond, a permissive "knowledge or possession" requirement ensures that prosecutors do not have a perverse incentive to shield themselves from *Brady* material.[204] Otherwise, *Brady* protections "might be nullified simply by keeping the prosecutor ignorant of information adverse to the government's case."[205] Likewise, *Brady* protections would be rendered toothless if prosecutors could avoid *Brady* obligations by outsourcing investigative tasks to privately owned algorithms. Indeed, many scholars have lamented this as a crucial problem of privatizing state functions—a problem that is growing.[206] Opaque privatization risks "corporate capture" and the unaccountable exercise of public power.[207] Thus, when the government decides to contract with the proprietor of a law enforcement algorithm for use in a public, investigatory function, the algorithm should be considered within the knowledge or possession of the prosecutor.

2. Material Either to Guilt or to Punishment

The materiality requirement—or its manipulation—may pose another hurdle to defendants' access to algorithmic information under *Brady*. Prosecutors are only obliged to disclose evidence "material either to guilt or to punishment" to the defendant.[208] Materiality thus serves two purposes. Before trial, it is the threshold that instructs prosecutors on whether evidence must be disclosed (material) or need not be disclosed (not material).[209] After trial, it imposes on the defendant a requirement to prove harm, that is, to show that there was a reasonable probability that the withheld evidence would have changed the outcome of the trial had it been disclosed.[210] Thus, "materiality" may be defined differently before and after trial, which may affect the defendant's ability to access algorithmic information under *Brady*. While the post-trial definition is firmly established, the pretrial standard is not.

After trial, the standard for materiality imposes a prejudice requirement—the disclosure must have created a "reasonable probability" of a different verdict.[211] Appellate judges should assess the trial record as a whole,[212] including trial transcripts, to decide whether the disclosure would have

[204] United States v. Brooks, 966 F.2d 1500, 1502 (D.C. Cir. 1992).

[205] BENNETT L. GERSHMAN, PROSECUTORIAL MISCONDUCT § 5:11 (2d ed. 2020).

[206] *See, e.g.*, Katyal, *supra* note 18, at 1242–46.

[207] Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 109 (2018).

[208] Brady v. Maryland, 373 U.S. 83, 87 (1963); *see also* Janet C. Hoeffel & Stephen I. Singer, *Activating a* Brady *Pretrial Duty to Disclose: From the Mouths of Supreme Court Justices to Practice*, 38 N.Y.U. REV. L. & SOC. CHANGE 467, 467–68 (2014).

[209] *Id.* at 470.

[210] *Id.*

[211] United States v. Bagley, 473 U.S. 667, 682 (1985); *see also* Hoeffel & Singer, *supra* note 208, at 470.

[212] Riley E. Clafton, *A Material Change to* Brady*: Rethinking* Brady v. Maryland*, Materiality, and Criminal Discovery*, 110 J. CRIM. L. & CRIMINOLOGY 307, 347–48 (2020).

changed the outcome.[213] However, appellate courts are hesitant to provide the extraordinary post-trial remedy of overturning convictions based on a *Brady* challenge.[214]

The pretrial standard, in contrast to the established post-trial standard, is contested.[215] The Supreme Court has suggested in dicta that the pretrial standard is the same as the post-trial one.[216] Prosecutors, erroneously citing that dicta as though it were binding precedent, may assert that they do not have a pretrial or at-trial duty to disclose favorable evidence unless they determine that there is a "reasonable probability" the evidence would change the outcome of the trial.[217] However, this lack of differentiation between pretrial and post-trial standards has been widely critiqued.[218] Scholars lament that such a pretrial standard is "literally impossible" to implement because "[f]rom the pretrial perspective, it is absurd to ask a prosecutor to determine anything about the *outcome* of a trial that has not yet occurred."[219] Drawing on the many unknowns of the future trial, prosecutors can "easily craft" some argument that disclosure of favorable information is unlikely to influence the trial outcome.[220] This is particularly true with opaque and complex algorithms. Given the unworkability of the standard, many courts have waived the materiality threshold, requiring the government to disclose *all* favorable information in its possession.[221] This is the prudent approach.[222] Unfortunately, some courts continue to apply the prejudice standard before trial, which allows prosecutors to "hid[e] behind the cloak of materiality" to shirk their *Brady* disclosure obligations at trial.[223] It would be quite difficult, then, for a

[213] Hoeffel & Singer, *supra* note 208, at 474.

[214] *E.g.*, Jessica Brand, *The Epidemic of* Brady *Violations: Explained*, APPEAL (Apr. 25, 2018), https://theappeal.org/the-epidemic-of-brady-violations-explained-94a38ad3c800 [perma.cc/JH6B-NXBR].

[215] Hoeffel & Singer, *supra* note 208, at 470–71 (arguing that the *Bagley* standard for materiality was "strictly concerned with determining the appellate standard for reversal," not pretrial or at-trial disclosures).

[216] *See, e.g.*, Kyles v. Whitley, 514 U.S. 419, 437 (1995); Hoeffel & Singer, *supra* note 208, at 472.

[217] Hoeffel & Singer, *supra* note 208, at 469 (asserting that applying the appellate prejudice standard *pretrial* "turns a due process right of the accused meant to ensure a fair trial into an entitlement of the prosecution to withhold favorable evidence").

[218] *Id.* at 485 ("In sum, at least five current members of the Supreme Court, several federal district court judges, and the ethical rules of conduct all recognize the absurdity of applying *Bagley*'s post-trial prejudice standard to a prosecutor's pretrial disclosure obligations . . . .").

[219] *Id.* at 474.

[220] *Id.* at 477.

[221] Cynthia E. Jones, *Here Comes the Judge: A Model for Judicial Oversight and Regulation of the* Brady *Disclosure Duty*, 46 HOFSTRA L. REV. 87, 101 (2017).

[222] *See* Hoeffel & Singer, *supra* note 208, at 473; Christopher Deal, Note, Brady *Materiality Before Trial: The Scope of the Duty to Disclose and the Right to a Trial by Jury*, 82 N.Y.U. L. REV. 1780, 1801–04 (2007).

[223] Hoeffel & Singer, *supra* note 208, at 473; *see, e.g.*, Lynch v. State, 260 So. 3d 1166, 1169–70 (Fla. Dist. Ct. App. 2018); Boyd v. United States, 908 A.2d 39, 59 (D.C. 2006).

defendant to overcome such a high, prosecutor-defined pretrial standard to obtain algorithmic evidence in time for trial. However, given the broad criticism of a pretrial prejudice requirement and the courts' warning that "arguable cases" should err on the side of disclosure,[224] algorithmic information should rarely be excluded before or at trial on the basis of a prosecutor-crafted assessment of materiality.[225]

III. The Missing Algorithm Instruction: An At-Trial Safeguard

As shown in Part II, law enforcement algorithms are akin to human witnesses in that they perform similar functions in criminal investigations and proceedings and raise similar issues related to credibility, reliability, and bias. This analogy to human witnesses is not entirely novel; it has been raised by practitioners and scholars[226] and was acknowledged as "creative" by at least one court.[227] This Part extends the analogy to justify a possible solution for situations in which the prosecutor or proprietor invokes a trade secret privilege despite a defendant's request for disclosure of the algorithmic information.

Extending the analogy of algorithm as human witness, this Note proposes that courts adapt the "missing witness" evidentiary rule[228] to "missing algorithms." This adapted rule would deploy a jury instruction for missing algorithmic evidence to remedy conflicts between *Brady*'s constitutional mandate and trade secrecy. This remedy provides a due process safeguard at trial without violating trade secrecy and without necessitating a solution as extraordinary as excluding algorithmic evidence altogether[229] or overturning[230] a conviction on appeal.

[224] *Boyd*, 908 A.2d at 61; *see also* Cone v. Bell, 556 U.S. 449, 470 n.15 (2009) (observing that "the prudent prosecutor will . . . resolv[e] doubtful questions in favor of disclosure"); Kyles v. Whitley, 514 U.S. 419, 439–40 (1995) (same).

[225] *See* Hoeffel & Singer, *supra* note 208, at 473.

[226] *E.g.*, People v. Superior Ct., 239 Cal. Rptr. 3d 71, 81 (Ct. App. 2018) (discussing defendant's analogy of DNA analysis tool to human lab analyst and expert witness); Roth, *supra* note 3, at 1972 (analogizing machine sources to human witnesses for Sixth Amendment right-to-confrontation purposes).

[227] *Superior Ct.*, 239 Cal. Rptr. 3d at 81.

[228] The missing witness rule was developed by the U.S. Supreme Court in *Graves v. United States*, 150 U.S. 118 (1893), well before the Federal Rules of Evidence and the Federal Rules of Civil Procedure were enacted. Since *Graves*, both federal and state courts have adopted variations of the basic *Graves* rule in both civil and criminal contexts. While the missing witness rule is not uniform from court to court, the rule is "alive and well." Michelle M. Rutherford, *Avoiding Application of the Missing-Witness Rule*, A.B.A. (Sept. 16, 2013), https://www.americanbar.org/groups/litigation/committees/commercial-business/articles/2013/avoiding-application-of-the-missing-witness-rule [perma.cc/H28Q-GNHX].

[229] *See Johnson* EFF Amicus Brief, *supra* note 57, at 16.

[230] *See* Kyles v. Whitley, 514 U.S. 419, 430–31 (1995).

A. *The Missing Witness Instruction*

The "missing witness" rule refers to the permissible inference a jury may draw from the absence of a potential witness who might have knowledgeable facts at issue in the case.[231] Take, for example, a defendant who is on trial for a robbery of a store. The prosecutor calls one eyewitness, the store manager, to testify before the jury. However, there were *two* eyewitnesses on the scene that saw the robbery occur—the store owner also witnessed the incident. The store owner, hostile to the robber, would be expected to testify favorably for the prosecution. But the prosecutor declines to call the store owner to the stand. The missing witness rule would allow the jury to infer that the prosecution refused to call the store owner because the owner's testimony would have been unfavorable (perhaps, for example, the store owner's description of the robber was inconsistent with the store manager's).[232]

The missing witness rule can be traced to the Supreme Court case *Graves v. United States*,[233] and both the defense and prosecution are allowed to invoke it in criminal trials.[234] There are two key prerequisites for a missing witness instruction: (1) the witness must have been "peculiarly" available to the opposing party (the witness is available to the prosecution but not reasonably accessible to the defense through other channels), and (2) the witness would have elucidated "noncumulative" information (the information is not already in the defense's possession).[235] One of the rationales[236] underlying this rule is spoliation, the suppression of evidence by a party.[237] The rule is intended to deter concealment of evidence and to encourage disclosure of all relevant evidence.[238] The reasoning is that when a party fails to produce a witness that knows facts about the case and the witness was "peculiarly available" to that

[231] 1A KEVIN F. O'MALLEY, JAY E. GRENIG & WILLIAM C. LEE, FEDERAL JURY PRACTICE AND INSTRUCTIONS § 14.15 (6th ed. 2008).

[232] The facts of this example are a simplified version of what occurred in *People v. Hall*, 960 N.E.2d 399 (N.Y. 2011). *See also* People v. Kitching, 583 N.E.2d 944, 946–47 (N.Y. 1991) (granting defendant's request for a missing witness instruction where prosecution called one officer at trial but not the second officer when both officers witnessed the drug transaction at issue in the case). In *Hall*, the appeals court agreed that the trial court had erred in refusing to grant the defendant a missing witness instruction, but ultimately held that the error did not entitle relief because the defendant had failed to preserve the issue. *Hall*, 960 N.E.2d at 402.

[233] 150 U.S. 118 (1893).

[234] *See* O'MALLEY ET AL., *supra* note 231, at 122–23.

[235] *Id.* at 121.

[236] Two other rationales include the "voucher" doctrine and "best evidence" doctrine. The voucher doctrine is a common law concept that a party vouches for the credibility of the witnesses that it calls to the stand. *See* Walker v. State, 818 A.2d 1078, 1086 (Md. 2003). The best evidence doctrine instructs that "if it be found that there is any better evidence existing than is produced, the very not producing it is a presumption that it would have detected some falsehood that at present is concealed." 3 WILLIAM BLACKSTONE, COMMENTARIES *368.

[237] Robert H. Stier, Jr., *Revisiting the Missing Witness Inference—Quieting the Loud Voice from the Empty Chair*, 44 MD. L. REV. 137, 141 (1985).

[238] *Id.*

party but not the opposing party, the jury could "naturally" draw an adverse inference from that failure.[239] The instruction is permissive, not mandatory—juries are *permitted* to draw the inference but are not required to do so. If allowed by the court, the inference is typically included in the closing argument to the jury and addressed by a jury instruction.

B. *The Missing Algorithm Instruction*

Similarly, a "missing algorithm" jury instruction would only be granted when two prerequisites are met: (1) the algorithmic system is peculiarly available to the prosecution, and (2) the algorithmic system would elucidate noncumulative information.[240] In addition, because the instruction would only be a remedy for *Brady* material, the instruction would only be available for algorithmic information that is "favorable" under *Brady*.[241]

The missing algorithm instruction makes logical sense when trade secrecy is invoked to exclude an algorithm. In a criminal trial, the prosecution must prove each element of its case against the defendant beyond a reasonable doubt.[242] When law enforcement substantially relies on an algorithm in its investigation or when the prosecution introduces an algorithm's output at trial and examining the algorithm may reveal bias or unreliability or lack of credibility, *Brady* requires that the defendant be given access to that impeachment material to help build their defense and persuade the jury that reasonable doubt exists.[243] When *Brady* material is not disclosed, "irrespective of the good faith or bad faith of the prosecution," a *Brady* "suppression" occurs.[244] And "justice suffers" when such a suppression occurs—even when a third-party proprietor has commercial interests at stake.[245] Thus, as with missing witness instructions, a jury should be permitted to draw a reasonable adverse inference from that suppression.

The missing algorithm instruction is also reasonable because government entities wield significant market power. As the primary consumers of law enforcement technologies, government entities can choose which proprietors to work with and how to craft their contractual relationships to ensure greater transparency.[246] For example, a government could condition its purchase of an algorithmic system on access to all documentation relating to the reliability

[239] Graves v. United States, 150 U.S. 118, 126 (1893) (Brewer, J., dissenting).

[240] *See supra* text accompanying notes 17–22 for an overview of algorithmic systems' components.

[241] *See supra* notes 5–11 and accompanying text.

[242] *In re* Winship, 397 U.S. 358, 364 (1970).

[243] Boyd v. United States, 908 A.2d 39, 61 (D.C. 2006); *see supra* Part II.

[244] Brady v. Maryland, 373 U.S. 83, 87 (1963).

[245] *See id.*

[246] *See* Katyal, *supra* note 18, at 1262; Erik Bakke, Note, *Predictive Policing: The Argument for Public Transparency*, 74 N.Y.U. ANN. SURV. AM. L. 131, 132–33 (2018) (observing that predictive policing tools had been adopted by 38 percent of police departments as of 2018 and that a 70 percent adoption rate was expected within two to five years).

of the system. The government could also secure limited permission to disclose any *Brady* information contained therein to defendants under a protective order.[247] In fact, some governmental entities already appear to be considering adjusting their contractual requirements to enhance algorithmic transparency.[248] The availability of a missing algorithm instruction would incentivize more governmental entities to do so.

Allowing the jury to draw an adverse inference from *Brady* suppression when the government raises a valid trade secret privilege may appear harsh, particularly since the trade secret *holder* is a private proprietor who is not a party in the criminal case. For example, the private proprietor might resist disclosure even when the prosecutor wishes to disclose. However, as discussed in Part II, it is reasonable—and arguably necessary in many cases—to treat the algorithmic system as acting on behalf of the government.[249] A prosecutor, in their unique role as a representative of the government,[250] cannot instruct a crime lab to help in its investigation or at trial, then shield the crime lab from adversarial scrutiny.[251] Likewise, the prosecutor cannot have it both ways with algorithmic systems. The government should be thinking about its *Brady* duties when it uses an algorithmic system to assist directly in an investigation or trial, and it should only work with proprietors that will allow the government to disclose the information it is constitutionally obliged to share with the defense. If the government imprudently contracts with a proprietor that refuses to allow the required disclosures, the missing algorithm inference can remedy that due process failure at trial.

Further, any harshness is mitigated by the prosecutor and proprietor's viable alternative—disclosing the algorithm under a protective order. Protective orders are issued routinely for trade secrets in the civil context.[252] These orders even enable disclosure of a party's trade secret to its direct competitor.[253] Such routinely accepted safeguards in the civil context should likewise be sufficient to protect trade secrets in criminal trials.[254] In light of the availability of protective orders, one scholar has suggested getting rid of the trade secret privilege in the criminal context altogether.[255]

[247] *See* Brauneis & Goodman, *supra* note 207, at 109.

[248] Katyal, *supra* note 18, at 1262.

[249] *See supra* Section II.B.1.

[250] United States v. Bagley, 473 U.S. 667, 675 n.6 (1985) (quoting Berger v. United States, 295 U.S. 78, 88 (1935)).

[251] Bracamontes v. Superior Ct., 255 Cal. Rptr. 3d 53, 64 (Ct. App. 2019).

[252] *See supra* note 154 and accompanying text.

[253] *See* Dustin B. Benham, *Proportionality, Pretrial Confidentiality, and Discovery Sharing*, 71 WASH. & LEE L. REV. 2181, 2240–41 (2014).

[254] The use of protective orders may raise other constitutional concerns. For example, protective orders would not allow members of the public or press to access the algorithm, which may violate the public's First Amendment right to receive information and ideas and to engage in democratic discourse. Vera Eidelman, *The First Amendment Case for Public Access to Secret Algorithms Used in Criminal Trials*, 34 GA. ST. U. L. REV. 915, 934–35 (2018).

[255] Wexler, *supra* note 62, at 1403.

While removing the privilege from the criminal context altogether would promote transparency and accountability, trends suggest the use of trade secrets to prevent *Brady* disclosures is on the rise.[256] Proprietors are aggressively and increasingly raising the privilege or asking governments to sign nondisclosure agreements at the outset.[257] And courts appear to be increasingly sympathetic to trade secret arguments at each stage of a criminal case.[258] In light of this trend, a missing algorithm instruction would provide a much-needed due process backstop. While the remedy does not provide the immediate transparency that full disclosure in all cases would, it provides longer-term incentives for the government to choose transparent practices and tools. This, in turn, would incentivize proprietors to develop transparent solutions.[259]

Outside of protective orders, the remedies currently available to defendants are either to request complete exclusion of the algorithmic evidence at trial or dismissal of the charges[260] or to file a post-trial appeal seeking to overturn the conviction altogether. Neither is a satisfactory solution. The former risks providing the defendant with a windfall and punishing the prosecutor for raising a privilege.[261] Further, the former would rarely provide defendants relief given how difficult it is for defendants to exclude evidence at trial successfully.[262] Nor would the former provide any relief for defendants deprived of *Brady* evidence *not* introduced at trial (like a facial recognition tool that provided many other possible suspects). The latter may force the defendant to

[256] *See id.* at 1360 (first citing State v. Fair, No. 10-1-09274-5 SEA, slip op. at 3 n.1 (Wash. Super. Ct. Jan. 12, 2017), ECR No. 383; then citing State's Response to Def. Motion to Compel TrueAllele Source Code at 12–13, *Fair*, No. 10-1-09274-5 SEA, ECR No. 258; and then citing Letter Regarding Motion to Quash at 2, United States v. Johnson, No. 15-cr-00565 (S.D.N.Y. June 15, 2016)).

[257] *See* Katyal, *supra* note 18, at 1262 (explaining how the City of San Francisco has "rarely fought language in contracts with third-party vendors that recognized that the algorithms must be kept from the public"); Joh, *supra* note 95, at 23–26.

[258] For example, in *People v. Johnson*, the prosecution resisted disclosure of the TrueAllele probabilistic DNA genotyping tool by raising a trade secret privilege. People v. Johnson, No. F071640, 2019 WL 3025229, at *8 (Cal. Ct. App. July 11, 2019); *see also* People v. Superior Ct., 239 Cal. Rptr. 3d 71, 77 (Ct. App. 2018). This is the case not just in the *Brady* context but in a wide variety of cases. *See* Katyal, *supra* note 18, at 1240 (discussing scholarship tracking how "nondisclosure privileges have grown, leading to trends that tend to favor commercial interests over public ones").

[259] Katyal, *supra* note 18, at 1220.

[260] *See Johnson* EFF Amicus Brief, *supra* note 57, at 16.

[261] Peter J. Henning, *Prosecutorial Misconduct and Constitutional Remedies*, 77 WASH. U. L.Q. 713, 717 (1999); *see* Elizabeth Napier Dewar, Note, *A Fair Trial Remedy for* Brady *Violations*, 115 YALE L.J. 1450, 1467–68 (2006).

[262] To exclude evidence on the grounds that it would lead to unfair prejudice, a party must show that the evidence is "so inflammatory on its face" that it would divert the jury from material issues. United States v. Huyck, 849 F.3d 432, 440 (8th Cir. 2017); *see also* Jim Hilbert, *The Disappointing History of Science in the Courtroom:* Frye*,* Daubert*, and the Ongoing Crisis of "Junk Science" in Criminal Trials*, 71 OKLA. L. REV. 759, 762–63 (2019) (lamenting that courts' failure to exclude even "junk science" in criminal cases has "undoubtedly resulted in wrongful convictions").

spend years in prison while the appeal is pending[263] and requires the appellate court to conduct a difficult hindsight review of whether the admission of the evidence was prejudicial.[264]

The missing algorithm instruction provides a more balanced alternative to those "extreme" solutions.[265] It permits the jury, rather than requiring the judge, to balance the defendants' access to algorithms and proprietors' trade secrecy concerns. Allowing the jury to draw an inference in favor of the defendant is not a punitive measure against the prosecutor;[266] it is a due process safeguard, one that is appropriate given the prosecutor's ability to allow access under a protective order as an alternative.

A missing algorithm instruction might take the following form:

> In order for the defendant to receive a fair trial, the government is required to inform the defense of any information known to the government that casts doubt on the credibility of the government's own evidence. In this case, the government failed to turn over promptly information favorable to the defense, namely [algorithmic material], of which the defense learned only on [date], when [means of disclosure]. The government has declined to disclose this information because of trade secret (intellectual property) concerns. The government had the option to disclose the information under a protective order. Although this denial of access does not necessarily bear on the guilt or innocence of the defendant, you may, if you think it appropriate in light of all the evidence, take into account the possible harm to the defense caused by this denial when evaluating whether the government has proven the defendant's guilt beyond a reasonable doubt.[267]

This instruction clearly conveys the government's disclosure duty—and its breach of that duty—to the jury. But it also conveys the reason for that breach and asks the jury to consider any inferences in consideration of that fact. Additionally, the jury is instructed to consider "all the evidence." That evidence would include any validation studies for the algorithm the prosecutor may have produced at trial. Whether the jury would deem the validation studies sufficient would depend on whether the studies were independently conducted, the studies' methodology, and other indicia of their credibility.[268] The missing algorithm instruction would therefore encourage prosecutors to

[263] *See* Boyd v. United States, 908 A.2d 39, 62 (D.C. 2006); *see also* Deal, *supra* note 222, at 1783, 1783 n.26.

[264] Dan Simon, *A Third View of the Black Box: Cognitive Coherence in Legal Decision Making*, 71 U. CHI. L. REV. 511, 575–80 (2004).

[265] *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, 279 (2017).

[266] *But see* Jones, *supra* note 8, at 447–52 (proposing adverse-inference instructions for intentional *Brady* suppressions).

[267] This example instruction has been modeled on the adverse-inference instructions proposed by other scholars in nonalgorithmic *Brady* contexts, including Dewar, *supra* note 261, at 1457–60, and Jones, *supra* note 8, at 450–52.

[268] *See* Katyal, *supra* note 18, at 1245 (discussing breath-test-device proprietor's invocation of trade secrecy to block independent testing of the device).

submit those studies at the outset and reward governmental entities that contract with transparent and credible proprietors. Further, "all the evidence" means that an adverse inference would *not* be drawn when the prosecution has presented a strong case bolstered by other witnesses and evidence. In contrast, an adverse inference is more likely to be drawn when the algorithm provides the key or sole piece of evidence.[269]

The instruction would be requested by the defense in a motion before or at trial. The timing would largely depend on when the suppression came to light. If requested at trial, the defense would make its request outside of the jury's presence. Ultimately, the decision to grant this remedy would be within the trial court's discretion. The trial court could also give more specific instructions and limit the defendant's closing argument as to the scope of the adverse inference that can be drawn.

Admittedly, a missing algorithm instruction is far from a cure-all. One significant situation in which this remedy would not be curative is when prosecutors do not even disclose the use of law enforcement algorithms.[270] Unfortunately, this has happened in many cases in which a novel algorithm aided the investigation.[271] As a result, most defendants do not know that an algorithm was involved in their investigation unless that information is serendipitously discovered.[272] For example, Willie Lynch discovered that facial recognition technology was used to identify him only eight days before his trial.[273] Many defendants never find out even after they are convicted.[274] One striking example: in Pinella County, Florida, law enforcement used facial recognition technology for *fifteen* years without ever providing the public defender's office any indication of its use in *Brady* disclosures.[275] Fortunately, organizations are becoming increasingly vigilant about law enforcement uses of algorithmic tools.[276] And the availability of a missing-algorithm-instruction remedy may encourage more defense attorneys in pretrial discovery to learn whether an algorithm was used against their client.

Another shortcoming of this remedy is that defendants will still have to satisfy the *Brady* hurdles of "knowledge or possession" and "materiality." But as explained in Part II, the human-witness analogy—which highlights the common need for due process safeguards between algorithmic tools and human witnesses—helps show why law enforcement algorithms should in most cases clear these two hurdles. Defendants who can overcome these *Brady* prerequisites will be able to request the jury-instruction remedy at trial instead of

[269] *See, e.g.*, *Lynch* ACLU Amicus Brief, *supra* note 28, at 10 (noting that sole defense raised was misidentification).

[270] *See id.* at 1.

[271] *See supra* text accompanying note 124.

[272] *See* Jones, *supra* note 8, at 433 & n.81.

[273] *Lynch* ACLU Amicus Brief, *supra* note 28, at 1.

[274] *See supra* note 124.

[275] LAPERRUQUE, *supra* note 128.

[276] *See, e.g.*, RICHARDSON ET AL., *supra* note 143, at 17–18.

having to wait until an appeal. And courts are more likely to grant this less extreme remedy than to overturn a conviction entirely.[277]

Critics of this remedy may raise two additional concerns. First, critics may argue that the defense will be able to "create" reasonable doubt among jurors by overinflating how favorable or material the algorithmic information is.[278] However, "[d]isclosure law cannot be predicated on the assumption that juries are [so] irrational" that a missing algorithm instruction would induce them to arbitrarily or capriciously discount the prosecution's case.[279] And the risk of creating reasonable doubt can be mitigated by a more tailored jury instruction.[280]

Second, critics may argue that the traditional missing witness rule is disfavored in some jurisdictions and should be limited rather than extended. But courts' concerns over this rule usually involve adverse inferences drawn against the *defendant*—not the prosecutor.[281] Those concerns make sense given that defendants do not bear the burden of proof at trial and are not required to produce any evidence or any witnesses. Allowing the jury to draw an adverse inference against the defendant would risk shifting the burden of proof to the defendant. But law enforcement algorithms serve the prosecution team. The prosecutor bears the burden of convincing a jury that there is no reasonable doubt of guilt, and failing to produce the witness whose testimony was relied upon in the investigation or at trial may very well raise reasonable doubt. Therefore, the missing algorithm instruction would merely notify the jury that it should decide, in light of the other evidence presented, whether or not the prosecution team's decision to disallow access and prevent the defendant from testing the algorithm's credibility is significant enough to raise doubt.

CONCLUSION

As privately developed law enforcement algorithms proliferate, due process protections must keep pace. While algorithmic systems may be a cost-effective solution for efficient investigations and prosecutions, "[s]ociety wins not only when the guilty are convicted but when criminal trials are fair."[282] Yet trade secret evidentiary privileges are increasingly shielding algorithms from scrutiny. To ensure the continued fairness of the criminal justice system, a new due process safeguard is necessary. The missing algorithm instruction, an at-trial solution, may provide just that.

[277] *See* Dewar, *supra* note 261, at 1457.

[278] Hoeffel & Singer, *supra* note 208, at 480.

[279] Bruce A. Green, *Federal Criminal Discovery Reform: A Legislative Approach*, 64 MERCER L. REV. 639, 675 (2013).

[280] Hoeffel & Singer, *supra* note 208, at 480.

[281] O'MALLEY ET AL., *supra* note 231; *see also* Harris v. State, 182 A.3d 821, 825 (Md. 2018).

[282] Brady v. Maryland, 373 U.S. 83, 87 (1963).