PROCURING ALGORITHMIC TRANSPARENCY

Elizabeth A. Rowe and Nyja Prior

PROCURING ALGORITHMIC TRANSPARENCY

Elizabeth A. Rowe and Nyja Prior+*

INTRODUCTION

One evening in May 2020, sixty-four-year-old Michael Williams was returning home from an after-dinner trip to his neighborhood convenience store in Chicago's South Side.[1] He was flagged down by a twenty-five-year-old acquaintance, Safarian Herring, who asked for a ride.[2] Williams obliged, and Herring climbed into the front seat.[3] As Williams proceeded down South Stony Island Avenue toward an intersection, Herring was shot on the side of his head.[4] Williams told police that the shot was fired when a car pulled up beside him, the passenger fired into Williams' car, and Williams then ran a red light to escape.[5] All parties agree that after Herring was shot, Williams drove him directly to a hospital, where Herring would survive a few days before succumbing to his injuries.[6]

A few months later, Williams was charged with first-degree murder on the theory that it was Williams who shot Herring from inside the car that night.[7] Prosecutors did not have an eyewitness, a gun, or a motive.[8] Instead, they had ShotSpotter—an artificial intelligence ("AI") surveillance system that uses hidden microphone sensors to detect sounds.[9] The sounds are then processed through a secret algorithm that determines whether they are gunshots,

* Henry L. and Grace Doherty Charitable Foundation Professor of Law and Horace W. Goldsmith Research Professor of Law, University of Virginia School of Law.

+ Associate, Knobbe Martens Olson & Bear, LLP. We express our appreciation to Robert Brauneis, Christopher Crawford, John Duffy, Tait Graves, Michelle Jacobs, Sonia Katyal, Sharon Sandeen, Steven Schooner, Joshua Schwartz, Christopher Slobogin, and Rebecca Wexler for insights, comments, or conversations about the ideas expressed in earlier versions of this work, as well as to participants of workshops at the University of Virginia School of Law, the University of Washington School of Law, and the 2021 IP Scholars Conference. Thank you to Pete Love, Vieux Toure, and Kenneal Harrigan for excellent research assistance.

1. Garance Burke et al., *How AI-Powered Tech Landed Man in Jail with Scant Evidence*, ASSOCIATED PRESS (Mar. 5, 2022), https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220.

2. *Id.*

3. *Id.*

4. *Id.*

5. *Id.*

6. Todd Feathers, *Police Are Telling ShotSpotter to Alter Evidence from Gunshot-Detecting AI*, VICE (July 26, 2021, 8:00 AM), https://www.vice.com/en/article/qj8xbq/police-are-telling-shotspotter-to-alter-evidence-from-gunshot-detecting-ai.

7. Burke et al., *supra* note 1.

8. *Id.*

9. Feathers, *supra* note 6.

pinpoints their location, and alerts the police.[10] The government's theory against Williams was (1) that ShotSpotter proved the fatal shot was fired at a particular corner on South Stony Island Avenue, (2) that evidence from a security video camera demonstrated that Williams's car was at that location, and (3) that there was no passing car that could have fired the shot.[11]

However, there were three main weaknesses in the government's reliance on ShotSpotter to support its theory. First, ShotSpotter's algorithm initially characterized the sound as a firecracker (with 98% confidence), but a ShotSpotter analyst manually overrode the algorithm and "reclassified" the sound as a gunshot.[12] Second, the algorithm placed the shot location on Lake Shore Drive which is about a mile away from the South Stony Island Avenue location where prosecutors claim the murder occurred.[13] Once again, that location was manually changed months later in "post processing" by another ShotSpotter analyst, allegedly at the request of the Chicago police, to coordinates on South Stony Island Avenue where Williams's car was seen on the video camera.[14] Third, the government's theory required the shot to have been fired inside Williams's car, but according to ShotSpotter, its contract warns against relying on the algorithm to locate shots fired inside vehicles or buildings, a fact which it claims to have communicated to prosecutors.[15]

Williams's attorneys attacked those weaknesses in the evidence. They sought discovery on the government's communications with ShotSpotter. They also filed a motion to exclude the ShotSpotter evidence and obtain ShotSpotter's secret operating protocols.[16] Further, they challenged the after-the-fact manual changes by the analysts and sought their identities, arguing that "[t]hrough this human-involved method, the ShotSpotter output in this case was dramatically transformed from data that did not support criminal charges of any kind to data that now forms the centerpiece of the prosecution's murder case against Mr. Williams."[17] However, the company refused to identify the names of the employees who altered the algorithm.[18] Indeed, prosecutors chose to withdraw the ShotSpotter evidence rather than reply to the defense's motion

10. *See* Motion to Exclude ShotSpotter Evidence Pursuant to *Frye* and Rule 403 at 3–4, State v. Williams, No. 20CR0899601 (Ill. Cir. Ct. Apr. 22, 2021) [hereinafter Motion to Exclude ShotSpotter Evidence], https://regmedia.co.uk/2021/08/02/shotspotter_evidence_filing.pdf.

11. The surveillance camera did show another car running the red light next to Williams's car, but because the windows in that car appeared to be rolled up, prosecutors dismissed the idea that the shot could have been fired from that car. Burke et al., *supra* note 1.

12. *Id.*; Feathers, *supra* note 6.

13. Feathers, *supra* note 6.

14. *Id.*

15. Burke et al., *supra* note 1.

16. *See* Motion to Exclude ShotSpotter Evidence, *supra* note 10, at 1.

17. *See id.* at 30.

18. *See id.* at 2 n.3.

to suppress,[19] and the government eventually dismissed all charges.[20] The outcome for Williams was, at best, a mixed bag. From the standpoint of a criminal defendant's constitutional rights, perhaps in this instance Williams was "lucky" to not have the evidence used against him. Regrettably, however, he remained in jail for eleven months (twice infected with Covid-19 behind bars) until the case was finally dismissed.[21]

Multiple news investigations revealed that the company's analysts frequently alter alerts when requested by police departments.[22] ShotSpotter, used in over 100 cities in the U.S., claims its algorithms as trade secrets[23] and does not permit independent testing.[24] Prior to publication of the news stories about the Williams case, the MacArthur Justice Center at Northwestern Pritzker School of Law also investigated ShotSpotter.[25] It reported that the City of Chicago had entered into a $33 million, three-year contract with ShotSpotter.[26] Further, there were no studies on the program's reliability or on its accuracy in distinguishing gunshots from "firecrackers, backfiring cars, construction noises, helicopters, and other loud, impulsive sounds."[27] Analysis revealed that in about a two-year period, 89% of gunshot alerts were not gun-related.[28] During that same period, police were deployed 40,000 times (in mostly Black and Brown neighborhoods) in search of gunfire that did not exist.[29]

The ShotSpotter story typifies the symbiotic relationship between private sector sellers of technology and government purchasers of technology at every stage of the criminal justice system. Just as in the private marketplace, artificial intelligence tools ("AI") undoubtedly have the potential to improve government functions and efficiency. However, as ShotSpotter reveals, both

19. *See* Feathers, *supra* note 6.

20. Burke et al., *supra* note 1.

21. *Id.*

22. *E.g.*, Feathers, *supra* note 6.

23. *Agreement between the City of Fresno and ShotSpotter*, CITY OF FRESNO 3–4 (Mar. 26, 2015), https://www.fresno.gov/cityclerk/wp-content/uploads/sites/9/2016/10/SSTalsoShotSpotterSrvsandLicenseAgmtexp2018.pdf (expressly restricting the city of Fresno, CA from disclosing ShotSpotter's data due to trade secrecy); Matt Drange, *We're Spending Millions on This High-Tech System Designed To Reduce Gun Violence. Is it Making a Difference?*, FORBES (Nov. 17, 2016, 8:30 AM), https://www.forbes.com/sites/mattdrange/2016/11/17/shotspotter-struggles-to-prove-impact-as-silicon-valley-answer-to-gun-violence/?sh=6eddabbc31cb (detailing an interview with economics Professor Jennifer Doleac of the University of Virginia and her failed attempts to obtain ShotSpotter data due to claims of trade secrecy, even after she contacted ShotSpotter's CEO Ralph Clark directly and being informed that the data could only be obtained if she paid $50,000 for each city studied).

24. Feathers, *supra* note 6.

25. *See, e.g.*, Press Release, MacArthur Just. Ctr., ShotSpotter Generated over 40,000 Dead-End Police Deployments in Chicago in 21 Months, According to New Study (May 3, 2021), https://www.macarthurjustice.org/shotspotter-generated-over-40000-dead-end-police-deployments-in-chicago-in-21-months-according-to-new-study/.

26. *Id.*

27. *Id.*

28. *Id.*

29. The city's predictive policing technology also uses ShotSpotter data. *Id.*

law enforcement and taxpayers may gain little if the technology is unreliable or ultimately inadmissible for convictions because of secrecy.

Scholars[30] in both criminal law and intellectual property have thoughtfully examined several related factors at the intersection of intellectual property, criminal justice, algorithms, and transparency. They have written about what *should* be done to address the secrecy problem, proposing a range of potential approaches, *inter alia*, greater transparency, abolishing trade secret protection for algorithms in criminal justice, or banning algorithms absent full disclosure.[31] For instance, in his recent book, Christopher Slobogin notes that "[e]ven if it turns out that advanced machine-learning [risk assessment systems] are demonstrably more accurate than simpler versions . . . they should be banned from criminal proceedings, at least when they are 'inscrutable'; litigants, policymakers and decision-makers must be provided information about how they work."[32] Robert Brauneis and Ellen Goodman suggest that more meaningful transparency will be achieved if vendors are required "to create and deliver records that explain key policy decisions and validation efforts, without necessarily disclosing precise formulas or algorithms."[33] From the broader legislative standpoint, Tait Graves and Sonya Katyal call for greater transparency through suggested federal and state statutory reforms that may "mandate disclosure of certain data . . . or explicitly permit the sharing and disclosure of such data."[34] Finally, as an evidentiary matter, Rebecca Wexler makes the case that the trade secret privilege should have no place in criminal proceedings because "trade secret holders should wield no special power to block criminal defendants' access to evidence altogether."[35]

In this Article, we expand upon that body of work by offering a realistic and practical approach as to *how* to achieve transparency given existing trade secret law and the relatively strong property rights that private vendors have under that law. In short, we point to a specific legal tool from the already existing arsenal of private law in an effort to address some of the larger public law concerns. While the prior literature has focused on constitutional challenges to algorithmic tools, including due process challenges, and on *ex post* judicial

30. *See, e.g.*, Charles Tait Graves & Sonia K. Katyal, *From Trade Secrecy to Seclusion*, 109 GEO. L.J. 1337, 1370–76 (2021); CHRISTOPHER SLOBOGIN, JUST ALGORITHMS: USING SCIENCE TO REDUCE INCARCERATION AND INFORM A JURISPRUDENCE OF RISK (2021); Cary Coglianese & Lavi M. Ben Dor, *AI in Adjudication and Administration*, 86 BROOK. L. REV. 791 (2021); Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183 (2019); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018); Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103 (2018); Natalie Ram, *Innovating Criminal Justice*, 112 NW. U. L. REV. 659 (2018); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 21 (2014).

31. *See* sources cited *supra* note 30.

32. SLOBOGIN, *supra* note 30, at 111 (footnote omitted).

33. Brauneis & Goodman, *supra* note 30, at 176.

34. Graves & Katyal, *supra* note 30, at 1420.

35. Wexler, *supra* note 30, at 1353.

remedies in individual litigation long after the government has purchased software from a developer, this Article pivots to a novel viewpoint. We go back to the basics of the initial transaction.

Significantly, we reorient the analysis to an earlier time period—the point at which the government agency initially decides to purchase the software. Looking back to that earlier period, we point to a different field of law entirely—the law on government procurement and contracting—and suggest that many of the relevant concerns regarding excessive trade secrecy and essential government transparency could be resolved through negotiations in the shadow of that body of law. Contract law is thus central to our proposal. Contracts can balance the competing interests of secrecy and disclosure, and contractual negotiations between government agencies and private vendors are the means for achieving such balance on a transaction-by-transaction basis.

Using the criminal justice system as an illustration, this Article observes that there is a perceived theoretical incongruity between the underlying purpose of trade secret law in a private competitive sphere and the values of openness that are fundamental to public governmental functions. Yet, trade secret law is not designed to foster absolute secrecy. To the contrary, trade secret law is built to solve Arrow's information paradox by facilitating the sharing of information in a manner that does not result in loss of the value of the information to its owner.[36] We therefore posit that the existing theoretical framework of trade secret law reveals both the limited nature of the problem (mere initial secrecy) and the evident solution (contractually authorized disclosures).

The Article thus aims to build on the developing literature in this area by offering a novel transaction-by-transaction, procurement-based proposal that ultimately integrates and carefully weaves together criminal law and procedure, constitutional law, contract law, intellectual property law, and procurement law. It attempts to offer a solution that is immediate and practical. It also underscores and highlights the fundamental problem for which a theoretical and doctrinal solution has yet to be discovered. Namely, intellectual property law was not designed to promote the public interest in governmental transparency.[37] To the contrary, it was designed to protect and enforce private property rights, an objective which may seem to be at odds with some of the values of democratic governance.[38] Yet intellectual property law, like property law more generally, is designed to foster contractual transfers of rights and accommodations of conflicting interests.[39] Where the government procures trade-secret-protected algorithmic tools, the procurement contracts can and should accommodate the public's need for some disclosure and transparency.

36. Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 336–37 (2008).

37. *See infra* Subpart II.C.

38. *See infra* Subpart II.B.

39. Lemley, *supra* note 36, at 336–37.

Overall, our proposal is unique and combines several key components. First, it is an *ex ante* approach. Rather than trying to solve a transparency issue during the course of a criminal trial, which is long after the government has purchased the software and begun to use it, our approach tries to resolve the issue at the front end. This is ultimately in the interest of both sides of the transaction *ex ante*. It is more efficient to have a system in place that gets it right the first time. Moreover, there is an increased risk that courts will find forensic algorithms inadmissible at *Frye* or *Daubert* hearings if they have not been independently tested and validated and do not provide access to defense counsel because of overly broad secrecy provisions.[40] Thus, police departments would be incentivized to negotiate disclosure terms *ex ante* rather than risk not being able to use evidence to obtain a conviction, which is what happened with ShotSpotter in Chicago.[41]

Second, it is a *transaction-by-transaction approach*. This offers at least two important benefits. States—and even state courts—would not need to create a one-size-fits-all approach to algorithmic transparency. Perhaps some vendors might not fear disclosure as much as others based on the nature of the technology at issue or its use. For example, some vendors might rely more on copyright and patent rights to protect their IP; they might have less to fear from disclosure and thus might demand more modest protections. For other vendors, trade secrets might be the crown jewels of their technology; thus, they are likely to demand, and to legitimately need, more protection. In our view, this would not mean no transparency, but it might mean more limited disclosures and more protections against unauthorized disclosure.

The transaction-by-transaction approach also allows tailoring based on considerations on the governmental side of the procurement contract. For example, the public interest in governmental transparency might be more pressing in some contexts than in others. Algorithms used to set criminal sentences or generate admissible evidence (like ShotSpotter) may be at one end of the spectrum, where constitutional rights and traditions seem most clearly to demand that the defendants' lawyers need disclosure and have rights to challenge the algorithmic model. On the other hand, algorithms to allocate police resources or perform administrative tasks might be different and may not require as much disclosure.

Another reason for favoring a transaction-by-transaction approach is that it promotes federalism and localism. A pro-transparency city government can negotiate for more transparency, even if the courts or state government in that state are unwilling to take such an aggressive stance. One could argue that in any new area of law involving new circumstances, conditions, and technologies, public policy should favor localism for the traditional Brandeisian "laboratories

40. *See* SLOBOGIN, *supra* note 30, at 84.

41. *See* Feathers, *supra* note 6.

of democracy" reasons.[42] It is also easier to change city contracting policies than it is to enact new federal and state laws on trade secrets. For instance, only one state has passed legislation addressing trade secrecy in criminal justice. On March 28, 2019, Idaho became the first state to completely remove trade secret protections within the criminal justice system for pretrial risk assessment tools and require algorithmic transparency and open access to the public for such tools.[43] While a bold step, this legislation is nevertheless narrow as it is limited to pretrial risk assessment tools. It therefore does not apply to many other algorithmic models such as evidence-generating software like ShotSpotter, DNA analysis software, or facial recognition software. There has also been some movement toward proposing legislation at the federal level to eliminate the trade secret evidentiary privilege in criminal proceedings,[44] but reading political tea leaves, one might expect it is unlikely to become law any time soon.[45]

Third, our approach is *negotiated*. Typically, consumers enter into standardized contracts with sellers without the ability to negotiate their terms. These contracts are not necessarily invalid, but courts may examine the terms more closely to determine whether they are unconscionable.[46] Naturally, these agreements will often be more favorable to the party who drafted them rather than the consumer.[47] In many ways, this appears to be the current status quo, where vendors dictate terms that forbid disclosure, and the government agency–consumer accepts, probably with little pushback.[48] However, the government is no regular consumer. It is the largest purchaser of goods and services, having spent over $14 billion on technology products and services in

42. *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments . . . .").

43. IDAHO CODE § 19-1910 (2019).

44. *See* Press Release, Mark Takano, Rep., U.S. House of Representatives, Reps. Takano and Evans Reintroduce the Justice in Forensic Algorithms Act to Protect Defendants' Due Process Rights in the Criminal Justice System (April 8, 2021), https://takano.house.gov/newsroom/press-releases/reps-takano-and-evans-reintroduce-the-justice-in-forensic-algorithms-act-to-protect-defendants-due-process-rights-in-the-criminal-justice-system; *see also* Justice in Forensic Algorithms Act of 2021, H.R. 2438, 117th Cong. (2021).

45. *See, e.g.*, *117 Legislative Outlook H.R. 2438,* LEXIS, https://plus.lexis.com/document/documentlink/?pdmfid=1530671&crid=28f14df7-3387-45ba-9942-02ae22a38a08&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A62DF-5H01-JSXV-G38W-00000-00&pdcontentcomponentid=133053&pdproductcontenttypeid=undefined&pdiskwicview=false&pdpinpoint=&ecomp=7gktk (last visited Oct. 8, 2022).

46. *See* Jay P. Kesan et al., *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 424 (2013).

47. *Id.* at 425.

48. *See, e.g.*, Agreement between the City of Fresno and ShotSpotter, *supra* note 23, at 3–4.

2020.[49] It has leverage and bargaining power. As such, our negotiated approach envisions use of that power to contract for greater transparency in the procurement context while respecting the rights of vendors.[50] Notwithstanding the government agencies and vendors who may not be inclined toward sharing and might instinctively prefer the status quo's absolute-confidentiality terms, it is worth taking seriously the risks that a court down the road might not agree with those terms[51] or that a legislature may mandate access (similar to the Idaho statute).[52] Thus, our negotiated contract approach helps mitigate against these uncertainties as it affords a more tailored and flexible solution that meets the parties' interests.

Additionally, a negotiated approach allows each side of the potential transaction to decline proposed licensing terms. There is informational value in knowing which vendors and which government agencies value transparency and which do not. For instance, by encouraging market negotiations about transparency, our approach could deliver valuable information about how much transparency vendors may willingly tolerate. If vendors say "no" to especially pro-transparency jurisdictions, the willingness to forego seemingly profitable licensing deals tells public policy makers just how high a price vendors place on secrecy. Similarly, on the government side, agencies are likely to prioritize the benefits that AI technologies provide over transparency. When AI produces the results that governmental officials want, such as fingerprinting, image identification, or DNA matching, few questions are likely to be raised about the validity of their algorithmic models.[53] Even more, after an agency has adopted an AI tool that produces the desired results, there is little incentive for the agency to question the tool.[54] Ultimately, and for accountability, an agency's choices and actions convey valuable information to relevant constituents.

Yet another advantage of our negotiated approach is that reliance on constitutional and legal minima may not be optimal. If the best alternative to negotiated transparency is the "base" level to which a party may be deemed constitutionally (or otherwise) entitled as a post-litigation remedy, it may be largely insufficient. Not only is it likely to benefit or be directed toward only that party (rather than the general public), in the *ex post* litigation approach, courts are relatively limited in that they may enforce only the degree of

49. *A Snapshot of Government-Wide Contracting for FY 2020*, U.S. GOV'T ACCOUNTABILITY OFF.: WATCHBLOG (June 22, 2021), https://www.gao.gov/blog/snapshot-government-wide-contracting-fy-2020-infographic.

50. *See* Andrea M. Matwyshyn, *Privacy, The Hacker Way*, 87 S. CAL. L. REV. 1, 5 (2013) (arguing that contract law can be used as a means to protect consumer privacy).

51. *See* State v. Pickett, 246 A.3d 279, 324 (N.J. Super. Ct. App. Div. 2021).

52. *See* IDAHO CODE § 19-1910 (2019).

53. *See* Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CALIF. L. REV. 721, 745–47 (2007).

54. *See id.* at 746 (noting that "[s]o long as [police and prosecutors] remain satisfied, the [forensic method] laboratories need not engage in any new development or self-criticism").

transparency that is deemed "necessary" under the law.[55] However, such minima may not be optimal for the particular circumstances (or more broadly). Instead, our focus on *ex ante*, negotiated transparency holds at least the potential for more transparency.

Fourth, our approach is *consistent with procurement policy*. The transaction-by-transaction approach is consistent not only with trade secret law but with existing federal and general law and policy on government procurement. While procurement tends to conjure images of government transactions based on awards to the lowest bidder, it is important to understand that procurement law and policies are fundamentally about more than just price.[56] Accordingly, procurement law includes the kind of flexibility that would permit government agencies to negotiate and contract for the kinds of terms that we propose for greater transparency. Indeed, the World Economic Forum's guidelines for AI procurement encourage consideration of both trade secrecy protections for vendors and possibilities for facilitating transparency.[57] Our proposal could supplement those guidelines with additional specificity on how to negotiate transparency within the confines of U.S. law.

In sum, there are three features of procurement law that support our proposal: competitive negotiation, qualification, and consideration of collateral social and economic policies. Competitive negotiation allows an agency significant discretion to establish criteria, other than price, to be included in its solicitation or request for proposals (including our limited disclosure terms). The qualification feature supports an agency's authority to demand that the technology it procures meets certain terms and conditions (perhaps disclosure and performance standards), even if they are different from what is required by the private sector or even other agencies. Finally, an established history of using procurement law to achieve social and economic policies in other contexts (e.g., nondiscrimination and small business support) fits entirely with our proposal to use contract terms to further algorithmic transparency, especially in the absence of appropriate legislation or other regulations.[58] Indeed, we entertain the possibility that a by-product of using procurement in this context is that it may spur legislation, particularly as the public and corporate interests realize that the executive branch could be establishing de facto norms through the procurement process.

---

55. *Cf.* Patrick Murmann & Simone Fischer-Hübner, *Tools for Achieving Usable Ex Post Transparency: A Survey*, 5 IEEE ACCESS 22965, 22966 (2017).

56. *See generally* Joshua Schwartz, Cases and Materials for a Survey of Government Procurement Law (Fall 2021) (unpublished manuscript) (on file with author).

57. WORLD ECON. F., GUIDELINES FOR AI PROCUREMENT 10 (2019), https://www3.weforum.org/docs/WEF_Guidelines_for_AI_Procurement.pdf.

58. *See generally* CHRISTOPHER MCCRUDDEN, BUYING SOCIAL JUSTICE: EQUALITY, GOVERNMENT PROCUREMENT, AND LEGAL CHANGE (2007) (examining how government procurement policies are used to achieve social justice goals).

As the Article proceeds, Part I uses the criminal justice system as a case study from which to analyze the transparency issue and provides summary background on the current status of the procurement and use of forensic algorithmic tools by law enforcement. It also explores legal challenges and considerations, including cases where criminal defendants have (mostly without success) sought access to source code through the courts or FOIA. Part II presents the tension between trade secrecy and transparency, illustrating that the very foundations of this area of intellectual property, including its competitive purpose, property rationale, and the absence of robust consideration of the public interest in governmental transparency, make the two areas (secrecy and transparency) seemingly inconsistent. Part III then attempts to identify the common ground that could bridge the gap between these two areas with a contractual approach that already fits the procurement practices of government agencies and the existing framework of protective measures for trade secret disclosure. It explores the specific shortcomings of the current system of acquisition of artificial intelligence and other algorithmic technologies in the criminal justice system and discusses the types of contractual provisions that might be negotiated by private developers and government agencies to simultaneously protect proprietary interests while permitting limited disclosure. The Part ends by exploring, along with potential drawbacks, the benefits of this approach for the various stakeholders, including better control and accountability, increased integrity of the criminal justice system, and greater certainty and consistency for vendors.

I. ALGORITHMS IN THE CRIMINAL JUSTICE SYSTEM

An increasing number of jurisdictions continue to adopt statistical algorithmic software in various criminal justice contexts in an attempt to maximize resources, reduce bias, and promote justice.[59] Forensic technologies that incorporate algorithms are utilized throughout the system for facial recognition, DNA analysis, fingerprint analysis, and ballistic analysis.[60] As specifically relevant to this exemplar, they are also used at the law-enforcement

59. Risk of recidivism predictions are most commonly considered in front-end sentencing but can be a factor for consideration in back-end sentencing where parole revocation is at issue. *See* Eric Holder, U.S. Att'y Gen., Remarks at the National Association of Criminal Defense Lawyers 57th Annual Meeting and 13th State Criminal Justice Network Conference (Aug. 1, 2014); Jeremy Travis, *Back-End Sentencing: A Practice in Search of a Rationale*, 74 SOC. RSCH. 631, 632–34, 637–38 (2007) (noting that front-end sentencing occurs in criminal courts and is more transparent and legally constrained than back-end sentencing, which involves parole revocation that only needs to be found by a preponderance of evidence and does not provide the parolee with the same rights afforded to criminal defendants).

60. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFF., FORENSIC TECHNOLOGY: ALGORITHMS USED IN FEDERAL LAW ENFORCEMENT 5–11, https://www.gao.gov/assets/gao-20-479sp.pdf#:~:text=Federal%20law%20enforcement%20agencies%20GAO; *see also* Wexler, *supra* note 30, at 1363–64.

level, during trial as evidence, and for sentencing determinations.[61] Despite the well-intentioned motivations to adopt such technologies, there are many instances where algorithm implementation occurs before rigorous testing has been conducted.[62]

Algorithms in the criminal justice system are intended to make the process more efficient, cost-effective, and fair, but unfortunately, this is not always the case.[63] In general, algorithms help humans perform tasks faster, but artificial intelligence systems are ultimately built by humans and do not contain the independent ability to evaluate moral or ethical distinctions beyond how the algorithm or machine is initially programmed.[64] Indeed, while an algorithmic approach may seem objective on the surface, human developers preprogram every system with factors weighed with inherent power differentials decided upon by the initial developers, and a system's results are constrained by the developer's definitions of success.[65] The wide ranging presence of AI at every stage of the criminal justice system raises concerns about unchecked uses and the potential for complicating and exacerbating systemic problems.[66] Nevertheless, these adoptions will undoubtedly continue to flourish, especially because they offer benefits and efficiencies. While it is beyond the scope of this Article to delve into a more comprehensive sampling, one representative example (risk assessment algorithms) is discussed in more detail below.

A. The Example of Risk Algorithms

The U.S. criminal justice system has increasingly come to rely on algorithms to sentence criminal defendants in response to calls for reducing racial disparities and mass incarceration. According to the NAACP, the United States comprises 5% of the world's population yet has 25% of the world's prisoners.[67]

61. *See* Alex Chohlas-Wood, *Understanding Risk Assessment Instruments in Criminal Justice*, BROOKINGS (June 19, 2020), https://www.brookings.edu/research/understanding-risk-assessment-instruments-in-criminal-justice/.

62. *See, e.g.*, Brauneis & Goodman, *supra* note 30, at 152 (describing researchers' inability to obtain records about the creation and implementation of algorithms already in use in twenty-three states); Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), (https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html (describing DataWorks' (a facial-recognition company) lack of accuracy or bias testing for its algorithm that has been on the market since 2005).

63. *See* SLOBOGIN, *supra* note 30, at 29–30 (noting that algorithmic decision-making in the criminal justice system could provide less biased outcomes than those by humans).

64. Ashley M. London & James B. Schreiber, *AI Report: Humanity Is Doomed. Send Lawyers, Guns, and Money*!, 58 DUQ. L. REV. 97, 105 (2020).

65. *See id.*; *see also* Ngozi Okidegbe, *Discredited Data,* 107 CORNELL L. REV. (forthcoming 2022) (discussing biases resulting from training algorithms using carceral data sources).

66. *See infra* Subpart I.B. *See generally* Sonja B. Starr, *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, 66 STAN. L. REV. 803 (2014).

67. *Criminal Justice Fact Sheet*, NAACP, https://www.naacp.org/criminal-justice-fact-sheet/ (last visited Sep. 9, 2020).

Of those prisoners, African-Americans constitute 38% of the over 2 million prisoners in the United States—five times the rate of incarceration of non-minorities.[68] Evidence-based initiatives, academics and sentencing commissions assert, can combat these disparities by determining more consistent criminal penalties based on less-biased predictions of a defendant's risk of reoffending.[69] Proposed revisions of the Model Penal Code ("MPC"), for example, currently support the use of "actuarial instruments or processes" to estimate individual risks to public safety and advocate their formal incorporation into sentencing guidelines.[70]

The United States' prison population has over 2.2 million people with current statistics indicating that historically marginalized groups are overrepresented in the incarcerated population.[71] Proponents of AI in the criminal justice system (including prosecutors, academics, law professors, law enforcement officers, and software developers) assert that algorithms are an ideal solution for reducing high levels of incarceration and maintaining consistent prison sentencing across all racial groups because of AI's accurate and efficient predictive modeling capabilities.[72] For example, former prosecutor and New Jersey Attorney General Anne Milgram favors algorithms in the criminal justice system because she believes data and analytics can be useful in determining risk levels for pretrial holding and sentence durations in a way that would reduce prison populations by allowing low-risk offenders to be released.[73] Another proponent, Richard Berk, a criminology and statistics

68. Wendy Sawyer & Peter Wagner, *Mass Incarceration: The Whole Pie*, PRISON POL'Y INITIATIVE (Mar. 14, 2022), https://www.prisonpolicy.org/reports/pie2022.html

69. *See generally* Starr, *supra* note 66, at 815.

70. *Id.*; MODEL PENAL CODE: SENT'G § 6B.09 cmt. a, at 387–89 (AM. LAW INST., Proposed Final Draft 2017) (noting that the MPC argument in favor of evidence-based sentencing is demonstrated by the official commentary: "Responsible actors in every sentencing system—from prosecutors to judges to parole officials—make daily judgments about . . . the risks of recidivism posed by offenders. These judgments, pervasive as they are, are notoriously imperfect. They often derive from the intuitions and abilities of individual decisionmakers, who typically lack professional training in the sciences of human behavior").

71. *See Criminal Justice Fact Sheet*, *supra* note 67.

72. *See, e.g.*, SLOBOGIN, *supra* note 30, at 1; Coglianese & Ben Dor, *supra* note 30, at 827–28 (arguing that utilizing AI in the administrative context has the same benefits as its use in the private sector, namely accuracy and efficiency, that allow for more accurate forecasts for governmental decision-making); Sam Corbett-Davies et al., *Even Imperfect Algorithms Can Improve the Criminal Justice System*, N.Y. TIMES (Dec. 20, 2017), https://www.nytimes.com/2017/12/20/upshot/algorithms-bail-criminal-justice-system.html (noting algorithmic risk scores allow for more consistency to combat disparities resulting from individual judge preference where stricter judges impose bail twice as often as lenient judges).

73. Anne Milgram, Why Smart Statistics Are the Key to Fighting Crime (Oct. 2013) (transcript available at https://www.ted.com/talks/anne_milgram_why_smart_statistics_are_the_key_to_fighting_crime?language=en). Ms. Milgram later accepted a role at the Arnold Foundation and led a team of researchers and statisticians to build a universal risk assessment tool to predict whether an individual is likely to commit an act of violence if released. *See* Kathleen Hickey, *Former New Jersey Attorney General Leads an Effort to Develop Risk-Assessment Tool to Help Judges Make Data-Driven Sentencing Decisions*, GCN (Feb. 21, 2014), https://gcn.com/data-analytics/2014/02/get-out-of-jail-or-do-more-time-risk-tools-help-judges-

professor at the University of Pennsylvania, has designed various algorithms currently used in Pennsylvania, and Berk says these are more accurate, fair, and transparent than judicial discretion subject to unconscious bias.[74]

Given this apparent support, court systems have continued to adopt algorithms for criminal justice purposes. As of August 2021, nearly every state has adopted some form of algorithm for making risk assessment determinations for different proceedings within the criminal justice system.[75] More local jurisdictions within each state[76] are adopting forensic algorithms for additional purposes beyond risk assessment, including facial recognition,[77] bail determination,[78] criminal sentencing,[79] and DNA matching.[80]

Contrary to state practices, the federal criminal justice system has not readily adopted risk assessments. Indeed, federal risk assessments virtually disappeared from federal sentencing when formal guidelines were instituted to require judges to issue backward-looking sentences based on culpability instead of forward-looking sentences considering risk of future crime.[81] Congressional and executive delays in adopting algorithm-based risk assessments may also be

decide/290177/. Ms. Milgram hopes that this universal risk assessment tool will eventually be used by every judge in the United States. *See* Milgram, *supra*.

74. *See* Dana Casadei, *Predicting Prison Terms and Parole*, DOWNTOWN NEWSMAG. (Mar. 24, 2020), https://www.downtownpublications.com/single-post/2020/03/24/Predicting-prison-terms-and-parole.

75. *AI in the Criminal Justice System: Pre-Trial Risk Assessment Tools*, ELEC. PRIV. INFO. CTR., https://epic.org/algorithmic-transparency/crim-justice/ (last visited Sep. 9, 2021); *see also* Rhys Dipshan et al., *The United States of Risk Assessment: The Machines Influencing Criminal Justice Decisions*, LEGALTECH NEWS (July 13, 2020, 07:00 AM), https://www.law.com/legaltechnews/2020/07/13/the-united-states-of-risk-assessment-the-machines-influencing-criminal-justice-decisions/?slreturn=20200816100945.

76. *See* Coglianese & Ben Dor, *supra* note 30, at 794 (noting that based on researchers' telephone and email exchanges with the National Center for State Courts, there are approximately 15,000 to 17,000 different state and municipal courts, which range based on changes in size and organization of the latter); *see also State Court Structure Charts*, CT. STAT. PROJECT, http://www.courtstatistics.org/state_court_structure_charts?SQ_VARIATION_28850=0 (last visited Sep. 17, 2020).

77. *See, e.g.*, Hill, *supra* note 62 (detailing the story of a wrongfully arrested Black man based on a flawed match from a facial recognition algorithm).

78. *See, e.g.*, Holland v. Rosen, 277 F. Supp. 3d 707, 718 (D.N.J. 2017) (allowing for the use of a public safety assessment algorithm to weigh nine objective factors, excluding race and gender considerations, to influence bail determinations based on statistical likelihood of failure to appear, new criminal activity, and new violent criminal activity).

79. *See, e.g.*, State v. Loomis, 881 N.W.2d 749, 769–70 (Wis. 2016) (allowing for input from an algorithm predicting the risk of a recidivism for making a sentencing determination, subject to certain limitations).

80. Press Release, Cybergenetics, Computers Are Helping Justice (June 16, 2017), https://www.cybgen.com/information/newsroom/2017/jun/Cybergenetics-to-New-York-Times-Computers-are-helping-justice.shtml. In the case against Darryl Pinkins, who was misidentified and wrongfully convicted of rape and robbery, TrueAllele led to the release and exoneration of Pinkins after twenty-seven years of incarceration. *Id.* TrueAllele was able to identify additional DNA samples that FBI interpretation had initially failed to recognize. *Id.*

81. Brandon L. Garrett, *Federal Criminal Risk Assessment*, 41 CARDOZO L. REV. 121, 123–24 (2019).

attributed to constitutional limitations[82] and federalism.[83] Additionally, federal statutes are subject to jurisdictional restraints unlike state legislatures, which are able to exercise plenary police powers without being limited to enumerated powers contained in the Constitution.[84] Despite these limitations, Congress may nevertheless enact substantive and procedural criminal laws under the Necessary and Proper Clause when such a law is reasonably related to other constitutionally enumerated powers.[85]

Though federal courts and prison systems have not been as quick to adopt algorithmic tools (concrete adoption statistics do not appear to be readily ascertainable), the trend may be changing. For example, on December 21, 2018, President Trump—with bipartisan support—signed the First Step Act ("FSA") into law.[86] The FSA is focused on reducing recidivism through prison reform and allows for governmental contracting to develop the Prisoner Assessment Tool Targeting Estimated Risk and Needs ("PATTERN"), an algorithmic instrument that predicts the likelihood of recidivism for parolees within three years of federal prison release.[87] The FSA and PATTERN were enacted and developed in response to calls for risk assessments in federal parole decisions.[88] Development and finalization of PATTERN is still ongoing,[89] but federal

82. *See* Reid v. Covert, 354 U.S. 1, 5–6 (1957) ("The United States is entirely a creature of the Constitution. Its power and authority have no other source. It can only act in accordance with all the limitations imposed by the Constitution." (citation omitted)); U.S. CONST. art. I, § 1 ("All legislative Powers herein granted shall be vested in a Congress of the United States . . . ."); U.S. CONST. art. I, § 8, cl. 6 (granting Congress the power to provide for punishment for counterfeiting); U.S. CONST. art. I, § 8, cl. 10 (allowing Congress to define and punish piracies and felonies committed on the high seas and offenses against international law); U.S. CONST. art. III, § 3, cl. 2 (empowering Congress to set punishment requirements for treason).

83. *See* U.S. CONST. amend. X ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.").

84. *See, e.g.*, United States v. Lopez, 514 U.S. 549, 567 (1995); *see also* Engle v. Isaac, 456 U.S. 107, 128 (1982) ("The States possess primary authority for defining and enforcing the criminal law. In criminal trials they also hold the initial responsibility for vindicating constitutional rights. Federal intrusions into state criminal trials frustrate both the States' sovereign power to punish offenders and their good-faith attempts to honor constitutional rights.").

85. U.S. CONST. art. I, § 8, cl. 18 ("The Congress shall have Power . . . [t]o make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States . . . .").

86. U.S. DEP'T OF JUST., THE FIRST STEP ACT OF 2018: RISK AND NEEDS ASSESSMENT SYSTEM (2019), https://www.ojp.gov/First-Step-Act-of-2018-Risk-and-Needs-Assessment-System; *see* First Step Act of 2018, Pub. L. No. 115-391, sec. 101, § 3635(6), 132 Stat. 5194, 5208; *see also* Coglianese & Ben Dor, *supra* note 30, at 802.

87. U.S. DEP'T OF JUST., *supra* note 86, at 43 (noting that the PATTERN instrument's model prediction algorithm is based on static risk factors and that "dynamic items that are associated with either an increase or a reduction in risk" comply with FSA requirements); *see also* Brandon Garrett & John Monahan, *Assessing Risk: The Use of Risk Assessment in Sentencing*, JUDICATURE, Summer 2019, at 42, 43 (noting the FSA, "perhaps the most far-reaching federal sentencing reform in a generation, mentions risk no less than 100 times and relies on risk assessments to allocate prison programming and prisoner release").

88. U.S. DEP'T OF JUST., *supra* note 86; *see* First Step Act of 2018, Pub. L. No. 115-391, 132 Stat. 5194.

89. U.S. DEP'T OF JUST., *supra* note 86, at 70–90 (discussing ongoing changes and modifications to PATTERN as a result of independent review committees and stakeholder meetings).

enactment of both the FSA and PATTERN seem to be indicative of expanding predictive algorithm use in the federal criminal justice system.

It is worth noting at this juncture that when we speak broadly about "the criminal justice system," there are differences between federal and state agencies and practices. Thus, there is no unified system, which inevitably leads to inconsistencies and wide-ranging, divergent practices and policies (even within states).[90]

B. Procurement of Algorithms

Procurement is the process by which government agencies may enter into contracts for the "principal purpose of . . . furnish[ing] services in the United States through the use of service employees."[91] There are separate federal and state procurement systems. State adoptions of technologies for use in the criminal justice system are possible through licensing procurement based on broad legislative permissions, which typically require adherence to only minimal standards of justice.[92] Beyond that, states have discretion to negotiate and enter into terms and agreements with vendors.[93] For example, as a condition for utilizing risk recidivism algorithms, developers will often require the user—including law enforcement and judiciaries—to sign a memorandum of understanding ("MOU") prior to implementation to prohibit disclosure of algorithms deemed to be trade secrets.[94] How states choose to respond to MOU requirements and handle implementation is largely based on principles of federalism as there is no uniform federal requirement equally applicable to the states.[95] In Florida, for example, private parties must expressly designate what

90. Trevor G. Gardner & Lisa L. Miller, *Criminal Justice*, CTR. FOR THE STUDY OF FEDERALISM, http://encyclopedia.federalism.org/index.php/Criminal_Justice (last updated May 2018) (describing how the array of federal, state, and local criminal justice systems constitute America's decentralized approach to criminal justice and often results in differing policies surrounding the same issue, such as capital punishment).

91. 29 C.F.R. § 10.2 (2022); *see also* 41 U.S.C. § 6701(3)(A) (defining a service employee as an individual performing duties under a government contract for the benefit of the United States).

92. *See* Christopher Bavitz & Kita Hessekiel, *Examining the Role of the State in the Development and Deployment of Algorithmic Technologies*, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y (July 11, 2018), https://cyber.harvard.edu/story/2018-07/algorithms-and-justice. *See generally* CHRISTOPHER BAVITZ ET AL., BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y, ASSESSING THE ASSESSMENTS: LESSONS FROM EARLY STATE EXPERIENCES IN THE PROCUREMENT AND IMPLEMENTATION OF RISK ASSESSMENT TOOLS (2018) [hereinafter ASSESSING THE ASSESSMENTS], https://ssrn.com/abstract=3297135 (expressing concern toward the standards of justice in play when states adopt these technologies).

93. *See, e.g.*, *CJIS Livescan Contracts*, FLA. DEP'T OF L. ENF'T, https://www.fdle.state.fl.us/CJIS/Livescan-Contracts (last visited Sep. 8, 2021) (listing the current Florida law enforcement contracts for purchasing Livescan devices); Exec. Order No. 14,006, 86 Fed. Reg. 7483 (Jan. 26, 2021).

94. *See* Brauneis & Goodman, *supra* note 30, at 138–39. Developers often try to obtain written confidentiality agreements or MOUs for algorithm use, even in the criminal justice context. *Id.*

95. U.S. CONST. amend. X ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.").

information is considered a trade secret; otherwise, confidentiality is considered waived.[96]

Government agents responsible for procurement generally do not have guidance on best practices when comparing and evaluating different artificial intelligence tools, which sometimes results in premature algorithm deployment.[97] Lack of implementation guidelines have been a strong point of criticism. Harvard's Criminal Justice Policy Program argues that without proper calibration to reflect the relevant jurisdiction, any potential benefits from the algorithm may be undermined by disparities or displacement of other considerations.[98] Further, court adoption of algorithms does not typically require judicial training. Therefore, for risk assessments, judges may not know how the software works, what exactly the numerical risk score means, or whether the risk score relies solely on populational outcomes derived from data based on individuals with certain characteristics that the developer arbitrarily chose.[99] In other words, the algorithm may be accurate for group averages, but not for specified individuals within the group, which poses significant problems if judges erroneously give undue weight to algorithmic-based risk scores. If proper validation and review are not in place, these problems may not be discovered until well after the predictive algorithm has been in use.

1. Exemplar Developers

Although they vary, state court systems have adopted algorithms developed by for-profit companies, non-profit organizations, or government units to determine bail, pretrial detention, sentencing, prison management, and parole.[100] Northpointe (now Equivant), a private, for-profit company established in 1989, developed one of the most widely used algorithms for risk assessment: Correctional Offender Management Profiling for Alternative Sanctions ("COMPAS").[101] Equivant's COMPAS differentiates between risk scales and needs scales.[102] The COMPAS risk scales attempt to predict

96. *See* Brauneis & Goodman, *supra* note 30, at 139.

97. *See* Bavitz & Hessekiel, *supra* note 92; ASSESSING THE ASSESSMENTS, *supra* note 92, at 2.

98. CRIM. JUST. POL'Y PROGRAM, HARV. L. SCH., MOVING BEYOND MONEY: A PRIMER ON BAIL REFORM 20 (Oct. 2016), https://www.prisonpolicy.org/scans/cjpp/FINAL-Primer-on-Bail-Reform.pdf.

99. *Id.* at 21. These issues are especially prominent when algorithms are developed by private companies. For example, when risk assessments characterize certain risks as "high," "moderate," or "low" based on a policy assessment as opposed to true statistics, judges may give undue weight to deciding in favor of a specific outcome. *See id.*

100. *AI in the Criminal Justice System: Pre-Trial Risk Assessment Tools*, *supra* note 75.

101. *Northpointe Suite Risk Needs Assessment*, EQUIVANT, https://www.equivant.com/northpointe-risk-need-assessments/ (last visited Oct. 6, 2022).

102. EQUIVANT, PRACTITIONER'S GUIDE TO COMPAS CORE 4 (2019), http://www.equivant.com/wp-content/uploads/Practitioners-Guide-to-COMPAS-Core-040419.pdf. *See generally* NATHAN JAMES, CONG. RSCH. SERV., R44087, RISK AND NEEDS ASSESSMENT IN THE FEDERAL PRISON SYSTEM (2018).

recidivism, with the purpose of "discriminat[ing] between offenders who will and will not recidivate," whereas the needs scales attempt to "describe the offender."[103] According to Equivant, COMPAS is comprised of forty-three scales that are user-configurable at different decision points based on populational and local criminal justice system needs.[104]

In a study by *ProPublica*, researchers discerned that the COMPAS algorithm relies on scores derived from various combinations of 137 questions answered by either the defendant or criminal records, though the calculations used to determine the risk score are not publicly disclosed due to trade secrecy assertions.[105] COMPAS and other algorithms serve as pretrial risk assessments, though courts use the scores at varying stages of criminal proceedings. As of 2016, at least nine states allow judges to consider COMPAS scores when making sentencing determinations.[106]

On the non-profit side, the Arnold Foundation has been a leading developer of risk assessment software, aiming to improve the criminal justice decision-making process by developing safer, fairer, and cost-effective data-driven risk assessment tools.[107] The Foundation developed an automated Public Safety Assessment ("PSA") based on existing Kentucky data from criminal defendant interviews because it viewed Kentucky as a data collection leader in the pretrial field.[108] Early versions of the PSA evaluated nine criminal history factors and three questions from defendant interviews but had a goal of removing the interview-dependent questions.[109] The Foundation considered "hundreds of risk factors," including those related to prior arrests, prior convictions, drug and alcohol use, mental health, familial status, and employment, and they determined that the algorithm alone—without the defendant interview—was highly effective in its predictions.[110] Later versions of the PSA provide a judicial dashboard with scores for "risk of violence" and "failure to appear."[111] In an independent study conducted by filing forty-two open records requests in twenty-three states, researchers discerned that the Arnold Foundation created its risk assessment algorithm by analyzing data in

103. EQUIVANT, *supra* note 102, at 7.

104. *Id.* at 2.

105. Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

106. *Id.* (explaining that states allowing COMPAS score consideration during sentencing include Arizona, Colorado, Delaware, Kentucky, Louisiana, Oklahoma, Virginia, Washington, and Wisconsin).

107. LAURA & JOHN ARNOLD FOUND., RESEARCH SUMMARY: DEVELOPING A NATIONAL MODEL FOR PRETRIAL RISK ASSESSMENT 1–2 (2013); *see also* Casadei, *supra* note 74 (identifying other common algorithms including the Ohio Risk Assessment System-Pretrial Assessment Tool (ORAS-PAT), Virginia Pretrial Risk Assessment Instrument (VPRAI), and Virginia Pretrial Risk Assessment Instrument-Revised (VPRAI-R)).

108. LAURA & JOHN ARNOLD FOUND., *supra* note 107, at 3.

109. *Id.* at 3–4.

110. *Id.*

111. Milgram, *supra* note 73.

750,000 cases; however, there was no information about how the data was analyzed, whether there were any alternatives, or how those alternatives compared to the algorithms that were eventually implemented.[112] The authors concluded that secrecy surrounding the PSA was the result of insufficient judicial and legislative insistence on disclosure practices and deference to overbroad trade secret assertions.[113]

2. Algorithms Need Data

Algorithms cannot operate effectively without sufficient data.[114] Traditional statistical tools require human intervention to choose specific variables and select the precise mathematical relationships between the variables; once machine learning is involved, artificial intelligence allows algorithms to discover correlations "on their own" after they have been programmed to do so.[115] In the criminal justice context, risk assessment software considers factors such as "socioeconomic status, family background, neighborhood crime, employment status," education, employment history, and demographic information to generate a high or low score with specific percentages based on an individual's criminal risk.[116] While developers are often reluctant to explicitly include race in these algorithms, Professor Deborah Hellman has argued that it is legally permissible to do so and that doing so may actually improve fairness.[117]

Statisticians use these demographics, along with sentencing data and historical recidivism rates, to identify which variables occur in the most relevant cases, and those data points are then used to create predictive models.[118] Statisticians then reverse the process to try to locate the selected variables in new cases, which, if successful, may then be applied to active cases to generate recidivism risk scores.[119] Like all statistical models, the quality of the algorithm being used depends on many factors, including sample size, testing duration, record completeness, and modeling strategy.[120]

---

112. Brauneis & Goodman, *supra* note 30, at 141.

113. *Id.* at 110.

114. *See generally* Willem Sundblad, *Data Is the Foundation for Artificial Intelligence and Machine Learning*, FORBES (Oct. 18, 2018, 10:30 AM), https://www.forbes.com/sites/willemsundbladeurope/2018/10/18/data-is-the-foundation-for-artificial-intelligence-and-machine-learning/#4bd8c64051b4 ("[D]ata is both the most underutilized asset of manufacturers and the foundational element that makes AI so powerful.").

115. Coglianese & Ben Dor, *supra* note 30, at 795–96.

116. *AI in the Criminal Justice System: Pre-Trial Risk Assessment Tools*, supra note 75.

117. Deborah Hellman, *Measuring Algorithmic Fairness*, 106 VA. L. REV. 811, 818 (2020).

118. ANGÈLE CHRISTIN ET AL., COURTS AND PREDICTIVE ALGORITHMS 1, 4 (Oct. 27, 2015), https://www.law.nyu.edu/sites/default/files/upload_documents/Angele%20Christin.pdf.

119. *Id.* at 4.

120. *See, e.g.*, DAVID STEINHART, ANNIE E. CASEY FOUND., JUVENILE DETENTION RISK ASSESSMENT: A PRACTICE GUIDE TO JUVENILE DETENTION REFORM 52 (2006), https://www.aecf.org/m/resourcedoc/aecf-juvenileddetentionriskassessment1-2006.pdf.

More advanced programs, such as COMPAS, analyze a large series of dataset inputs (e.g., criminal history, age, education level) that are obtained from public records or defendant answers to reveal which correlations best fit the data relationship between the inputs and outcomes.[121] In essence, each factor is weighed against the algorithm's associated risk factor input to generate a risk score. To measure the algorithmic model's performance, data scientists compare false positives and false negatives that the algorithm generates for random guesses based on group data.[122] This graphical representation creates what is known as a "receiver operating characteristic" ("ROC") curve that generates numerical values between 0.5 and 1 to compare algorithm accuracy to random guesses; however, this approach only works when the algorithm's outputs are ranked as least-likely to most-likely to be associated with a given outcome.[123]

Readers should note that the above descriptions are merely general illustrations rather than complete descriptions of any specific predictive algorithm. Indeed, software developers often attempt to maintain many operative features of how specific algorithms work as trade secrets (e.g., which factors are considered and how heavily these factors are weighed in the final risk score calculation). Furthermore, in the context of predictive algorithms and transparency, it is worth clarifying that scholars are mostly concerned about understanding the model—i.e., what variables are used and how they are processed to result in a prediction—and understanding the validity of the model—i.e., to what degree the model is accurate, biased, etc. A given model might be implemented in computer code in different ways, so it is the model, rather than how it is implemented in code, that could be revealing. Thus, in many cases, disclosure of the source code does not allow one to understand the model because, for example, the variables (e.g., "variable 1") may not be named in a way that helps to understand what they represent. Moreover, even if the code aided in understanding the model, mere code disclosure would not necessarily help to assess the validity of the model.[124]

3. Inconsistent Testing and Implementation.

Due to the technical skill and financial costs associated with developing predictive algorithms, many states are likely to require third-party contracting for software services. Absent express state requirements for trade secret or

121. *See* EQUIVANT, *supra* note 102, at 31–32.

122. *See* Brauneis & Goodman, *supra* note 30, at 121.

123. *Id.*

124. *See, e.g.*, SLOBOGIN, *supra* note 30, at 108 (discussing the congressional decision to require public disclosure of only the PATTERN algorithm, not the underlying validation studies or data).

confidentiality designations,[125] these contracts likely include default terms requiring stringent confidentiality—benefiting the service provider while simultaneously failing to provide for clear validation standards.

The below examples are only a few publicly available instances of problematic outcomes associated with improper algorithm testing, and some occurrences may never be publicized. A 2013 study examined nineteen different risk methodologies and found that software developers only examined algorithm validity in one or two studies.[126] There were no external independent reviews.[127] Because states have the ability to exercise plenary police powers, there is undoubtedly variability among jurisdictional uses of algorithms, including possession rights, which makes any efforts for establishing consistency difficult to achieve.[128] This is especially true when proper testing is not conducted for algorithms with serious implications such as higher bail requirements or harsher prison sentences.

Indeed, new algorithm technologies are often prematurely adopted in the criminal justice system without proper validation studies. For example, New York adopted an algorithm-based probationary pilot program which was expanded to the entire state probation department in 2010, yet a comprehensive statistical evaluation was not published until 2012.[129] In Michigan, Detroit police relied on DataWorks Plus's faulty algorithmic identification of a grainy surveillance video still to arrest a Black man for a crime he did not commit in what was likely the first publicized faulty facial recognition case.[130] Although DataWorks Plus was developed in 2005 and has had significant time for testing, the company's general manager confirmed that scientific testing to formally measure accuracy or bias has not been performed.[131]

As it turns out, COMPAS validity measurements take advantage of the industry-accepted standard of meeting only a 70% probability requirement that a randomly chosen defendant is classified correctly, regardless of whether that classification is of high or low risk of recidivism.[132] This standard essentially allows for a 30% chance that a low-risk defendant will be ranked as high-risk

125. *See, e.g.*, Brauneis & Goodman, *supra* note 30, at 139 (explaining the MOU between the Arnold Foundation and a Florida court requiring trade secret designation).

126. *See* Jeff Larson et al., *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

127. *See id.*

128. *See* Katyal, *supra* note 30, at 1244–45 (discussing limitations on discovery orders in terms of "information within the custody, possession, or control by the State," for which states can choose to allow code developers to maintain possession of algorithmic source code and thus evade the scope of discovery).

129. Angwin et al., *supra* note 105. New York City was initially excluded from the pilot program. *Id.*

130. *See* Hill, *supra* note 62 (explaining that if police had conducted further investigation before relying so heavily on the facial recognition algorithm, they would have discovered that the suspect had posted an Instagram video during the time of the robbery, which showed him driving home from work).

131. *See id.*

132. *See* John Lightbourne, *Damned Lies & Criminal Sentencing Using Evidence-Based Tools*, 15 DUKE L. & TECH. REV. 327, 336 (2017).

and receive a longer or harsher sentence than the defendant otherwise would have if the algorithm had predicted correctly.[133]

In Florida, state testing deficiencies and preliminary indications of racially disparate impacts motivated *ProPublica* to obtain risk scores for more than 7,000 people arrested in Broward County between 2013 and 2014 to determine how many individuals were charged with a new crime over a two-year period following their arrest—the same standard used by COMPAS developers.[134] The 2016 *ProPublica* study found the risk scores to be highly unreliable. Of the total number of people predicted to commit a subsequent violent crime, only 20% did so.[135] For those deemed likely to commit any future crime, only 61% were arrested within a two-year period.[136]

Some states have been more forthcoming than others with their data and predictive algorithm implementation processes. For instance, Pennsylvania provides predictive algorithm information on its website.[137] However, this is likely because the Pennsylvania Commission on Sentencing developed its own algorithm as opposed to contracting with a service provider.[138]

C. Legal Challenges & Considerations

The law always seems to trail technological advancements, and predictive algorithms are no different as courts have only just begun tackling the associated legal implications of artificial intelligence. Of the cases that have addressed challenges to predictive algorithms, little is known about how much weight trial court judges ascribe to such risk assessments, especially in determining whether a risk score was a dispositive factor.[139] Although risk scores, such as those provided by COMPAS, are intended to be used only as advisory guidance, judges have cited risk scores in their sentencing decisions.[140] Despite the large impact that risk scores may have, courts have generally been unwilling to provide defendants with access to the algorithms to ensure proper computations.[141] If considered persuasive precedent, these decisions may have

133. *See id.*

134. *See* Angwin et al., *supra* note 105.

135. *Id.*

136. *Id.*

137. *See* SENTENCING RISK ASSESSMENT INSTRUMENT, PA. COMM'N ON SENT'G, https://pcs.la.psu.edu/guidelines-statutes/risk-assessment/ (follow "Sentence Risk Assessment Instrument" hyperlink") (last visited July 11, 2020); *see also* Stephanie Wykstra, *Just How Transparent Can a Criminal Justice Algorithm Be?*, SLATE (July 3, 2018, 08:00 AM), https://slate.com/technology/2018/07/pennsylvania-commission-on-sentencing-is-trying-to-make-its-algorithm-transparent.html.

138. *See* sources cited *supra* note 137.

139. *See* Richard Berk, *An Impact Assessment of Machine Learning Risk Forecasts on Parole Board Decisions and Recidivism*, 13 J. EXPERIMENTAL CRIMINOLOLGY 193, 194 (2017) (noting that the public has "scant information about how actuarial risks assessments have affected practices and outcomes").

140. Angwin et al., *supra* note 105.

141. *See id.*

widespread implications in the form of algorithmic access if other jurisdictions choose to adopt similar reasoning.

In Wisconsin, for instance, criminal justice leaders appear to favor algorithm use. The Wisconsin Department of Corrections has adopted algorithms in each step of the criminal proceedings, and judges have cited risk scores as factors in issuing a criminal sentence.[142] For example, Paul Zilly, convicted of stealing a push lawn mower and tools, reached a plea agreement in which the prosecutor would recommend a year in county jail; however, the judge reviewed Zilly's COMPAS risk score and instead imposed a two-year sentence in state prison followed by three years of supervision.[143] After Equivant's founder testified that COMPAS was not originally designed to be used for sentencing, the judge (on appeal) reduced Zilly's prison sentence to eighteen months.[144]

In *State v. Loomis*, the Wisconsin Supreme Court held that COMPAS scores, when based on accurate input information, did not violate due process protections for individual sentencing.[145] The defendant challenged the risk score, arguing that he was unable to ascertain how his risk score was determined because it was unclear how specific factors were weighed, and that the developer's trade secret assertion amounted to withholding information considered for sentencing purposes.[146] The court rejected this challenge by reasoning that the PSR was accompanied by additional factors such that courts could sufficiently assess score accuracy and that risk scores would only be a due process violation if used as the exclusive determinative factor.[147]

Another source code example (not involving a predictive tool, but DNA analytics) comes from California. In *People v. Superior Court* (*Chubbs*), the California Court of Appeals denied the defendant's request for the algorithmic source code used to calculate the likelihood of the presence of the defendant's DNA at the crime scene based on a complex DNA sample.[148] The court reasoned that the source code was protected under California's trade secret privilege[149]—likely the first decision of its kind to extend evidentiary privileges for trade secret protection in the criminal context.[150] In requiring a

142. *See* Julia Angwin et al., *Risk Scores Attached to Defendants Unreliable, Racially Biased*, MILWAUKEE J. SENTINEL (May 30, 2016), http://archive.jsonline.com/news/crime/risk-scores-attached-to-defendants-unreliable-racially-biased-b99732973z1-381306991.html.

143. *See id.*

144. *Id.*

145. *See* State v. Loomis, 881 N.W.2d 749, 749, 766–67 (Wis. 2016). The Wisconsin Supreme Court affirmed an eight-year sentence based on the defendant's plea to two lesser charges associated with a drive-by shooting and a presentence report ("PSR"). *Id.*

146. *Id.* at 761.

147. *Id.* at 764–65, 768, 771.

148. *See* People v. Superior Court (*Chubbs*), No. B258569, 2015 WL 139069, at *9 (Cal. Ct. App. Jan. 9, 2015).

149. *Id.* at *1, *5–6.

150. Wexler, *supra* note 30, at 1358–59.

particularized showing that the algorithm is necessary to the defendant's defense, the *Chubbs* court heightened the discovery burden from the standard good cause showing.[151] Instead of simply requiring a protective order, the court withheld potentially critical information in its entirety from the defendant.[152]

Some courts outside of California[153] are citing *Chubbs* in criminal proceedings to justify trade secret exemptions for algorithm disclosure, including that of TrueAllele.[154] Other courts, especially in Wisconsin, have cited *Loomis* for at least two propositions. First, courts may consider COMPAS risk scores without algorithmic model disclosure so long as the score is not determinative;[155] second, COMPAS scores constitute a proper factor within the scope of judicial discretion in sentencing.[156] At least where horizontal stare decisis is concerned, proponents of algorithm non-disclosure suggest that the trade secret issue has already been decided such that courts can consider risk recidivism scores while withholding certain elements from defendants.[157]

Despite the apparent trend favoring increased predictive algorithm use, some judges and civil rights groups have expressed skepticism about algorithmic accuracy. For example, in *Loomis*, Judge Abrahamson's concurring opinion notes that COMPAS may serve as a useful tool for sentencing considerations, but the "court's lack of understanding of COMPAS was a significant problem in the instant case" because few questions could be answered about how the algorithm worked, and it was unclear as to whether the algorithm made a true individualistic determination.[158] Additionally, the Leadership Conference on Civil and Human Rights has also suggested that algorithms can be beneficial to the criminal justice system but only if the models

151. *See Chubbs,* 2015 WL 139069, at *6.

152. *Id.* at *9.

153. *Chubbs* cannot be cited in California because it is an unpublished opinion. *See* CAL. R. CT. 8.1115(a) ("[A]n opinion of a California Court of Appeal . . . that is not certified for publication or ordered published must not be cited or relied on by a court or a party in any other action.").

154. *See* Wexler, *supra* note 30, at 1360–61, 1360 n.71.

155. *See, e.g.*, State v. Belen, No. 2017AP293-CRNM, 2018 Wisc. App. LEXIS 191, at *11 n.5 (Wis. Ct. App. Feb. 14, 2018) (allowing the sentencing court to consider the defendant's COMPAS score following a conviction of child neglect resulting in death because the score was only reviewed, not discussed); State v. Parrish, No. 2017AP1442-CRNM, 2018 Wisc. App. LEXIS 316, at *2 n.2 (Wis. Ct. App. Mar. 5, 2018) (affirming the trial court's decision to follow the presentence investigation report's sentencing recommendation because the report was not a determinative factor).

156. *See* State v. Hurt, 2017AP1660-CR, 2018 WL 11430435, at *1 (Wis. Ct. App. Nov. 21, 2018) (noting that COMPAS can be used at sentencing subject to certain limitations).

157. *See, e.g.*, Cary Coglianese & David Lehr, *Transparency and Algorithmic Governance*, 71 ADMIN. L. REV. 1, 1, 34 (2019) (arguing that full algorithm disclosure is not required—even when algorithms are outcome determinative—because true transparency is satisfied by the contractors' explanation of the algorithm's "purpose, design, and basic functioning").

158. State v. Loomis, 881 N.W.2d 749, 774–75 (Wis. 2016) (Abrahamson, J., concurring).

(1) are independently validated; (2) can be challenged by defendants; and (3) are available for public scrutiny in terms of design, structure, and accuracy.[159]

The criminal justice system in the United States is based on the premise that "it is far worse to convict an innocent man than to let a guilty man go free."[160] Allowing for sentencing decisions based on algorithms that may falsely identify the risk level of defendants in up to 30% of cases seems directly contrary to this notion of justice. As is evident in *Loomis*, courts do consider algorithms when issuing sentencing decisions.[161] Moreover, predictive policing algorithms used before and during crime investigations have the potential to contribute to the confirmation bias of unquestioned algorithm reliability. Academics have also challenged location-based predictive policing tools that break cities into block-by-block districts to predict when crimes might occur based on historical data.[162] And investigative reporters are still finding new uses of predictive policing tools that have not been publicly disclosed.[163] Given the level of importance placed on such algorithms, it should be apparent that statistical accuracy should be an important consideration prior to algorithm implementation. Otherwise, such decisions will only reinforce public confidence in risk scores that have not been fully validated and are based on standards well-below scientifically accepted confidence intervals.[164]

1. Access Denied

In *Loomis* and *Chubbs*, the Wisconsin Supreme Court and the California Court of Appeals, respectively, considered whether to permit disclosure of algorithmic models.[165] Many algorithmic models are considered "black boxes," or systems whose inputs and outputs may be known but whose internal

159. *See* Greg Chaney, *The Criminal Justice System's Algorithms Need Transparency*, LAW360 (Mar. 31, 2019, 8:02 PM), https://www.law360.com/articles/1143086/the-criminal-justice-system-s-algorithms-need-transparency.

160. *See In re Winship*, 397 U.S. 358, 372 (1970) (Harlan, J., concurring).

161. *See Loomis*, 881 N.W.2d at 767–69.

162. The most common locational algorithm is PredPol, which updates its predictions throughout the day. *See* Will Douglas Heaven, *Predictive Policing Algorithms Are Racist. They Need To Be Dismantled.*, MIT TECH. REV. (July 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/.

163. *See, e.g.*, Ali Winston, *Palantir Has Secretly Been Using New Orleans To Test Its Predictive Policing Technology*, THE VERGE (Feb. 27, 2018, 3:25 PM), https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd (discussing the New Orleans Police Department's use of Palantir for data mining to predict which individuals may commit violent crimes—a use City Council members were not even aware of).

164. *See supra* Subpart I.B.3.

165. *See Loomis*, 881 N.W.2d at 763–64, 768, 771 (finding that the COMPAS model did not have to be disclosed because it was not the sole factor in sentencing); People v. Superior Court (*Chubbs*), No. B258569, 2015 WL 139069, at *5–9 (Cal. Ct. App. Jan. 9, 2015) (determining that requiring algorithm disclosure would be a violation of California's trade secret law).

workings are unknown.[166] These models use information in an unknown manner to produce results or predictions that appear facially neutral but may actually yield discriminatory results.[167]

Aside from the black box algorithmic models, the inputs and outputs of data used by the algorithmic models can also be problematic. Algorithms are trained to operate based on real-world facts. If the inputs an algorithm relies on are inherently biased, then the resulting outputs are also likely to be biased.[168] Because algorithms often rely on established data and statistician-determined inputs,[169] the inputs have potential to exacerbate racial disparities if statisticians fail to revise underlying algorithmic models reliant upon existing criminal statistics. Thus, the algorithmic models may be facially neutral but still generate unintentional race-based discrepancies.[170]

Ultimately, criminal defendants are unable to challenge what appear to be algorithmic model defects without some form of access to the underlying information. Advocates for opening algorithmic black boxes to partial disclosure cite studies indicating patterns of bias, inaccurate predictions, and discrimination.[171] Data scientist Cathy O'Neil has continuously found that mathematical models are not free of bias and instead reinforce discrimination, especially where race and lower socioeconomic status are concerned, because algorithms are designed for the masses instead of tailored to individual characteristics.[172] For example, O'Neil notes that algorithm developers can influence the concentration of law enforcement officers in minority neighborhoods by using arrest data from specific areas instead of the relevant jurisdiction as a whole.[173] This may seem unlikely at first glance, but ZIP code reliance can provide significant information that algorithms rely on for predictive outcomes.[174]

166. The issue of the "black box" has been ongoing for over a decade. *See, e.g.*, Elizabeth A. Rowe, *Striking a Balance: When Should Trade-Secret Law Shield Disclosures to the Government?*, 96 IOWA L. REV. 791, 826–35 (2010) (addressing when the government can request disclosure of "black box" algorithms).

167. *See* Anupam Chander, *The Racist Algorithm?*, 115 MICH. L. REV. 1023, 1024–25 (2017).

168. *Id.*

169. *See generally supra* Subpart I.B for a discussion on how algorithms are developed.

170. *See supra* notes 63–66 and accompanying text.

171. *See supra* Subpart I.B.3.

172. *See* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 24–27 (2016).

173. Cathy O'Neil, The Era of Blind Faith in Big Data Must End (Apr. 2017) (transcript available at https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end?language=en).

174. For instance, in the marketing context, by using propensity models to determine the likelihood of certain outcomes, ZIP codes allow algorithms to make determinations about income, education level, family composition, and lifestyle to such an extent that vendors can alter online pricing and availability based on shopper locations. *See* Katherine Noyes, *Will Big Data Help End Discrimination—or Make it Worse?*, FORTUNE (Jan. 15, 2015, 3:16 PM), https://fortune.com/2015/01/15/will-big-data-help-end-discrimination-or-make-it-worse/ (noting that ZIP codes often serve as proxies for advertising tactics that provide numerous insights beyond location).

Whether intentional or not, relying on such data in the criminal justice system without proper testing and verification procedures may create biased and discriminatory outcome predictions[175] and, in some instances, erroneous results.[176] Indeed, the *ProPublica* study, even when criminal history, recidivism, gender, and age were isolated, confirmed bias and discrimination in the COMPAS algorithm in finding that Black defendants were 77% more likely than Whites to be identified as high-risk for likelihood of committing a future violent crime.[177] Even if the COMPAS algorithmic model does not explicitly consider race, it may consider ZIP code, thus providing a possible explanation for the racial disparities.

Another study conducted by Megan Stevenson found that Kentucky's implementation of mandatory algorithm review before judges decide whether to hold a criminal defendant in jail before trial resulted in an increase in the number of White defendants being released within three days of booking while the percentage of Black defendants released within three days of booking remained essentially the same—a change that effectively created new inequities that were not present in the Kentucky bail system prior to the algorithm.[178] One possible explanation for this change could be attributed to population density as rural area judges granted release without bail more often than urban communities, the latter of which contain more diverse populations.[179] A different explanation based on a formal academic study, however, indicated that judges were more likely to impose bail as a condition for release for moderate-risk defendants who were Black and of lower socioeconomic status despite the default recommendation that bond be waived.[180] This study asked 340 judges to decide sentences for hypothetical defendants based on drug charges, with half of the cases including formal risk assessment information.[181] Even after

175. *See Criminal Justice Facts*, THE SENT'G PROJECT, https://www.sentencingproject.org/criminal-justice-facts/ (last visited Oct. 6, 2022) (noting that White men have a 1 in 17 probability of imprisonment while Black men and Latino men have a 1 in 3 and 1 in 6 chance, respectively, and that White women have a 1 in 111 probability of imprisonment while Black women and Latino women have a 1 in 18 and 1 in 45 chance, respectively.).

176. *See, e.g.*, *New Orleans Metropolitan Crime Commission Calls Arnold Foundation Public Safety Assessment "Flawed" as the Pretrial Justice Institute Attempts To Pivot Again*, AM. BAIL COAL. (Jul. 9, 2019), https://ambailcoalition.org/new-orleans-metropolitan-crime-commission-calls-arnold-foundation-public-safety-assessment-flawed-as-the-pretrial-justice-institute-attempts-to-pivot-again/ (detailing the New Orleans Metropolitan Crime Commission's findings that the Arnold Foundation's public safety risk assessment algorithm recommended free bond release for "75 percent of violent felony suspects and 93 percent of weapons felony suspects").

177. *See* Angwin et al., *supra* note 105.

178. Megan Stevenson, *Assessing Risk Assessment in Action*, 103 MINN. L. REV. 303, 362–366 (2018).

179. *Id.* at 309; *see also* Tim Simonite, *Algorithms Should've Made Courts More Fair. What Went Wrong?*, WIRED (Sep. 5, 2019, 7:00 AM), https://www.wired.com/story/algorithms-shouldve-made-courts-more-fair-what-went-wrong/.

180. *See* Jennifer Skeem et al., *Impact of Risk Assessment on Judges' Fairness in Sentencing Relatively Poor Defendants*, 44 LAW & HUM. BEHAV. 51, 53 (2020).

181. *Id.* at 52–53.

controlling for gender and race, the likelihood of incarceration was higher for poorer defendants, which may correlate with race.[182]

These studies are troubling because criminal justice algorithms, which are meant to ensure a fairer system, can create underlying bias and discrimination absent proper disclosure and testing in at least two ways, with the potential for overlap. First, if the algorithm is based on data that is not publicly available for bias testing and is subject to trade secret protection, sentencing judges may be overly reliant on algorithmic data predictions that have built-in discriminatory factors. Second, risk assessment scores can alter judicial discretion in the criminal sentencing context to make disparities worse, especially for Black defendants and defendants of lower socioeconomic status. To combat these problems, researchers suggest allowing for data-integrity checks to account for bias and reconsidering definitions of success to include occurrences outside of the status quo.[183] But to date, a significant number of jurisdictions continue to adopt algorithms without taking these precautionary steps.

2. State v. Pickett

Most recently, a New Jersey state court recognized these values and concerns. In the closely watched case of *State v. Pickett*,[184] the New Jersey Superior Court considered a request by a criminal defendant accused of murder to gain access to the TrueAllele source code used by the state's expert in rendering testimony concerning the likelihood that the defendant's DNA had been present at the scene of the murder. The defendant expressed concern that the computer program and underlying methodology the state's expert used was untested and potentially unreliable, and that "peer reviewed" articles offered to support the program were authored or funded by the expert or his organization.[185] At a *Frye* hearing (similar to a *Daubert* hearing), the trial court denied the defendant access to the software's source code and related documentation.[186]

As relevant to our negotiated approach, outlined *infra* in Subpart III.D, the parties in *Pickett* reached an impasse when trying to negotiate the terms of a protective order for source code.[187] The defendant agreed to a prohibition on disclosure to any individual with "any direct or indirect commercial or

182. *Id.* at 56; *see also* U.S. CENSUS BUREAU, REAL MEDIAN HOUSEHOLD INCOME BY RACE AND HISPANIC ORIGIN: 1967 TO 2017, https://www.census.gov/content/dam/Census/library/visualizations/2018/demo/p60-263/figure1.pdf (last visited Jul. 29, 2020) (showing that the median household income for all races combined is just over $60,000 per year, but for Blacks, it is just over $40,000 per year).

183. *See* O'NEIL, *supra* note 172, at 205–18.

184. State v. Pickett, 246 A.3d 279 (N.J. Super. Ct. App. Div. 2021).

185. *Id.* at 287, 291–92.

186. *Id.* at 283, 291.

187. *Id.* at 290.

employment interest in competing software products" and to certain other safeguards.[188] However, the prosecution insisted on additional and more expansive protections, including a requirement that the software be reviewed only at the prosecutor's office in a supervised inspection and permitting only handwritten notes on the 170,000 lines of code (a process which was estimated to take eight years to enable understanding the code).[189] Then there were the financial terms: a $1,000,000 automatic civil liability "in the event that the proprietary materials are improperly handled, negligently or otherwise" and $3,000,000 defense liability coverage.[190]

On appeal, the defendant contended that the source code and documentation were necessary to his defense and should be discoverable notwithstanding a claim that they contained trade secrets.[191] The parties and amici, including the ACLU, the Innocence Project, the Legal Aid Society, various bar associations, and other interested groups, submitted extensive briefing.[192] The appellate court held, consistent with some rulings from other jurisdictions, that if the state chooses to use an expert who relies on particular novel software to develop or support its conclusions to be offered at trial, then, upon a showing of particularized need, the defendant is entitled, under a suitable protective order, to access the software's source code.[193] In addition, supporting software development and related documentation (including documentation pertaining to "testing, design, bug reporting, change logs, and program requirements") was also needed to challenge the reliability of the software.[194] According to the court, "[a] criminal trial where the defendant does not have 'access to the raw materials integral to the building of an effective defense' is fundamentally unfair."[195]

While recognizing that the owner of a trade secret who establishes that the requested information is in fact a trade secret may refuse to disclose it, the court found that this privilege is not absolute.[196] The burden fell on the defendant seeking access to show:

> (1) whether there is a rational basis for ordering [production of] the information sought . . . ; (2) the specificity of the information sought; (3) the available means of safeguarding the company's intellectual property, such as

188. *Id.* at 290.
189. *Id.* at 309.
190. *Id.*
191. *Id.* at 291–92.
192. *Id.* at 292–98.
193. *Id.* at 284.
194. *Id.*
195. *Id.* at 299 (alteration in original) (quoting *In re* A.B., 99 A.3d 782, 790 (N.J. 2014)).
196. *Id.* at 300.

> issuance of a protective order; and (4) any other relevant factors unique to the facts of the case.[197]

The court found that the defendant had satisfied that burden.[198] The case was remanded, finding that "[a]nything less than full access contravenes fundamental principles of fairness, which indubitably compromises a defendant's right to present a complete defense."[199] The trial court was directed to compel disclosure of the source code and related materials "pursuant to an appropriate protective order."[200]

3. Special Constitutional Concerns for Criminal Justice?

Scholars have raised concerns about possible due process violations as algorithms have moved into virtually every sector of government decision-making.[201] The Fifth and Fourteenth Amendments provide that no person can be deprived "of life, liberty, or property, without due process of law" by the federal government or state governments, respectively.[202] As an extension of the Due Process Clause, the Sixth Amendment entitles a criminal defendant to the right to confront witnesses against him,[203] which is applicable to states as a result of ratification of the Fourteenth Amendment[204] and the Supreme Court's adoption of a selective incorporation approach where the Bill of Rights is concerned.[205] In general, unless a declarant is unavailable and the defendant had a prior opportunity to cross-examine the declarant, the Supreme Court has held that testimonial statements of witnesses absent from trial must be excluded

197. *Id.* at 284.

198. *Id.*

199. *Id.* at 311.

200. *Id.*

201. *See, e.g.*, Brauneis & Goodman, *supra* note 30, at 103–04, 128–29; Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1254 (2008); Ryan Calo & Danielle Keats Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 EMORY L.J. 797, 805 (2021); John Villasenor & Virginia Foggo, *Artificial Intelligence, Due Process, and Criminal Sentencing*, MICH. ST. L. REV. 295 (2020); Wexler, *supra* note 30; SLOBOGIN, *supra* note 30; Graves & Katyal, *supra* note 30, at 1376–81.

202. U.S. CONST. amends. V, XIV.

203. U.S. CONST. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right . . . to be *confronted* with the witnesses against him . . . ." (emphasis added)).

204. U.S. CONST. amend. XIV; *see* Duncan v. Louisiana, 391 U.S. 145, 148–49 (1968) (noting that the question of whether a right contained within the Bill of Rights shall be incorporated to be applicable to the States depends upon whether the right is among those "fundamental principles of liberty and justice which lie at the base of all our civil and political institutions;" whether the right is "basic in our system of jurisprudence;" and whether the right is "a fundamental right, essential to a fair trial" (first quoting Powell v. Alabama, 287 U.S. 45, 67 (1932); then quoting *In re* Oliver, 333 U.S. 257, 273 (1948); and then quoting Gideon v. Wainwright, 372 U.S. 335, 343–44 (1963))).

205. *See* Pointer v. Texas, 380 U.S. 400, 403 (1965) (holding that "the Sixth Amendment's right of an accused to confront the witnesses against him is likewise a fundamental right and is made obligatory on the States by the Fourteenth Amendment").

from evidence because of the defendant's rights under the Confrontation Clause.[206]

Nevertheless, whether the confrontation right applies to algorithms and outside of a trial[207] (e.g., pretrial or posttrial) is a very complex issue. Courts have held that machines do not count as hearsay declarants, so the confrontation right does not attach. As one commentor notes, "Under the machine-generated testimony doctrine, courts across the nation have held that machine-generated data does not trigger the Confrontation Clause because it is the machines—not the analysts operating them—that make the statements at issue, and machines are not 'witnesses' within the meaning of the Confrontation Clause."[208]

As studies have suggested, algorithm use in the criminal justice system has disproportionately impacted racial minorities and those of lower socioeconomic status,[209] which some argue should be considered a due process violation since they rely on generalized information not tailored to the individual's life and characteristics. For instance, Sonja B. Starr has argued that statistical sentencing based on specific characteristics is unconstitutional because use of group tendencies as a proxy for individual characteristics should not be constitutionally permissible.[210] That does not, however, appear to be a widely adopted view, as generalized information is routinely used for forensics and sentencing.[211]

While similar due process arguments have been made with respect to the disclosure issue, many defendants have been unsuccessful in challenging forensic algorithm use without disclosure as a due process violation.[212] The Supreme Court has cautioned that:

---

206. Crawford v. Washington, 541 U.S. 36, 59 (2004). *But see* FED. R. EVID. 804(b) (detailing exceptions to the rule against hearsay).

207. *See* 2 BARBARA E. BERGMAN ET AL., WHARTON'S CRIMINAL EVIDENCE § 6:10 (15th ed. 2017).

208. Brian Sites, *Rise of the Machines: Machine-Generated Data and the Confrontation Clause*, 16 COLUM. SCI. & TECH. L. REV. 36, 51 (2014).

209. *See* Angwin et al., *supra* note 105 (finding that even when criminal history, recidivism, gender, and age were isolated from the COMPAS study, Black defendants were still 77% more likely to be flagged for higher risk of future violent crime); Simonite, *supra* note 179 (noting a study showing that the use of risk-assessment tools resulted in harsher rates of incarceration for defendants of lower socioeconomic status).

210. Starr, *supra* note 66, at 827–28.

211. *See, e.g.*, Rebecca Foxwell, *Risk Assessments and Gender for Smarter Sentencing*, 3 VA. J. CRIM. L. 435, 454 (2015).

212. *See, e.g.*, State v. Loomis, 881 N.W.2d 749, 760–65, 771 (Wis. 2016) (denying the defendant's due process challenge to the court's failure to disclose the COMPAS algorithm because the risk assessment score was not the determinative factor regarding whether the defendant received an individualized sentence, and COMPAS has the *potential* to provide courts with more information). In another case, a court denied the defendant's due process challenge to a Confrontation Clause violation as a result of a DNA matching algorithm source code being withheld because under the specific facts of the case, the source code was not a declarant since there was human input when utilizing the algorithm and the creator of the source code testified in court. *See* People v. Wakefield, 107 N.Y.S.3d 487, 494, 497–98 (App. Div. 2019). Despite this holding, the court noted that algorithmic source code reliance can raise legitimate questions concerning due process and artificial intelligence. *Id.*; *see also* Press Release, Am. Civ. Liberties Union of Virginia, ACLU Brief Challenges

> Assurances of secrecy are conducive to the transmission of confidences which may bear no closer relation to fact than the average rumor or item of gossip, and may imply a pledge not to attempt independent verification of the information received. The risk that some of the information accepted in confidence may be erroneous, or may be misinterpreted, by the investigator or by the sentencing judge, is manifest.[213]

Nonetheless, courts seem unwilling to resolve this issue in favor of disclosure.[214] Further, courts have not fully discussed the distinction between reviewing individual pieces of information fed into an algorithm as opposed to actual review of how the score itself was calculated, which may be relevant when trying to demonstrate the level of judicial reliance on a given risk assessment score.[215]

4. FOIA Disclosures Unlikely

For software developers creating algorithms for use within the criminal justice system, meeting the requirements of the Freedom of Information Act's ("FOIA") Exemption 4 is of critical importance because the trade secret exemption often serves as a primary mechanism for preventing public disclosure of algorithmic models in response to FOIA requests.[216] Because courts are often unwilling or unable to fully disclose information pertaining to algorithms, criminal defendants may try to obtain information through FOIA. However, our review and analysis of the cases revealed that these attempts have been largely unsuccessful.[217]

---

the Constitutionality of Virginia's Sex Offender Risk Assessment Guidelines (Oct. 28, 2003), https://acluva.org/en/press-releases/aclu-brief-challenges-constitutionality-virginias-sex-offender-risk-assessment; Brooks v. Commonwealth, No. 2540-02-3, 2004 Va. App. LEXIS 29, at *3 (Va. Ct. App. Jan. 28, 2004) (dismissing the Virginia ACLU's challenge to the risk assessment tool because the algorithm was only advisory in nature).

213. Gardner v. Florida, 430 U.S. 349, 359 (1977); *see also* Villasenor & Foggo, *supra* note 201, at 324.

214. *See* sources cited *supra* note 212. *But see* Flores v. Stanford, No. 18 CV 2468, 2019 U.S. Dist. LEXIS 160992, at *29–30 (S.D.N.Y. Sept. 20, 2019) (denying the defendant, who was the chairwoman of the New York State Board of Parole's, motion to dismiss the plaintiff's class action claim that parole procedures for juveniles potentially serving life sentences violate due process because if the plaintiff's allegations are true that the Parole Board does not review individual files before making parole determinations, which are based at least in part on risk assessment algorithms, then there is plausible evidence that the Parole Board does not provide juveniles with procedurally adequate opportunities for release such that the defendant's motion cannot be granted as a matter of law).

215. *See* DANIELLE KEHL ET AL., BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y, ALGORITHMS IN THE CRIMINAL JUSTICE SYSTEM: ASSESSING THE USE OF RISK ASSESSMENTS IN SENTENCING 22–23 (2017), https://dash.harvard.edu/handle/1/33746041.

216. 5 U.S.C. § 552(b)(4) (creating an exemption to the FOIA for information submitted to the government that is classified as a trade secret, confidential commercial information, or confidential financial information). For more background on FOIA and policy implications, see Mark Fenster, *The Transparency Fix: Advocating Legal Rights and Their Alternatives in the Pursuit of a Visible State*, 73 U. PITT. L. REV. 443 (2012).

217. The authors reviewed a sample size of nineteen cases from 2017 to 2019—cases prior to the adoption of the *Argus Leader Media* (Food Mktg. Inst. v. Argus Leader Media, 139 S. Ct. 2356 (2019)) standard. It revealed that 68% of FOIA requests were denied based on judicial rulings in favor of nondisclosure under

In fact, court decisions have upheld plea agreements where defendants have waived their rights to request information pertaining to their case under open government laws,[218] which seems contrary to FOIA's purposes, particularly if defendants are unaware that risk-assessment algorithms were used in making a guilt determination (e.g., based on predictive policing practices) or will be used during sentencing proceedings. This lack of transparency can be detrimental during the sentencing process because most risk assessment tools were originally designed for criminal rehabilitation purposes, and if a defendant is deemed ineligible for alternative treatment, incarceration results.[219] The same risk assessment score is often used to determine length of incarceration—with potential to significantly differ based on changes in a single risk factor—which defendants can rarely challenge.[220] Apprehension about algorithmic transparency has increased further after *Food Marketing Institute v. Argus Leader Media*, in which the Supreme Court held that information is exempt from FOIA so long as the information is treated as confidential and its owner has received assurance that the information will remain confidential.[221]

Another practical limitation of obtaining records through FOIA is that the government cannot give that which it does not possess. Therefore, to the extent private vendors retain ownership, control, and possession of their algorithmic models, records, and source codes, they remain beyond the reach of public records requests.[222] There are also FOIA exemptions that protect law-enforcement and court records.[223] Thus, even outside the FOIA context, criminal defendants have been unsuccessful in obtaining algorithmic models and other proprietary information during discovery because it was in possession of the developer (not the government) and claimed as a trade secret.[224]

Exemption 4. The sample was obtained by performing a Lexis Advance search for "FOIA" and "trade secrets" from January 1, 2017 through June 23, 2019. Forty-three results were returned, with twenty-four being excluded from the analysis due to trade secret disclosure not being a primary issue or because they were earlier decisions that were further discussed on appeal. (sample on file with authors).

218. *See, e.g.*, Caston v. Exec. Off. for the U.S. Att'ys., 572 F. Supp. 2d 125, 129 (D.D.C. 2008) (denying a FOIA request because the plaintiff voluntarily and intelligently waived his right to request information from any United States department or agency in a plea agreement); United States v. Lucas, 141 Fed. App'x 169, 170 (4th Cir. 2005) (affirming denial of a FOIA request because the petitioner waived his right to such requests in a plea agreement), *cert. denied*, 546 U.S. 1196 (2006).

219. Angwin et al., *supra* note 105.

220. *Id.*

221. Food Mktg. Inst. v. Argus Leader Media, 139 S. Ct. 2356, 2366 (2019).

222. *See* Brauneis & Goodman, *supra* note 30, at 135.

223. 5 U.S.C. § 552(b)(7). *See generally* Brauneis & Goodman, *supra* note 30, at 160–61.

224. *See, e.g.*, State v. Kuhl, 741 N.W.2d 701, 708–09 (Neb. Ct. App. 2007).

II. THE TENSION BETWEEN TRADE SECRECY AND PUBLIC TRANSPARENCY

It is axiomatic that trade secrecy is built for secrecy, not openness. It is built for competitors in the private sector environment to protect their private property, not the public interest in having access to such information.[225] In the context of calls for greater public transparency, this tension between trade secrecy and government transparency has been lamented by scholars who note that trade secrecy has changed from protecting against a competitor's misappropriation to a shield protecting the proprietor from public investigation.[226] Nonetheless, the situation is more nuanced. We view the trade secrecy framework as presenting both the problem and the solution when it comes to disclosure. While trade secret law requires some degree of secrecy, it also permits alienability and sharing of secrets under contractual terms structured (within limits) by the parties and designed to serve the unique needs of the parties.

For instance, trade secret litigation routinely occurs in courts while observing the public right of access to court filings and proceedings and the protection of the litigants' trade secrets. The right of access is firmly entrenched in the law throughout the United States.[227] At the same time, there are protections available under the federal Defend Trade Secrets Act (DTSA)[228] and the Uniform Trade Secrets Act (UTSA)[229] to safeguard trade secrets from disclosure during litigation, which serve as qualifications on the public's right of access to court proceedings. Thus, even in trade secret misappropriation cases, there is tension between the qualified right of public access and the litigants' need to protect the confidentiality and value of their trade secrets.

The qualified right to public access can be overcome "only by an overriding interest based on findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest."[230] The protection of trade secrets has long been recognized as one of these overriding interests that justifies an exception to this right. Indeed, the Supreme Court has recognized that "sources of business information that might harm a litigant's competitive standing" are exempted from public disclosure.[231]

225. *See* Graves & Katyal, *supra* note 30, at 1342.

226. *See, e.g.*, Katyal, *supra* note 30, at 1246–47.

227. *See* Press-Enter. Co. v. Superior Ct., 478 U.S. 1, 8 (1986).

228. 18 U.S.C. §§ 1835–1836.

229. UNIF. TRADE SECRETS ACT § 5 (UNIF. L. COMM'N amended 1985).

230. *Press-Enter. Co.*, 464 U.S. at 510; *see* Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 606–07 (1982) ("Where, as in the present case, the State attempts to deny the right of access in order to inhibit the disclosure of sensitive information, it must be shown that the denial is necessitated by a compelling governmental interest, and is narrowly tailored to serve that interest.").

231. Nixon v. Warner Commc'ns, 435 U.S. 589, 598 (1978).

Trade secret rights potentially apply to the technologies discussed in this Article and protect data, software, and algorithms in these technologies. In general, trade secret rights cover operability and functionality of devices, and algorithmic models are often within one of these categories.[232] In fact, these rights are sufficiently strong that putative trade secret owners may refuse to reveal the protected information, even to the government.[233] Developers are also cautious because with trade secrecy, others may lawfully attempt to reverse engineer the software unless prohibited by contract. Further, trade secret rights are destroyed if improperly disclosed, and trade secret owners are required to take reasonable efforts to protect information that they deem a trade secret; courts typically expect such efforts, at a minimum, will include nondisclosure agreements.[234]

A combination of trade secrecy and contract law through licensing agreements can be a powerful combination for controlling proprietary information.[235] This is why developers and private vendors rely not only on their property rights but often insist on contracts that contain confidentiality and nondisclosure limitations. Accordingly, while it is not often acknowledged, there are weighty rights and constitutional concerns on both sides that make this trade secret "problem" a thorny conundrum, and any thoughtful solutions must recognize and wrestle with the legitimate arguments and interests on both sides.

A. Built for Competitive Environment

As originally conceptualized (and in much of the world outside of the United States), the protection of business secrets is grounded in the "maintenance of business ethics and the prevention of unfair competition."[236] Along with the present-day recognition of trade secrets as a form of intangible property, the unfair competition aspects of trade secret law remain an important part of its genetics, as evidenced by the elements of a trade secret misappropriation claim.[237] Further, most trade secret cases involve misappropriation by former employees or business competitors.[238] Strikingly, the circumstances presented in these government-vendor cases, however, are not that. Instead, they represent an attempt between noncompetitors to keep

232. *See generally* LIFESCIENCE ALLEY, LONG COMMENT REGARDING A PROPOSED EXEMPTION UNDER 17 U.S.C. 1201, at 5 (2015), https://www.copyright.gov/1201/2015/comments-032715/class%2027/LifeScience_Alley_Class27_1201_2014.pdf.

233. *See* Rowe, *supra* note 166, at 793–94.

234. *See* ELIZABETH A. ROWE & SHARON K. SANDEEN, TRADE SECRET LAW: CASES AND MATERIALS 199–201 (3d ed. 2020).

235. *See* Elizabeth A. Rowe, *Sharing Data*, 104 IOWA L. REV. 287, 303 (2018).

236. *See* ROWE & SANDEEN, *supra* note 234, at 21.

237. *See generally id.* at 281–82.

238. *Id.* at 300.

the nature of their business dealings secret from the public (even when the public is paying for the service or product).[239]

B. For Developers, Algorithms and Data are Property

For the purposes of this Article, it is important to bear in mind that it is not only criminal defendants who have constitutional rights to be considered in this debate but also trade secret owners. A case that is frequently cited for the proposition that trade secrets are a form of private property is *Ruckelshaus v. Monsanto Co.*[240] In *Ruckelshaus*, the Supreme Court considered whether certain provisions of the Federal Insecticide, Fungicide, and Rodenticide Act were unconstitutional.[241] Monsanto argued that the provisions of the law that required it to disclose certain information and data were unconstitutional because they amounted to a property taking without just compensation in violation of the Fifth Amendment to the U.S. Constitution.[242] To succeed on its claim, Monsanto had to first establish it had a property interest in the information. In finding a property interest in Monsanto's data, the Court in *Ruckelshaus* explained:

> Because of the intangible nature of a trade secret, the extent of the property right therein is defined by the extent to which the owner of the secret protects his interest from disclosure to others. Information that is public knowledge or that is generally known in an industry cannot be a trade secret. If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished.[243]

Although it is clear from the language of *Ruckelshaus* that the Supreme Court limited its holding to information that qualifies for trade secret protection, some scholars, like Pamela Samuelson,[244] expressed concern that the holding of *Ruckelshaus* might be used to claim property rights in lesser forms of information. This view remains a critical issue today, especially in the context relevant to this Article. It has become a particularly pressing issue in FOIA litigation where, due to the Supreme Court's decision in *Food Marketing Institute v. Argus Leader Media,*[245] businesses may believe that they have property-like rights in any information they deem confidential.

---

239. *See* Katyal, *supra* note 30, at 1247.

240. Ruckleshaus v. Monsanto Co., 467 U.S. 986 (1984).

241. *Id.* at 990.

242. *Id.* at 998–99.

243. *Id.* at 1002 (citations omitted).

244. *See* Pamela Samuelson, *Information as Property: Do* Ruckelshaus *and* Carpenter *Signal a Changing Direction in Intellectual Property Law?*, 38 CATHOLIC U. L. REV. 365, 365–68 (1989).

245. Food Mktg. Inst. v. Argus Leader Media, 139 S. Ct. 2356 (2019).

Thus, whether information is characterized as property can have real-world consequences, and when deciding whether information will be treated as property, context matters. Information that meets the definition of a trade secret is property to the extent it can be precisely defined and is maintained within the exclusive control of the putative trade secret owner.[246] Significantly, an emphasis on trade secrets as a property right leads to lesser importance and weight on the public interest in governmental transparency. This property rationale provides the underlying basis for the claim of "ownership" over the technologies, their data, algorithms, and practically anything else that can be captured by intellectual property and trade secrecy, even when they are serving government functions. As a result of the asserted right to exclude (or restrict access and disclosure), ShotSpotter does not want gunshot data disclosed,[247] and the developer of Stingrays does not want police departments to report their use or courts to know about and review them.[248] Similarly, CMI, Inc., the developer of Intoxilyzer, a breathalyzer device, refuses to disclose its source code.[249] Unsurprisingly, each of these developers argues that its source codes are protected by property rights under a trade secret theory.

C. No Robust Role for Public Interest in Governmental Transparency

The conception of trade secrets as property is fundamental to its design and underlying legal framework. This makes it almost antithetical to consideration of the public interest in governmental transparency.[250] As compared to the clarity of intellectual property rights, the "public interest" generally is murky and unsettled.[251] Indeed for the purposes of this Article, it should be noted plainly that there is no mechanism for robust consideration of "the public interest" in the U.S. trade secret framework, except in some rather limited circumstances that themselves are under-developed.[252] Other than whistleblower protections[253] and some First Amendment[254] exceptions, public

246. *See generally* Ramon A. Klitzke, *Trade Secrets: Important Quasi-Property Rights*, 41 BUS. L. 55 (1986).

247. *See* Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1283–84 (2020).

248. *See* Wexler, *supra* note 30, at 1366–67.

249. *See* Andrea Roth, *Trial by Machine*, 104 GEO. L.J. 1245, 1272 (2016).

250. As it pertains to this context, a more comprehensive discussion of the public interest and trade secrecy is beyond the scope of this Article.

251. *See, e.g.*, Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201, 1232–33 (2000).

252. *See, e.g.*, Sharon K. Sandeen & Ulla-Maija Mylly, *Trade Secrets and the Right to Information: A Comparative Analysis of E.U. and U.S. Approaches to Freedom of Expression and Whistleblowing*, N.C. J.L. & TECH., March 2020, at 1, 55; Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection,* 105 CALIF. L. REV. 1 (2017).

253. 18 U.S.C. § 1833.

254. *See, e.g.*, Elizabeth A. Rowe, *Trade Secret Litigation and Free Speech: Is It Time to Restrain the Plaintiffs?*, 50 B.C. L. REV. 1425, 1433 (2009); Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 808–11 (2007).

interest considerations most frequently arise (albeit in a relatively cursory fashion) in the consideration of equitable principles[255] for injunctive relief in trade secret misappropriation cases. Thus, for the purposes of this Article, we operationalize it as the public interest in governmental transparency. This public–secret tension is at the heart of any attempt to understand and better balance private interests in intellectual property with the public's right to information.[256] The tools used to effectuate that balance in litigation involve carefully constructed protective orders, but outside of the litigation context, the contractual approach—confidentiality agreements—as championed in this Article provides an *ex ante* tool for sharing trade secret information.

As some scholars have argued, the struggle for transparency from secrecy may be further exacerbated by developers' overclaiming their trade secret rights.[257] This is also not unusual in IP or unique to trade secrecy.[258] However, it is fundamentally the legal structure that provides this perceived thumb on the scale in favor of IP owners to the potential detriment of the public interest in governmental transparency. In the case of algorithms in the criminal justice system, the contractual nondisclosure agreements, coupled with asserted trade secret rights, reflect an example of intellectual property laws providing greater protection than contract law alone would provide.

How we define the public interest and what constitutes an exception to the weighty private property rights of trade secret owners is left open to debate and circumstances. Several states have recognized, for instance, that it is against the public interest to enter into settlement agreements that shield information about dangers to the public's health and safety.[259] Similar public policy carve-outs have also been made in the employment law area to permit whistleblowing by employees despite their having signed confidentiality agreements.[260] No such exception exists for trade secrets related to technologies in the criminal justice system, or even generally, technologies acquired from private vendors by government agencies for public decision-making or critical public functions.

To be sure, the best (though not perfect) option here would be for Congress to rule the kinds of contractual provisions that restrict disclosure in

255. *See* Elizabeth A. Rowe, *eBay, Permanent Injunctions, and Trade Secrets*, 77 WASH. & LEE L. REV. 553, 567 (2020).

256. *See* Sandeen & Mylly, *supra* note 252, at 55.

257. *See, e.g.*, Tanya Applin & Sharon K. Sandeen, *Trade Secrecy, Factual Secrecy and the Hype Surrounding AI*, *in* RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND ARTIFICIAL INTELLIGENCE (Ryan Abbott ed., forthcoming 2022) (on file with authors).

258. *See* Elizabeth A. Rowe, *Patents, Genetically Modified Foods, and IP Overreaching*, 64 SMU L. REV 859, 883–84 (2011).

259. *See* Elizabeth E. Spainhour, *Unsealing Settlements: Recent Efforts to Expose Settlement Agreements That Conceal Public Hazards*, 82 N.C. L. REV. 2155, 2158–61 (2004) (discussing state laws, like Florida's, that declare private settlements that conceal public hazards void as a matter of public policy).

260. *See* MARK A. ROTHSTEIN ET AL., EMPLOYMENT LAW § 8.9 (2d ed. 1999).

this context void as a matter of public policy.[261] According to the *Second Restatement of Contracts*, a contract is unenforceable for public policy reasons if either "legislation provides that it is unenforceable or the interest in its enforcement is clearly outweighed in the circumstances by a public policy against the enforcement of such terms."[262] Thus, in this instance, a legislature could deem that the public interest in promoting governmental transparency could outweigh the developers' interests in controlling the information made available about its product.

For example, the last time Congress considered and debated the balance between patent protection for seed producers and the public interest in research, it demonstrated a clear preference for and recognition of the importance of research.[263] In 1970, Congress expanded the intellectual property protection afforded to plants by enacting the Plant Variety Protection Act (PVPA).[264] Prior to the enactment of the PVPA, hybrid-seed companies enjoyed trade secret protection over the plant varieties they developed. The PVPA, through the issuance of a plant variety certificate, confers exclusive rights to breeders of certain sexually reproduced or tuber-propagated plant varieties.[265] Notably though, the Act contains a research exemption, explicitly providing that "[t]he use and reproduction of a protected variety for plant breeding or other bona fide research shall not constitute an infringement of the protection provided under this chapter."[266] Thus, it is possible that a similar type of legislative balance could be achieved in this context.

Along those lines, there is a recent, directly applicable example of what a legislator or legislature could do. Idaho Representative Greg Chaney proposed H.B. 118, which the Idaho legislature formally passed on March 28, 2019, that makes Idaho the first state to completely remove trade secret protections within the criminal justice system for pretrial risk assessment tools and also requires algorithmic transparency and open access to the public for "inspection, auditing, and testing" of those tools.[267] While a bold step, this legislation is nevertheless narrow in that it is limited to pretrial risk assessment tools. It therefore does not apply to many other algorithmic models such as evidence-generating software like ShotSpotter, DNA analysis software, or facial recognition software. There has also been some movement toward legislation at the federal level. Congressman Mark Takano has proposed the Justice in Forensic Algorithms Act. It aims to eliminate the trade secret evidentiary

261. Until that happens, courts (both state and federal) could also find that these contracts violate the public interest if there were a coherent doctrine on which to rely.

262. RESTATEMENT (SECOND) OF CONTS. § 178 (AM. L. INST. 1981).

263. *See* Rowe, *supra* note 258, at 865.

264. Plant Variety Protection Act, Pub. L. No. 91-577, 84 Stat. 1542 (1970).

265. 7 U.S.C. § 2402(a).

266. 7 U.S.C. § 2544.

267. IDAHO CODE § 19-1910 (2019).

privilege in criminal proceedings as well as create standards for algorithms used for evidence.[268] However, reading political tea leaves, one might expect it is unlikely to become law any time soon.[269]

III. THE FIT: PROCUREMENT POLICIES & CONTRACTING

With all these tensions, is there any possible fit or overlap between trade secrecy and governmental transparency? This Article answers in the affirmative: procurement and contracting. Just as the mismatch between trade secrecy and government–private ventures present obstacles to public disclosure, the trade secrecy framework also supports a potential solution.

Trade secret law is not designed to foster absolute secrecy. To the contrary, trade secret law is built "to solve Arrow's information paradox by facilitating the . . . sharing of information" in a manner that does not result in loss of the value of the information to its owner.[270] Importantly, the trade secret framework provides that the person now in possession of the owner's secret is still (contractually) restrained in their ability to use and to disseminate the information further.[271]

Contract law is thus central to our proposal. Contracts can balance the competing interests of secrecy and disclosure, and contractual negotiations between government agencies and private vendors is the means for achieving such balance on a transaction-by-transaction basis. Contracts are routinely used with trade secrecy to ensure confidentiality and nondisclosure.[272] At the same time, contractual provisions can also be used to set out the terms and conditions of any permissible disclosure. This may be a problem and a solution, though, since trade secret owners receive promises of confidentiality in procurement contracts. Therefore, until there are legislative pronouncements that express public policy goals and interests regarding the disclosure of algorithms in the public sphere, private contracting (consistent with government procurement principles) could be used to address the problem. We contend that it is possible to envision contract law as a means to simultaneously support greater sharing in this context while also protecting the rights of vendors.[273]

---

268. *See* Takano, *supra* note 44.

269. *See, e.g.*, *117 Legislative Outlook H.R. 2438*, LEXIS, https://plus.lexis.com/document/documentlink/?pdmfid=1530671&crid=28f14df7-3387-45ba-9942-02ae22a38a08&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A62DF-5H01-JSXV-G38W-00000-00&pdcontentcomponentid=133053&pdproductcontenttypeid=undefined&pdiskwicview=false&pdpinpoint=&ecomp=7gktk (last visited Sept. 17, 2022).

270. *See* ELIZABETH A. ROWE & SHARON K. SANDEEN, TRADE SECRECY AND INTERNATIONAL TRANSACTIONS: LAW AND PRACTICE 66 (2015).

271. *See id.*

272. *See id.* at 66–67.

273. *See* Matwyshyn, *supra* note 50, at 5 (arguing that contract law can be used as a means to protect consumer privacy).

Government procurement is a necessity for societal functioning. At every level of government, officials and agencies contract for goods and services that cannot be provided in-house, whether due to employee shortages or limitations on requisite skill sets. As aptly characterized by Danielle Conway, however, procurement law is complex and dynamic.[274] Governmental authority to enter into contracts is derived from the Engagements Clause of the Constitution,[275] which the Supreme Court has held to be a valid exercise of constitutional authority.[276] Government procurement increases access to marketplace services with industry specialists and often reduces costs while simultaneously improving quality through the creation of competition.[277] For many decades, federal and local government agencies have been major purchasers of goods and services such as weapons, airplanes, office supplies, and infrastructure construction. Indeed, the government is the largest purchaser of goods and services.[278] In 2020, the federal government alone spent over $665 billion, and of that, over $14 billion was spent on technology products and services.[279]

Because public funds pay for government contracts, government procurement is subject to additional regulations beyond what is required in private contracts. For example, unlike private agreements where principals and agents may enter into contracts, only designated officers can legally bind the government through procurement efforts. Federal law requires agency leaders to establish and maintain procurement management programs to select, appoint, and terminate contracting officers.[280] Once selected or appointed, contracting officers have federal authority to "enter into, administer, or terminate contracts" which bind the government but only to the extent of the particular officer's authority.[281] Additionally, before entering into a contract, the government must publicize contract actions, provide for full and open competition, verify contractor qualifications, describe agency needs, and maintain specific records.[282]

---

274. DANIELLE M. CONWAY, STATE AND LOCAL GOVERNMENT PROCUREMENT, at xiii (2012).

275. U.S. CONST. art. VI, cl. 1.

276. United States v. Tingey, 30 U.S. 115, 128 (1831) ("[W]e are of opinion that the United States have such a capacity to enter into contracts.").

277. *See generally* KATE M. MANUEL ET AL., CONG. RSCH. SERV., R42826, THE FEDERAL ACQUISITION REGULATION (FAR): ANSWERS TO FREQUENTLY ASKED QUESTIONS (2015), https://fas.org/sgp/crs/misc/R42826.pdf.

278. *Id.* at 1.

279. *A Snapshot of Government-Wide Contracting for FY 2020*, U.S. GOV'T ACCOUNTABILITY OFF. (June 22, 2021), https://www.gao.gov/blog/snapshot-government-wide-contracting-fy-2020-infographic.

280. 41 U.S.C. §§ 1702(b)(3)(G), 3102; 48 C.F.R. § 1.603-1 (2016).

281. 48 C.F.R. § 1.602-1 (2022).

282. *See* 41 U.S.C. § 1710 (detailing the process and requirements for transitioning from an agency-performed function to contractor performance); 41 U.S.C. § 1712 (describing record requirements where contracting and procurement are concerned); 41 U.S.C. § 1303 (explaining the Federal Acquisition Regulation); 48 C.F.R. §§ 1–53 (further detailing the Federal Acquisition Regulation, which sets forth the federal procurement process; describes best practices, procedures, and requirements for agencies; and provides standard clauses and forms).

Government agencies' use of private vendors to perform government functions, for better or worse, has become commonplace.[283] Public contracting for agency management services related to policy, rulemaking, and decision-making processes are exempted from standard administrative procedures that would otherwise govern decisions of policy; general rulemaking procedures require publication in the Federal Register, a notice-and-comment period, and a statement of authority, but contracting does not require these things.[284] Therefore, existing agency practices of adopting AI frequently remain concealed and are not subject to public review.[285] This is due to the accompanying practices that are integral to the private commercial marketplace, including contracting and trade secrecy protective measures, but which have raised a host of concerns to scholars.[286] For instance, Danielle Citron notes that "the public . . . [and] government actors are unable to influence policy when it is shrouded in closed code."[287]

A. Contracting for Algorithms & AI

Similar to private entities, government agencies are also consumers of technology, albeit on a larger scale. Indeed, at nearly every level of government, agencies purchase or contract for AI services that rely on patterns and remove official or agent discretion from decision-making processes.[288] Proponents of AI procurement argue that government agencies often lack staff with the requisite capabilities to participate in AI research and development.[289] While this is likely a realistic assessment of lacking government capacity to develop complex algorithms, public policy warrants recognition of the fact that developers often keep relevant code secret, and agency staff and officials are likely unable to assess technological design for the same reasons that they cannot develop AI.[290] Additionally, officials in favor of procurement often view

283. *See, e.g.*, Deepa Varadarajan, *Business Secrecy Expansion and FOIA*, 68 UCLA L. REV. 462, 465 (2021); GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY (Jody Freeman & Martha Minnow eds., 2009); Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367, 1369 (2003).

284. *See* 5 U.S.C. § 553(a)(2) (pertaining to exclusion); 5 U.S.C. § 553(b) (pertaining to default agency rules).

285. *See* Deirdre K. Mulligan & Kenneth A. Bamberger, *Procurement as Policy: Administrative Process for Machine Learning*, 34 BERKELEY TECH. L.J. 773, 780 (2019).

286. *See, e.g.*, Varadarajan, *supra* note 283, at 465–66; David S. Levine, *The Impact of Trade Secrecy on Public Transparency, in* THE LAW AND THEORY OF TRADE SECRECY 406, 407 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011); FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015); Danielle Keats Citron, *Open Code Governance*, U. CHI. LEGAL F. 355, 356–57 (2008).

287. Citron, *supra* note 201, at 1290–91.

288. *See* Mulligan & Bamberger, *supra* note 285, at 788.

289. *See* Jenna Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, BIG DATA & SOC'Y, Jan.–June 2016, at 1, 4; Mulligan & Bamberger, *supra* note 285, at 789.

290. *See* Burrell, *supra* note 289, at 4; Mulligan & Bamberger, *supra* note 285, at 789.

AI technologies as a new way to fulfill agency missions through what is viewed as administrative technologies.[291]

Despite what appears to be an increased preference for predictive algorithms, federal regulation of AI has largely been focused on self-driving autonomous vehicles, aviation, and war-related functions,[292] which suggests that AI contracts are subject to arguably outdated—or nonexistent—laws. Even on the state and local level, AI regulation has been limited and slow to keep up with government procurement needs. For instance, Robert Brauneis and Ellen Goodman's study found that many government agencies did not have significant records about the creation and implementation of algorithms and AI already in use.[293] They attributed the lack of records to agency failure to generate documents and contractor failure to provide documentation to governmental clients.[294]

Though AI contracting has been expeditious and regulation unhurried, some cities have taken an affirmative approach. For example, New York City was the first city to establish a task force to examine AI systems prior to adoption;[295] Oakland established a privacy commission to recommend best practices for AI adoption;[296] Seattle has allowed for public comment on AI surveillance technologies;[297] and Portland, Oregon adopted the Smart City PDX program to protect citizen privacy when AI is used.[298] Nevertheless, these examples serve as exceptions, not the current norm.

Perhaps one reason government agencies do not focus on transparency concerns is because of the proprietary interests of AI developers and the benefits that such programs provide. When AI produces the results that governmental officials want, such as fingerprinting, image identification, or DNA matching, few questions are likely to be raised about the validity of the methodology.[299] Indeed, AI developers who provide algorithms for the criminal justice system have a limited market: police investigators and government attorneys. This may put pressure on developers to produce results that law

---

291. *See* Mulligan & Bamberger, *supra* note 285, at 789.

292. *See* LIBR. OF CONG., 2018-016815, REGULATION OF ARTIFICIAL INTELLIGENCE IN SELECTED JURISDICTIONS 27–30 (2019).

293. Brauneis & Goodman, *supra* note 30, at 152.

294. *Id.*

295. *See* Press Release, City of New York, Mayor de Blasio Announces First-in-Nation Task Force to Examine Automated Decision Systems Used by the City (May 16, 2018), https://www1.nyc.gov/office-of-the-mayor/news/251-18/mayor-de-blasio-first-in-nation-task-force-examine-automated-decision-systems-used-by.

296. *See Privacy Advisory Commission*, CITY OF OAKLAND, https://www.oaklandca.gov/boards-commissions/privacy-advisory-board (last visited Oct. 9, 2022).

297. *See Surveillance Technologies Under Review*, CITY OF SEATTLE, https://www.seattle.gov/tech/initiatives/privacy/surveillance-technologies (last visited Oct. 11, 2020).

298. *See Using Data and Technology to Improve People's Lives*, SMART CITY PDX, https://www.smartcitypdx.com/ (last visited Oct. 11, 2020).

299. *See* Murphy, *supra* note 53, at 745–47.

enforcement agencies favor and prevent disclosure of their AI software, which might then result in independent third-party review.[300] (As we discuss later, the limited market also increases the government's bargaining power to negotiate its terms.) Further, after an agency has adopted an AI tool deemed to be valid and, better yet, that produces the desired results, there is little incentive for the agency to question the tool when doing so could provide evidence of algorithmic flaws.[301]

B. Existing Mechanisms for AI Review Are Not Sufficient

As the above processes reveal, government procurement of AI appears lacking in independent testing and verification prior to implementation. With facial recognition technology, for instance, some states and local governments have implemented their own laws,[302] leaving government procurement of AI highly discretionary and lacking in uniformity. Even at the federal level, government agencies are not subject to standard administrative rulemaking procedures when contracting is involved.[303]

Congressional and state regulation of government AI procurement does not have to be an all-or-nothing approach. As suggested by the Leadership Conference on Civil and Human Rights, AI can be beneficial for government agencies, including the criminal justice system, if certain standard requirements are in place.[304] For instance, prior to AI implementation, the Leadership Conference suggested independent validation, opportunities for defendant challenges, and public accessibility to AI design, structure, and accuracy tests to ensure accountability.[305] Because trade secrecy has been a limiting factor for public disclosure,[306] additional proposals could be considered as an attempt to

300. *See id.*

301. *See id.* at 746 ("So long as [police and prosecutors] remain satisfied, the [forensic method] laboratories need not engage in any new development or self-criticism.").

302. *See, e.g.*, OAKLAND, CAL., CODE §§ 9.64.010–.070 (2018); *see* Shirin Ghaffary, *San Francisco's Facial Recognition Technology Ban, Explained*, VOX (May 14, 2019, 7:06 PM), https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained; Nik DeCosta-Klipa, *Boston City Council Unanimously Passes Ban on Facial Recognition Technology*, BOSTON.COM (June 24, 2020), https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban; Taylor Hatmaker, *Portland Passes Expansive City Ban on Facial Recognition Tech*, TECHCRUNCH (Sept. 9, 2020, 7:45 PM), https://techcrunch.com/2020/09/09/facial-recognition-ban-portland-oregon/.

303. 5 U.S.C. § 553(a)(2)–(b).

304. *See* Chaney, *supra* note 159.

305. *See id.*

306. Algorithms and AI are generally not considered patentable material, so software developers often opt for trade secret protection. *See* Alice Corp. v. CLS Bank Int'l, 573 U.S. 208, 221–23 (2014) (holding that algorithms are abstract ideas ineligible for patent protection because using the claims on a computer is not enough to transform the algorithm into patentable subject matter); Diamond v. Diehr, 450 U.S. 175, 191 (1981) (holding that mathematical formulas in the abstract are not proper subjects eligible for patent protection). Public disclosure of trade secrets results in loss of trade secrecy, which is why developers are often hesitant to disclose the source code. *See* 18 U.S.C. § 1839(3). However, note that the DTSA does not preempt state law. *See* Rivendell Forest Prods., Ltd. v. Ga.-Pac. Corp., 28 F.3d 1042, 1046 (10th Cir. 1994)

balance AI developers' interests with public disclosure. In addition to the procurement approach outlined in this Article,[307] some scholars have suggested exclusive government contracts for which transparency could be a condition precedent, tax incentives, or an amendment to the exception for nondisclosure where government procurement is involved.[308]

C. Proposal Consistent with Procurement Policies

Our transaction-by-transaction procurement approach is consistent not only with trade secrecy law, but with existing federal procurement law and policy. While procurement tends to conjure government transactions based on awards to the lowest bidder, it is important to understand that procurement law and policies are fundamentally about more than just price.[309] Accordingly, these policies allow for the kind of flexibility that would permit government agencies to negotiate and contract for the kinds of terms (discussed below) that facilitate greater transparency. Indeed, the World Economic Forum's Guidelines for AI Procurement encourage consideration of trade secrecy protections for vendors with possibilities for facilitating transparency,[310] and our proposal could supplement those guidelines with additional specificity on how to achieve transparency within the confines of U.S. law. In sum, there are three features of procurement law that support our proposal: competitive negotiation, qualification, and collateral social and economic policies.

1. Competitive Negotiation

An underlying premise of procurement is that it will be achieved through full and open competition.[311] Accordingly, various procedures have been established in order to effectuate that goal. In addition to sealed bidding, Congress, through the Competition in Contracting Act, also added competitive negotiation as an alternative means of achieving full and open competition.[312] This was seen as an opportunity to introduce more flexibility in procurement procedures while maintaining the features that facilitate a competitive

("[A] trade secret can include a system where the elements are in the public domain, but there has been accomplished an effective, successful and valuable integration of the public domain elements and the trade secret gave the claimant a competitive advantage which is protected from misappropriation.").

307. *See infra* Subpart III.C.

308. *See* 5 U.S.C. § 553(a)(2) (stating that government contracting falls under the Administrative Procedure Act's exemption of matters relating to "agency management" or "to public property, loans, grants, benefits, or contracts"). *See generally* Wexler, *supra* note 30, at 1422–23.

309. *See* Schwartz, *supra* note 56, at 67–68.

310. WORLD ECON. F., GUIDELINES FOR AI PROCUREMENT 10 (2019), https://www3.weforum.org/docs/WEF_Guidelines_for_AI_Procurement.pdf.

311. *See* 41 U.S.C. § 3301.

312. *See id.*

process.[313] An agency thus has significant discretion to establish criteria other than price to be included in its solicitation or request for proposals (RFP).[314]

Unlike in a sealed bidding process where submissions by a contractor are either accepted or rejected based on pre-established criteria, the competitive negotiation is a more open process that allows for discussions with the contractor regarding terms before a final decision is made.[315] This therefore creates an opportunity for a government agency that values transparency to set certain disclosure requirements among the minimum standards in an RFP to acquire AI or other technology. In addition, we think technical specifications regarding accuracy and fairness, among other things, could also be a competitive feature of the procurement process.

2. Qualification and Responsibility

The term "qualification" in procurement law captures a set of procedures that provide for assessing whether an entity that seeks to do business with the government meets the qualification or responsibility standards to perform the requested work.[316] This helps ensure, for instance, that bidders are responsible and have the right equipment and personnel, quality assurance and safety programs, and business ethics.[317] Thus, a law enforcement agency could request that offerors offer an AI system that would meet certain terms and conditions when sold to law enforcement, even if different from terms to others in the private sector or even other agencies. In addition, perhaps this may also be used to qualify the type of organization or contractor with which the agency will do business for forensic algorithms. Thus, an entity without a positive reputation for providing technology that is sufficiently accurate in the law-enforcement context or which has traditionally refused limited disclosure of proprietary information, thus negatively affecting prosecutors' ability to use evidence against a defendant or obtain convictions, might not qualify.

3. Collateral Socioeconomic Policies

Finally, it is worth noting that procurement law is already built to accommodate what is referred to as collateral socioeconomic policies, including, for instance, policies that favor small businesses.[318] Indeed, sometimes procurement has led the way: our federal procurement laws made it illegal to discriminate based on race even prior to the enactment of Title VII of

313. *See* Schwartz, *supra* note 56, at 546.
314. *Id.* at 591.
315. *Id.* at 614.
316. *See, e.g.*, 48 C.F.R. §§ 9.103 to 9.104-4 (2022).
317. *See* 48 C.F.R. § 9.104-1 (2022).
318. *See* Kingdomware Techs., Inc. v. United States, 579 U.S. 162, 164–66 (2016).

the Civil Rights Act.[319] Similarly, we foresee achieving algorithmic transparency through procurement in much the same way. Some other collateral socioeconomic policies that already operate in federal procurement include preferences for disadvantaged business owners,[320] equal employment opportunity policies,[321] preference for domestic goods,[322] and labor standards.[323] Moreover, presidents routinely issue executive orders that concern social and environmental issues through procurement.[324] For example, the Clinton, Bush, Obama, Trump, and Biden administrations have all issued executive orders on procurement.[325] As such, adding algorithmic transparency (or algorithmic justice and fairness more broadly) as contract terms is consistent with furthering these kinds of policies through procurement, especially in the absence of appropriate legislation or other regulations.[326]

The above three features of procurement reinforce that our transaction-by-transaction procurement approach is consistent with existing frameworks in procurement law, trade secret law, and contract law. Indeed, more broadly, we think procurement law might also be a pathway for addressing broader questions having to do with algorithmic justice.[327] With respect to the technological acquisitions that are the subject of this Article, there are reasonable concerns about the level of expertise available to the range of government agencies, particularly in local and state offices. A system of outside technical advisors or experts would likely be needed to work with government agencies to supplement and improve such a scheme. In fact, a by-product of using procurement in this context is that it may spur legislation, particularly as the public and corporate interests realize that the executive branch could be establishing de facto norms through the procurement process.

The view that the government may further social and economic policies or algorithmic governance through procurement policies or contract terms, while potentially controversial, is nonetheless supported by the market-participant

319. *See* Exec. Order No. 11,246, 30 Fed. Reg. 12,319 (Sept. 28, 1965).

320. *See* 15 U.S.C. § 637(a).

321. Exec. Order No. 11,246, 30 Fed. Reg. 12,319 (Sept. 28, 1965) (barring discrimination on the basis of race, sex, religion, or national origin).

322. *See, e.g.*, Buy American Act, §§ 10a–10c, 41 U.S.C. §§ 8301–8305.

323. *See, e.g.*, Davis-Bacon Act, § 276a, 40 U.S.C. §§ 3141–3144; Walsh-Healey Act, 41 U.S.C. § 6502–6511; Service Contract Act of 1965, 41 U.S.C. §§ 6701–6707.

324. Statutes could serve as a limit on such orders and spur additional legislation.

325. *See* Romeo N. Niyongere, *European-Style Green Public Procurement in the American Context: What It Could Look Like*, 49 PUB. CONT. L.J. 785, 799–801 (2020); Exec. Order No. 12,873, 58 Fed. Reg. 54,911 (Oct. 22, 1993) (President Clinton); Exec. Order No. 13,423, 72 Fed. Reg. 3,919 (Jan. 26, 2007) (President Bush); Exec. No. Order 13,693, 80 Fed. Reg. 15,871 (Mar. 25, 2015) (President Obama); Exec. Order No. 13,897, 84 Fed. Reg. 59,709 (Nov. 5, 2019) (President Trump); Exec. Order No. 14,057, 86 Fed. Reg. 70,935 (Dec. 13, 2021) (President Biden).

326. *See generally* MCCRUDDEN, *supra* note 58.

327. In future work, Professor Rowe will explore using procurement beyond transparency to address issues such as algorithmic standards and technical expertise in the government's acquisition of technology, as well as the interaction with legislative constraints.

exception to the Dormant Commerce Clause.[328] When, through procurement, the government behaves as a market participant rather than a regulator, it has more discretion and can behave differently in those distinct roles.[329] Finally, there may be potential legal objections by contractors who are denied contracts for failure to meet algorithmic-related technical or transparency standards. However, to the extent such objections are based on due process or equal protection claims, they are unlikely to be successful because, among other reasons, contractors do not have property rights in prospective contracts[330] and distinctions among vendors would not be based on suspect classifications like sex or race.[331]

D. Proposed Contract Terms to Protect Trade Secrets & Permit Limited Disclosure

We propose a transaction-by-transaction procurement approach whereby those government agencies that value transparency and accountability can negotiate for and insert the appropriate disclosure provisions into their vendor contracts. As a baseline, any proposed solution to disclosure is best viewed not as an all-or-nothing, zero-sum game but along a spectrum where there is some sharing while also protecting intellectual property rights. To be sure, determining how and what to share will be quite challenging, and questions abound. For instance: Should disclosure be context-based? Should the parties anticipate and negotiate for future court-based challenges? What slices of the pie are actual trade secrets, and which are merely confidential? Most importantly, what can be shared without competitive harm? It is important to be mindful that there are several parts to a computer program, including the algorithmic models, source code, object code, and related files and instructions.[332] Each may be protected and layered with intellectual property rights through patent law, copyright law, or trade secret law. It may also be useful to distinguish between raw data and the interpretation of that data as well as models, inputs, and outputs.[333]

There can be tremendous flexibility in crafting the terms of the agreement based on the parties' preferences, the nature of the technology in question, and how it will be used. Key points for consideration and negotiation, however, should be the nuts and bolts of any disclosure: who, what, when, and how. The

328. *See, e.g.*, Reeves, Inc. v. Stake, 447 U.S. 429, 434–36 (1980).

329. *See id.* at 438–39.

330. *See, e.g.*, Chamber of Com. v. Napolitano, 648 F. Supp. 2d 726, 736 (D. Md. 2009) (holding that there is no right to be a government contractor).

331. *See, e.g.*, Lehnhausen v. Lake Shore Auto Parts Co., 410 U.S. 356, 363 (1973).

332. *See generally Basics of Computer Programming for Beginners*, SOFTWARE TESTING HELP, https://www.softwaretestinghelp.com/basics-of-computer-programming/ (Sept. 24, 2022).

333. *See* PASQUALE, *supra* note 286, at 80–83.

"why" is likely to be the agency's threshold public policy position of whether to contract for transparency in the first instance.

We recognize that many, or perhaps most, agencies may not be motivated to contract for transparency on their own initiative. However, democratic governance processes along with procurement discretion could persuade the reluctant agency to adopt this tool or make the conscious, intentional choice *not to contract* for transparency—a choice which will have to be defended to voters and the relevant public. As the parties are contracting for transparency, their respective interests should realistically guide their discussions. For the trade secret owner, protecting trade secrets from disclosure remains paramount in order to avoid losing them.[334] Not only are trade secret rights destroyed if secret information is improperly disclosed, but trade secret owners are required to take reasonable efforts to protect information that they deem a trade secret; courts typically expect such efforts, at a minimum, will include nondisclosure agreements.[335] Thus, managing the terms of confidentiality and limits of disclosure are critical.

1. Who?

As a threshold matter, it would seem that most agencies may wish to allow for the agency itself to examine and independently verify the accuracy, validity, and reliability of any software that it seeks to acquire. In the first instance, the agency-purchaser could reserve the right to inspect and analyze the code subject to protective orders. This may vary depending on the type of technology in use by the agency (for instance, risk assessment versus facial recognition) and how heavily the agency weighs its desire to verify validity. When AI produces the results that government officials want, such as fingerprinting, image identification, or DNA matching, few questions are likely to be raised about the validity of the methodology.[336]

With respect to risk assessment algorithms, prominent criminal justice scholars who support the use of these technologies by law enforcement, while being mindful of due process considerations, also support the need for independent assessments of such tools. For instance, Christopher Slobogin notes:

> Egalitarian and retributive justice cannot be evaluated without knowing whether risk scores are based on race, gender, age, wealth classifications, or proxies for them, and the extent to which they purport to help the state achieve its aim in evaluating risk. The accuracy of the probabilities and other results reached by [a risk assessment algorithm] cannot be confirmed unless

334. *See* ROWE & SANDEEN, *supra* note 234, at 199–200.

335. *See id.* at 199–201.

336. *See* Murphy, *supra* note 53, at 745–47.

> the underlying data and the empirical analysis using it can be evaluated by others.[337]

As such, consideration and negotiation of terms for evaluation by experts in the context of criminal trials or other litigation are important.

Consideration of third-party access is also important. For instance, will the terms provide that if a court orders disclosure in a criminal proceeding or other proceeding, attorneys may be granted access subject to protective orders (as occurs in the civil context), or will disclosure be limited only to experts (and which experts)? Will disclosure be tailored to the purpose for which the information is used? Will disclosure be made to courts, and if so, under seal? Are researchers included, and how is that defined? It may also be appropriate to seek agreement on the need to disclose the names of employees who developed, created, modified, or otherwise worked on the technology. This way they could be available to attorneys, experts, or courts to testify. In the ShotSpotter case discussed earlier, the company refused to identify the names of the employees who altered the algorithm at the request of the Chicago police.[338]

Civil courts routinely use protective orders, and many have models for appropriate protective orders to be used to safeguard disclosure of trade secrets.[339] When a protective order sets out the terms of confidentiality for exchange of materials, public access is generally not an issue.[340] Even in litigation involving trade secrets, court records can be sealed to protect trade secrets, although courts are mindful of parties overclaiming information to be sealed.[341]

2. What?

In negotiating what may be disclosed, it is important to note that transparency does not necessarily require everything, including the secret sauce. In the mix of potential ingredients such as models, data, codes, processes, trials, verifications, and testing, decisions can be made by balancing what are actual trade secrets requiring preservation and what are merely confidential or

337. SLOBOGIN, *supra* note 30, at 109.

338. *See* Motion to Exclude ShotSpotter Evidence, *supra* note 10, at 2.

339. *See, e.g.*, N. DIST. OF ILL., MODEL CONFIDENTIALITY ORDER, https://www.ilnd.uscourts.gov/_assets/_documents/_forms/_judges/COX/sec_qual_po.pdf (last visited Sept. 11, 2022); N.Y. SUPREME CT., STIPULATION AND ORDER FOR THE PRODUCTION AND EXCHANGE OF CONFIDENTIAL INFORMATION, https://www.nycourts.gov/LegacyPDFS/courts/comdiv/NY/PDFs/JMasley-CStip.pdf (last visited Sept. 10, 2022); N. DIST. OF CAL., MODEL STIPULATED PROTECTIVE ORDER (FOR STANDARD LITIGATION), https://www.cand.uscourts.gov/wp-content/uploads/forms/model-protective-orders/CAND_StandardProtOrd.Feb2022.pdf (last visited Sep. 10, 2022).

340. *See* DePuy Synthes Prods., Inc. v. Veterinary Orthopedic Implants, Inc., 990 F.3d 1364, 1370 (Fed. Cir. 2021).

341. *See, e.g.*, *id.* at 1371–73.

proprietary for which a managed sharing arrangement makes sense.[342] Consideration of the standards or goals for transparency may also provide a useful framework. For instance, some scholars have noted that to meet its constitutional obligations, the government should disclose input variables collected about the individual in question; data to support the accuracy of the algorithm across individuals; and results from verification procedures.[343] Others have also argued that even if source code were made available, that alone is not necessarily sufficient transparency given the realities and complexities of machine learning.[344]

Depending on the technology at issue, transparency could also pose a risk of circumvention, which should be considered and avoided. While, for instance, disclosing source code in a DNA analysis tool poses almost no risk of helping future criminals evade detection of their DNA, disclosing too much information about risk assessment tools could, in contrast, conceivably assist someone in gaming the instrument to the extent that it relies on subject survey or Q&A input to get results (which some do).[345] The stage at which the tool is to be used as evidence may also affect the level of transparency negotiated since defendants already have certain rights for evidence used at trial, such as TrueAllele for DNA versus pretrial risk assessments like COMPAS.

It is also worth noting that while vendors might start from the standpoint that everything they wish to protect is a trade secret, that approach is unlikely to survive scrutiny from a trade secret law perspective. Some developers' agreements currently prevent police departments from disclosing the very existence of certain technologies in use for surveillance by the departments.[346] However, not all confidential information is a trade secret.[347] There are many components that go into AI systems—including hardware, software, the data that is fed into the system as input, and the output that is generated from the system.[348] Depending on the circumstances, some, but not all, of these components may be protectable trade secrets. Thus, in drafting agreements about what may be disclosed, it is important to be precise rather than take a one-size-fits-all approach. Of course, as some scholars have noted, there is also the question of whether the government should normatively be entitled to claim trade secrecy on information related to public functions,[349] and they query whether in the hybrid private–government contractual context addressed in this

342. *See* Coglianese & Lehr, *supra* note 157, at 48–49.

343. *See id.* at 41–42.

344. *See* Katyal, *supra* note 30, at 1251. *See generally* Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 NW. U. L. REV. 105, 162–64 (2010).

345. *See* Wexler, *supra* note 30, at 1367.

346. *See id.* at 1366–67.

347. ROWE & SANDEEN, *supra* note 234, at 43.

348. *See* Applin & Sandeen, *supra* note 257 (manuscript at 10–11).

349. *See* Graves & Katyal, *supra* note 30, at 1381–85.

Article, ownership and claims to trade secrecy should remain with the private developer.[350]

3. When and How?

The parties may wish to consider the circumstances under which disclosures may be made. This could range, for instance, from "upon request of any individual" to "only by court order." In trade secret litigation, courts routinely enter protective orders that set out in detail the terms of access, including what may be marked, how it should be labeled, use of confidentiality agreements, access by independent experts, limits on use and disclosure, and how and whether any materials shared should be destroyed or returned after use.[351] Sometimes only experts have access, not the parties.[352] Other times, any inspections are made in camera by a judge.[353] Certain information can be sealed in the court records, courtrooms can be temporarily cleared while some trade secret information is being discussed, or perhaps access can be limited for research purposes only.

Mindful of the court's gatekeeping function, one court has cautioned:

> Hiding the source code is not the answer. The solution is producing it under a protective order. Doing so safeguards the company's intellectual property rights and defendant's constitutional liberty interest alike. Intellectual property law aims to prevent business competitors from stealing confidential commercial information in the marketplace; it was never meant to justify concealing relevant information from parties to a criminal prosecution in the context of a *Frye* hearing.[354]

Assuming then, that a defendant has established a particularized need for the source code to determine its reliability, and the court orders production of the source code, the disclosure should be subject to a protective order.[355] Accordingly, such terms that permit in-camera reviews by a judge or other protective mechanisms would be consistent with the views of advocates for greater transparency in criminal justice trials.[356]

---

350. Some have noted that the private nondelegation doctrine ought to apply in these types of situations and that arrangements with private entities should be structured to preserve constitutional values and accountability. *See, e.g.*, Andrea Nishi, *Privatizing Sentencing: A Delegation Framework for Recidivism Risk Assessment*, 119 COLUM. L. REV. 1671, 1695 (2019) (quoting PAUL R. VERKUIL, OUTSOURCING SOVEREIGNTY: WHY PRIVATIZATION OF GOVERNMENT FUNCTIONS THREATENS DEMOCRACY AND WHAT WE CAN DO ABOUT IT 89 (2007)).

351. ROWE & SANDEEN, *supra* note 234, at 469–70; *see, e.g.*, N. DIST. OF CAL., *supra* note 339.

352. *See* Katyal, *supra* note 30, at 1277.

353. *See id.*

354. State v. Pickett, 246 A.3d 279, 283–84 (N.J. Super. Ct. App. Div. 2021).

355. *Id.* at 284.

356. *See, e.g.*, Wexler, *supra* note 30, at 1403–13; *see also* Citron & Pasquale, *supra* note 30, at 26.

Indeed, just as some jurisdictions already have adopted model language for protective orders in cases involving highly sensitive information and source code,[357] model language for AI procurement contracts, as contemplated in this Article, could also be drafted and made available. This would be an especially helpful starting point for under-resourced government agencies, especially those in smaller cities who may not have ready access to attorneys or relevant experts. For instance, software license agreements generally contain nondisclosure provisions, the gist of which allow disclosure (1) when required by law; (2) pursuant to a court order; (3) when prior written notice is provided from the government agency to the vendor; (4) when assistance is provided by the government agency in obtaining a protective order; (5) when sharing under "attorneys' eyes only"; and (6) when there are specific conditions on how any code or sensitive material is to be handled, reviewed, stored, and protected are made explicit.[358]

E. Benefits of Contract Approach

General contract law principles require mutual assent for contract formation.[359] Sometimes, however, particularly in situations where a consumer signs a contract with a manufacturer or developer without the ability to negotiate its terms, it is referred to as a contract of adhesion or standardized contract.[360] These contracts are not necessarily invalid, but courts may examine the terms more closely to determine whether they are unconscionable.[361] Naturally, these agreements will often be more favorable to the party that drafted them rather than the consumer.[362] Thus, as discussed earlier, this appears to be the status quo where developers dictate terms that forbid disclosure and the government agency accepts, probably with little pushback. Those circumstances notwithstanding, it is possible to envision contract law as a means to further support greater sharing by the government in the procurement context while respecting the rights of developers.[363]

---

357. *See, e.g.*, N. DIST. OF CAL., *supra* note 339.

358. *See* Memorandum of Understanding Between the Laura & John Arnold Found. & the Admin. Off. of the Cts., Arizona Sup. Ct. & the Superior Ct. of Pima Cnty. 3 (Jan. 26, 2016) (on file with authors) [hereinafter Arizona Memorandum of Understanding]; Memorandum of Understanding Between the Laura & John Arnold Found. & Superior Ct. of California, Cnty. of San Francisco 3 (Aug. 3, 2015) (on file with authors) [hereinafter California Memorandum of Understanding]; Memorandum of Understanding Between the Laura & John Arnold Found. & the Seventh Jud. Cir. of the State of Florida 3 (June 5, 2015) (on file with authors) [hereinafter Florida Memorandum of Understanding].

359. *See* 1 WILLISTON ON CONTRACTS § 4:1 (4th ed.), Westlaw (database updated 2022).

360. *See* Jay Kesan et al., *supra* note 46, at 424.

361. *See id.*

362. *See id.*

363. *See* Matwyshyn, *supra* note 50, at 5 (arguing that contract law can be used as a means to protect consumer privacy).

Organizations and agencies that are inclined toward disclosure can negotiate disclosure provisions in their contracts to suit their particular needs. For instance, we reviewed the terms of three Arnold Foundation contracts with courts in three different jurisdictions—Arizona, California, and Florida. While most of the other contract terms were almost identical among all three, the non-disclosure provisions varied. The Arizona clause provided in part, "The Arizona Courts agree to refrain from disclosing *any information* about the Tool, including information about the development, operation and presentation of the Tool, to any third parties without prior written approval from the Foundation."[364] The California provision contained the same language, prohibiting disclosure of any information, and further added that "[i]f, however, the Court is presented with a request for documents . . . the Court will immediately give notice to the Foundation of the request and . . . provide the Foundation with the opportunity to contest such process."[365] Finally, the Florida contract referred not to information generally but specifically to trade secrets. It required specific designation by the Foundation of any information it considers a trade secret pursuant to Florida law.[366] It then provided that "[t]he Circuit agrees to refrain from disclosing, absent the entry of a court order by a court of competent jurisdiction, *any trade secret* about the Tool" and that the Foundation would receive notice and opportunity to contest requests for production.[367] In addition, "The Circuit will reasonably assist the Foundation if necessary to defend properly designated trade secrets but will have no obligation to initiate an action to defend such designation."[368] Thus, this illustrates the flexibility with which the same vendor can offer the same technology to different agencies under individually tailored negotiated terms.

While the government agencies and developers who are not inclined toward sharing might instinctively prefer the status quo's absolute-confidentiality terms, it is worth examining the risks that a court down the road might not agree with those terms. For instance, as noted earlier, *State v. Pickett* is illustrative. There, the parties reached an impasse when trying to negotiate the terms of a protective order for source code.[369] The defendant agreed to a prohibition on disclosure to any individual with "any direct or indirect commercial or employment interest in competing software products" and to certain other safeguards.[370] However, the prosecution insisted on additional and more expansive protections, including a requirement that the software be reviewed only at the prosecutor's office in a supervised inspection, permitting

364. Arizona Memorandum of Understanding, *supra* note 358, at 3 (emphasis added).

365. California Memorandum of Understanding, *supra* note 358, at 3.

366. Florida Memorandum of Understanding, *supra* note 358, at 3.

367. *Id.* (emphasis added).

368. *Id.*

369. State v. Pickett, 246 A.3d 279, 308–09 (N.J. Super. Ct. App. Div. 2021).

370. *Id.* at 310.

only handwritten notes on the 170,000 lines of code (a process which was estimated to take eight years to enable understanding the code).[371] The appeals court remanded, finding that "[a]nything less than full access contravenes fundamental principles of fairness, which indubitably compromises a defendant's right to present a complete defense."[372] Instead, it directed the trial court to compel disclosure of the source code and related materials "pursuant to an appropriate protective order."[373]

The negotiated contract approach proposed in this Article helps mitigate against these uncertainties and brings a more tailored and flexible solution that meets the parties' interests. While a one-size-fits-all approach may bring some efficiencies (for instance, an agency could develop a "standard" set of provisions for all its AI vendors), it may not be ideal for all circumstances. Additionally, the procurement approach here provides both procedural and substantive advantages.

1. Better Control and Accountability

Individually tailored procurement practices could provide more flexibility for agencies to do what they wish and be in control of their decisions and choices. As critics have noted, governmental discretionary—and largely secretive—decision-making processes associated with AI procurement provide no assurance of accountability or validity of AI use.[374] In essence, government agencies are relying on AI developers to self-police and ensure their own algorithms' accuracy. The perception is that so long as the technology provides the respective agency with the results it is hoping for, the agency has little reason to question its functionality.

The reality is that a government agency is a consumer in a uniquely advantageous bargaining position compared to individual consumers in the private marketplace.[375] As such, agencies do not have to accept form agreements or contracts of adhesion. Instead, agencies can better command the terms for disclosure and ownership of the technologies that they acquire.[376] For instance, the government can negotiate and preserve ownership and control rights (if desired). Indeed, simply having possession of testing data and records would get the respective agency closer to being able to disclose the information in response to FOIA requests.[377] It will also allow agencies to allay concerns

371. *Id.* at 309.

372. *Id.* at 311.

373. *Id.*

374. *See supra* Subpart I.B.

375. *See* Brauneis & Goodman, *supra* note 30, at 165 (noting that government agencies have leverage even when they are not paying the vendor).

376. *See id.* at 164–65 (discussing the Seventh Judicial Circuit of Florida's terms with the Arnold Foundation for its PSA program).

377. *Id.* at 135–37.

that they have not adequately reviewed or evaluated the technical or functional aspects of the technology.[378]

2. Better System Integrity

Thinking through and weighing its desired contractual terms will allow an agency to be more intentional about its algorithmic decisions and processes not only from a procurement perspective but ultimately to better comply with its substantive legal obligations. Thus, in anticipating future court challenges, agencies will be better able to justify the design and validity of their decision-making algorithms.[379] This could further help avoid downstream negative consequences, including preserving convictions on appeal. As the court in *Pickett* noted:

> [I]f, as Dr. Perlin [the state's expert] maintains, the source code he wrote is free of harmful defects, and therefore will not impact the reliability of TrueAllele, then it is to everyone's advantage to learn that at the *Frye* hearing. If it should turn out there are source code errors that might affect TrueAllele's reliability, the time to discover that information is now, as part of the judge's gatekeeping role. Reliability must be resolved at the *Frye* hearing rather than in post-conviction relief proceedings.[380]

Ultimately, it is more efficient to have a system in place that gets it right the first time. It increases the risk that courts will find the technology inadmissible at *Frye* hearings if it has not been independently tested and validated and does not provide access to defense counsel because of overly broad secrecy provisions.[381] Moreover, it would be an incentive for departments to negotiate disclosure terms *ex ante* rather than risk not being able to use evidence to obtain a conviction, as happened with the case involving ShotSpotter in Chicago.[382] The fact that employees could manually change the data and algorithm—after the fact—to suit law enforcement is not only a bad look affecting the integrity and credibility of the system as a whole but for the particular technology as well.

3. Better for Vendors Too

Vendors ought to be able to protect their legitimate trade secret rights. Nothing in this Article should be read to suggest otherwise because it is important to preserve expenditures in research and development and spur further innovation that ultimately benefits consumers and the public.

---

378. *See supra* Subpart I.B.3.

379. *See* Coglianese & Lehr, *supra* note 157, at 43–44.

380. State v. Pickett, 246 A.3d 279, 301 (N.J. Super. Ct. App. Div. 2021).

381. *See* SLOBOGIN, *supra* note 30, at 84.

382. *See* Feathers, *supra* note 6.

Developers expend tremendous amounts of resources in research and development in order to build and create AI technologies.[383]

Accordingly, their desire to protect legitimate intellectual property rights in transactions with the criminal justice system are reasonable, and it is imperative that they do so. From the developers' perspective, documents and data related to their technology should be treated as if they are trade secrets. Thus, for example, trade secret data must be segregated from other kinds of data, particularly when they are made available to third parties, and all such parties should execute confidentiality agreements. Furthermore, the information should only be shared on a need-to-know basis.

"Contracts also continue to be vital to buttressing . . . intellectual property protections, as the specific agreements between the parties can sometimes provide extra protection beyond that which is available in each individual area of intellectual property."[384] A further advantage for developers is that they can negotiate what works best for their circumstances and the technology. If subject to broad regulations, requirements tend to be rigid, structured, and of one size.[385]

Indeed, transparency does not require an all-or-nothing approach. Legitimate trade secrets, such as the source code, could be protected and withheld from disclosure, releasing only those records and processes necessary to support validation and testing.[386] Furthermore, beyond trade secrecy, data security might also weigh against 100% disclosure in order to protect all parties, including the public.[387] These negotiated disclosure terms would provide better certainty and clarity going into the business relationship and perhaps better consistency; the contracts could be used for multiple agencies, rather than relying on the whim of individual state court decisions. Accordingly, there might be better control over the management and protection of trade secrets in these technologies licensed to the government instead of leaving it to chance. Indeed, sometimes developers could be subject to out-of-state subpoenas for

383. *See* Justin Jouvenal, *A Secret Algorithm Is Transforming DNA Evidence. This Defendant Could Be the First to Scrutinize It.*, WASH. POST (July 13, 2021, 8:00 AM), https://www.washingtonpost.com/local/legal-issues/trueallele-software-dna-courts/2021/07/12/66d27c44-6c9d-11eb-9f80-3d7646ce1bc0_story.html (noting that Cybergenetics "spent decades and millions of dollars" developing its DNA analysis software, TrueAllele).

384. *See* Rowe, *supra* note 235, at 310.

385. *See generally* Mulligan & Bamberger, *supra* note 285, at 779–80, 788.

386. *See* Brauneis & Goodman, *supra* note 30, at 132.

387. *See* Katyal, *supra* note 30, at 1185; Statement & Release, White House, National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (Jul. 28, 2021) https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ (stating that cybersecurity resiliency is of paramount importance against the cybersecurity threats towards government-operated systems that "are among the most significant and growing issues confronting our nation").

algorithmic models if the parties cannot agree on terms for protective orders.[388] Therefore, negotiating in advance of the transaction the terms of disclosure through the procurement process could help avoid surprises and further litigation costs.[389]

Moreover, recognizing the competitive marketplace in which these transactions occur, if suitable solutions are not achieved in the government–private vendor relationships for the procurement of AI, other "competitors" may exist. Thus, for instance, some government agencies may choose to partner with academic institutions that presumably would be less likely to resist disclosure and sharing to develop their software.[390] This, in turn, could lead to a significant loss of revenues for private developers who tend to rely heavily, and often exclusively, on government contracts. ShotSpotter, for instance, discloses that:

> To date, substantially all of our revenues have been derived from contracts with local governments and their agencies, in particular the police departments of major cities in the United States. . . . We believe that the success and growth of our business will continue to depend on our ability to add new police departments and other government agencies, domestically and internationally, as customers of our public safety solution . . . .[391]

4. Better for Public Interest in Governmental Transparency

Ultimately, as the elusive search for protection of the "public interest" continues, ideally through legislative policy developments, a more immediate measure becomes necessary. As scholars have noted, the public interest in governmental transparency is critical for democratic governance and the criminal justice system.[392] Given the lack of a robust public interest framework in trade secrecy,[393] the procurement approach proposed in this Article presents

388. *See* Whitney Kimball, *A Man on Death Row Has Waited Years for GitHub to Provide Key Evidence. Here's Why It Refuses.*, GIZMODO (May 27, 2021, 2:10 PM), https://gizmodo.com/a-death-row-inmate-has-waited-years-for-github-to-provi-1846976389.

389. Conceivably, from the developer's perspective, future product liability claims might also be limited or avoided if independent verification and testing were allowed at the outset.

390. *See* Brauneis & Goodman, *supra* note 30, at 152 (noting that Allegheny County contracted with university researchers to develop its predictive algorithm).

391. SHOTSPOTTER, INC., ANNUAL REPORT (FORM 10-K) 28 (March 29, 2021), https://ir.shotspotter.com/annual-reports; *see also* Feathers, *supra* note 6 (discussing that ShotSpotter's $33 million contract with Chicago accounted for 13% of the company's first quarter revenue of 2021, making it ShotSpotter's second biggest client after New York City, which accounted for 34%); Garance Burke et al., *How Tech Led to a Murder Charge with No Evidence*, MIA. TIMES, https://www.miamitimesonline.com/news/world_national/how-tech-led-to-a-murder-charge-with-no-evidence/article_31eafdae-04ef-11ec-954c-97438876f262.html (last updated Aug. 27, 2021) (stating the City of Miami has a $5 million dollar contract with ShotSpotter, and that "[t]he U.S. government has spent more than $6.9 million on gunshot detection systems, including ShotSpotter, in discretionary grants and earmarked funds . . .").

392. *See supra* Part I–II.

393. *See supra* Subpart II.C.

a concrete tool that might allow for a negotiated role for the public interest where it does not currently exist. Because there is no monolithic "public interest," we must be mindful of both the public interest in transparency and the public interest in the protection of IP. Both represent bedrock principles in their respective spheres, but as they collide in private–government ventures, procurement is one way to potentially achieve a peaceful resolution that serves both sides of the transaction and the courtroom.

Additionally, there is informational value in knowing which vendors and government agencies value transparency and which do not. For instance, by encouraging market negotiations about transparency, our approach could deliver valuable information about just how much transparency vendors may be willing to tolerate. If vendors say "no" to especially pro-transparency jurisdictions, the willingness to forego seemingly profitable licensing deals tells public policy makers just how high a price vendors place on secrecy. Similarly, an agency's choices and actions in choosing or not choosing to negotiate for transparency can convey valuable information to relevant constituents.

Finally, a lack of transparency does not only affect specific criminal defendants, but the public as a whole, including researchers. To the extent broad trade secret protections prevent nonprofits, university researchers, and other data scientists from performing critical research and studies on algorithms to determine whether the algorithmic models perform in an unbiased manner and what flaws may exist, they prevent algorithmic accountability.[394] For instance, there is little evidence that algorithm creators have tested for racial or other bias, and the few third-party studies that have been performed suggest that developers have failed to conduct such testing.[395] Testing and transparency are necessary because it is often difficult to check even the basic math on some algorithms to verify proper construction of algorithmic models and because the algorithms could be redesigned to function in a manner that would reduce bias and racial disparities.[396] Similarly, there is also the general benefit of overall accuracy (that most citizens might automatically assume exists) when the government chooses to use technology for decision-making in *any* context, whether it implicates voting, driving, filing taxes, or just walking down the street.

394. Chaney, *supra* note 159.

395. *See* Angwin et al., *supra* note 105 (finding that even when criminal history, recidivism, gender, and age were isolated from the COMPAS algorithm, Black defendants were still 77% more likely to be flagged for higher risk of future violent crime); Stevenson, *supra* note 178, at 305; Simonite, *supra* note 179 (noting that the use of risk-assessment tools by judges results in harsher rates of incarceration for defendants of lower socioeconomic status).

396. *See* Chaney, *supra* note 159.

5. Potential Drawbacks

Despite the benefits of the negotiated contractual approach, there are potential drawbacks worth considering. As we noted earlier, there are reasonable concerns about the level of expertise available to the range of government agencies, particularly in local and state offices to make informed decisions and undertake negotiations about these technologies. Many government agencies have far too little time and expertise to consider the optimal level of openness for a given predictive tool and to negotiate for it on an individual basis.[397] A system of outside technical advisors and legal experts would be useful to consult with interested agencies. Moreover, in cases in which a contractor is selling a tool to many government agencies (e.g., ShotSpotter, COMPAS), the contractor may be in a position to say no to the few (if only few) agencies that want significant transparency because it still has most of its business and it avoids what it, perhaps unreasonably, believes to be the risks of disclosure.

These concerns could be addressed by further considering two options (though there could be several others). The first is some form of cooperative purchasing. There are already several organizations that do cooperative purchasing for state, tribal, and local governments.[398] Organizing cooperative purchasing of predictive tools with a level of transparency that would be above what most local governments would get on an individual basis could be very important. The second would be the formation of a standard-setting, testing, and rating organization that could certify predictive tools as meeting certain standards for openness (possibly with several different levels) and maybe also for meeting certain statistical standards. Government agencies could then indicate through the procurement policies discussed earlier that they would purchase only tools that meet a certified level of openness.

CONCLUSION

As the government increasingly relies on private vendors to supply its technologies and the attendant algorithms that aid decision-making, the public's call for transparency will present significant challenges. Private vendors' assertions of trade secret rights in these technologies seemingly conflict with the public's need for disclosure. Ideally, legislated exemptions (both state and federal) could make clear the terms and conditions governing disclosure of

397. *See generally* Burrell, *supra* note 289, at 4; Mulligan & Bamberger, *supra* note 285, at 789.

398. These include private companies like Omnia Partners; nonprofit membership organizations like the National Cooperative Purchasing Alliance, National Association of State Purchasing Officials ValuePoint and BuyBoard; state government agencies like Sourcewell (a Minnesota agency); and the federal General Services Administration, which offers state and local governments GSA schedule purchasing.

algorithms in the public sphere. Such exemptions, however, are unlikely to occur on a wide scale.

In the meantime, the existing trade secrecy framework supports a potential solution. We proposed a transaction-by-transaction procurement approach whereby those agencies that value transparency and accountability can insert the appropriate disclosure provisions into their vendor contracts. This is a practice that is consistent not only with trade secret law but with existing federal and general law and policy on government procurement. Our proposal allows tremendous flexibility in crafting the terms of the agreement based on the parties' preferences, the nature of the technology in question, and how it will be used. Furthermore, it provides better flexibility and control for agencies. The approach has benefits for vendors as well, including that the negotiated disclosure terms would provide better certainty and clarity upon entering into a business relationship with the government rather than relying completely on the whim of individual state court decisions.

Finally, given the lack of a robust public interest framework in trade secrecy,[399] the procurement approach proposed in this Article presents a concrete tool that might allow for a negotiated role for the public interest in governmental transparency where it does not currently exist. With respect to the public interest more generally, our proposal can be generalized and applied broadly to various contexts. A lack of transparency affects not only criminal defendants but nonprofits, university researchers, other scientists and engineers, and members of the press concerned about their lack of access, as well as the larger problem of algorithmic accountability.[400]

399. *See supra* Subpart II.C.

400. Chaney, *supra* note 159.