NOTES

THE WEAPONIZATION OF TRADE SECRET LAW

*Lena Chan**

In criminal proceedings, courts are increasingly relying on automated decisionmaking tools that purport to measure the likelihood that a defendant will reoffend. But these technologies come with considerable risk; when trained on datasets or features that incorporate bias, criminal legal algorithms threaten to replicate discriminatory outcomes and produce overly punitive bail, sentencing, and incarceration decisions. Because regulators have failed to establish systems that manage the quality of data collection and algorithmic training, defendants and public interest groups often stand as the last line of defense to detect algorithmic error. But developers routinely call upon trade secret law, the common law doctrine that protects the secrecy of commercial information, to bar impacted stakeholders from accessing potentially biased software.

This weaponization of trade secret law to conceal algorithms in criminal proceedings denies defendants their right to present a complete and effective defense. Furthermore, the practice contravenes the early policy objectives of trade secret law that sought to promote a public domain of ideas on which market actors could fairly compete and innovate. To remedy this misalignment, this Note proposes a novel framework that redefines the scope of trade secret protection and revives the first principles underlying the doctrine. It concludes that while algorithms themselves constitute protectable trade secrets, information ancillary to the algorithm—such as training data, performance statistics, or descriptions of the software's methodology—do not. Access to ancillary information protects accused parties' right to defend their liberty and promotes algorithmic fairness while aligning trade secret law with its first principles.

* J.D. Candidate 2024, Columbia Law School. With thanks to Professor Shyamkrishna Balganesh, Professor Christopher Morten, and Professor Clarisa Long for their invaluable guidance and the staff of the *Columbia Law Review* for their insightful comments and edits. This Note is dedicated to my parents Keith Kwok-Wai Chan and Yuri Bae Chan, who inspire me constantly.

INTRODUCTION

When a Wisconsin circuit court sentenced Eric Loomis to six years of initial confinement and five years of extended supervision, it did so based on three bar charts, measured on a scale from one to ten.[1] These charts were generated by the Correctional Offender Management Profiling for

1. See Petition for Writ of Certiorari at 3–4, Loomis v. Wisconsin, 137 S. Ct. 2290 (2017) (No. 16-6387) (noting that "the State and the trial court referenced the COMPAS assessment and used it as a basis for incarcerating Mr. Loomis" and "COMPAS is in the form of a bar chart . . . on a scale of one to ten").

Alternative Sanctions (COMPAS) tool, a risk-assessment algorithm that provides "decisional support" to courts determining bail, parole, and sentencing outcomes.[2] COMPAS concluded that Mr. Loomis posed a "high risk to the community";[3] in light of that judgment, the circuit court denied Mr. Loomis parole.[4] Mr. Loomis suspected that COMPAS impermissibly considered his gender[5] and incorrectly assessed his "risk" given that the program was not designed as a sentencing tool.[6] But trade secret law, the common law doctrine that protects the secrecy of commercial information,[7] barred Mr. Loomis from viewing COMPAS's source code and confirming his suspicions.[8] Mr. Loomis appealed his sentence on the grounds that the secrecy surrounding COMPAS violated his due process rights by undermining his right to raise an effective defense and challenge the validity of his accusers' technology.[9] Despite the heavy liberty interests at stake, the Wisconsin Supreme Court determined that COMPAS was a protected trade secret and refused to grant Mr. Loomis access to the algorithm.[10]

---

2. State v. Loomis, 881 N.W.2d 749, 754 (Wis. 2016); see also State v. Loomis, No. 2015AP157-CR, 2015 WL 5446731, at *1 n.2 (Wis. Ct. App. Sept. 17, 2015) (describing the court's reliance on COMPAS to "make decisions about prison incarceration versus community supervision[] [and] to make decisions about bond").

3. For a discussion of the circuit court's analysis of Loomis's COMPAS score in sentencing, see *Loomis*, 881 N.W.2d at 755 ("You're identified, through the COMPAS assessment, as an individual who is at high risk to the community." (quoting *Loomis*, 2014 WL 5446731, at *1)).

4. See id. ("In terms of weighing the various factors, I'm ruling out probation because of the seriousness of the crime and because your history, your history on supervision, and the risk assessment tools that have been utilized, suggest that you're extremely high risk to re-offend." (internal quotation marks omitted) (quoting the circuit court's opinion)).

5. See *Loomis*, 2015 WL 5446731, at *3 (certifying to the Wisconsin Supreme Court the question of "whether a sentencing court's reliance on a COMPAS assessment runs afoul of *Harris*'s prohibition on gender-based sentencing" (cleaned up)).

6. Id. at 2 ("Loomis asserts that COMPAS assessments were developed for use in allocating corrections resources and targeting offenders' programming needs, not for the purpose of determining sentence.").

7. E.g., Amy Kapczynski, The Public History of Trade Secrets, 55 U.C. Davis L. Rev. 1367, 1380 (2022) (explaining how modern applications of trade secret law protect "all commercially valuable business secrets" from wrongful acquisition, use, or disclosure by third parties).

8. The state did not dispute Loomis's assertions that "the company that developed and owns COMPAS maintains as proprietary the underlying methodology that produces assessment scores" and that "the courts are relying on 'a secret non-transparent process.'" *Loomis*, 2015 WL 5446731, at *2.

9. Id. at *1 (certifying to the Wisconsin Supreme Court the question of "whether this practice violates a defendant's right to due process, either because the proprietary nature of COMPAS prevents defendants from challenging the COMPAS assessment's scientific validity, or because COMPAS assessments take gender into account").

10. State v. Loomis, 881 N.W.2d 749, 761 (Wis. 2016) (finding that COMPAS was "a proprietary instrument and a trade secret"). The U.S. Supreme Court denied Mr. Loomis's petition for writ of certiorari. See Loomis v. Wisconsin, 137 S. Ct. 2290, 2290 (2017).

This weaponization of trade secret law to conceal algorithms in criminal proceedings denies defendants like Mr. Loomis their right to present a complete and effective defense against their accusers.[11] Courts increasingly rely on automated decisionmaking to inform their judgments[12] even though these technologies come with significant risks.[13] Algorithms produce inaccurate[14] or discriminatory[15] outcomes when developers build them on datasets or features that incorporate bias.[16] In the criminal legal setting, the consequences are severe: Algorithmic errors generate overly punitive bail, sentencing, or incarceration outcomes that disproportionately harm racial and gender minorities.[17] Given the absence

---

11. See, e.g., State v. Pickett, 246 A.3d 279, 299 (N.J. Super. Ct. App. Div. 2021) ("[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." (quoting State ex rel. A.B., 99 A.3d 782, 790 (N.J. 2014))).

12. Courts often consider algorithmic predictions about the likelihood that a defendant may one day reoffend. Rebecca Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, 70 Stan. L. Rev. 1343, 1347–48 (2018) [hereinafter Wexler, Life, Liberty, and Trade Secrets] (describing how "judges and parole boards rely on risk assessment instruments, which purport to predict an individual's future behavior, to decide who will make bail or parole and even what sentence to impose").

13. Ziad Obermeyer, Brian Powers, Christine Vogeli & Sendhil Mullainathan, Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations, 366 Science 447, 447 (2019) ("There is growing concern that algorithms may reproduce racial and gender disparities via the people building them or through the data used to train them." (citations omitted)).

14. See, e.g., Danielle Keats Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249, 1256 (2008) (describing state-administered algorithms that "issued hundreds of thousands of incorrect Medicaid, food stamp, and welfare eligibility determinations and benefit calculations").

15. See, e.g., Amanda Levendowski, How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem, 93 Wash. L. Rev. 579, 601 (2018) (describing how a criminal legal algorithm was twice as likely to misclassify Black defendants as posing a high risk for reoffending relative to white defendants).

16. Biased datasets reproduce racial and gender disparities. See id. at 592 (describing how "training data infused with implicit bias can result in skewed datasets that fuel both false positives and false negatives"). Programmers train algorithms to perform a specified task (e.g., prediction or pattern recognition) by exposing the system to an input dataset and providing select examples of model decisionmaking. See M. I. Jordan & T. M. Mitchell, Machine Learning: Trends, Perspectives, and Prospects, 349 Science 255, 255 (2015) (describing how a programmer may develop a machine learning algorithm by "showing it examples of desired input-output behavior"); Levendowski, supra note 15, at 591 (explaining how developers train artificial intelligence systems by providing an "example" of decisionmaking and exposing the system to other "variations" from which it learns to make comparable decisions). From these examples, the algorithm learns to detect certain patterns or rules that guide future automated assessments. Harry Surden, Machine Learning and Law, 89 Wash. L. Rev. 87, 91 (2014).

17. Andrea Roth, Trial by Machine, 104 Geo. L.J. 1245, 1270 (2016) (describing the risk of "illegitimate or illegal discrimination" among algorithms that influence bail, testimony, verdicts, and sentencing in criminal trials (internal quotation marks omitted) (quoting Omer Tene & Jules Polonetsky, Judged by the Tin Man: Individual Rights in the Age of Big Data, 11 J. on Telecomm. & High Tech. L. 351, 358 (2013))).

of uniform regulation over data collection and algorithmic training,[18] individuals like Mr. Loomis often stand as the last line of defense to detect the inaccuracies of programs deployed against them. But when trade secret law allows developers to block defendants from reviewing their code's accuracy and methodology, the risks of algorithmic error and discrimination abound.[19] Without access to source code, individuals like Mr. Loomis cannot challenge the scientific validity of sentencing algorithms or present an effective defense against their accusers.[20]

The current state of trade secret law lets corporations conceal their algorithms to the detriment of people in the criminal legal system.[21] But the doctrine has not always been this way. While modern courts broadly seclude algorithmic information,[22] early courts narrowly protected secret inventions to encourage greater innovation than would otherwise exist in an unregulated market.[23] In fact, trade secret law first articulated principles of *restraint*: Courts were to protect secret ideas and inventions just enough to incentivize innovation and creation but not so much as to award intellectual monopolies and stifle competition.[24]

---

18. See François Candelon, Rodolphe Charme di Carlo, Midas De Bondt & Theodoros Evgeniou, AI Regulation Is Coming, Harv. Bus. Rev., Sept.–Oct. 2021, at 102, 106 ("In dealing with biased outcomes, regulators have mostly fallen back on standard antidiscrimination legislation. That's workable as long as there are people who can be held responsible for problematic decisions. But with AI increasingly in the mix, individual accountability is undermined."); Jon Kleinberg, Jens Ludwig, Sendhil Mullainathan & Cass R. Sunstein, Discrimination in the Age of Algorithms, J. Legal Analysis, 2018, at 1, 2 (suggesting that the lack of regulatory oversight over algorithms may exacerbate efforts to detect discrimination).

19. Sonia K. Katyal, The Paradox of Source Code Secrecy, 104 Cornell L. Rev. 1183, 1248 (2019) [hereinafter Katyal, The Paradox of Source Code Secrecy] ("[A]ssertions of trade secret protection . . . remain a key obstacle for researchers and litigants seeking to test the efficacy and fairness of government algorithms and automated decision making.").

20. See State v. Pickett, 246 A.3d 279, 301 (N.J. Super. Ct. App. Div. 2021) (arguing that defendants have a "competing and powerful" interest in forensic software used to incriminate them and that "shrouding the source code and related documents in a curtain of secrecy substantially hinders defendant's opportunity to meaningfully challenge reliability").

21. Rebecca Wexler, It's Time to End the Trade Secret Evidentiary Privilege Among Forensic Algorithm Vendors, Brookings Inst. (July 13, 2021), https://www.brookings.edu/blog/techtank/2021/07/13/its-time-to-end-the-trade-secret-evidentiary-privilege-among-forensic-algorithm-vendors/ [https://perma.cc/M967-3T7R] ("Developers who sell or license forensic algorithms to law enforcement routinely claim that they have a special trade secret entitlement to entirely withhold relevant evidence about how these systems work from criminal defense expert witnesses.").

22. See, e.g., Q-Co Indus. v. Hoffman, 625 F. Supp. 608, 617 (S.D.N.Y. 1985) ("Computer software, or programs, are clearly protectible under the rubric of trade secrets . . . .").

23. See Adam D. Moore, A Lockean Theory of Intellectual Property, 21 Hamline L. Rev. 65, 65 (1997) ("In order to enlarge the public domain, permanently society protects certain private domains temporarily.").

24. See infra section I.A. for a discussion of trade secret law's limited scope.

Given this misalignment with early policy objectives, courts and scholars alike must reassess the propriety of extending trade secret protection to algorithmic information. Part I reviews the origins of trade secret law to clarify the first principles that shaped the doctrine. Rather than conceal proprietary information, early trade secret law sought to promote a *public* domain of ideas on which market actors could fairly compete and innovate. Part II examines how trade secret protection of "ancillary information"[25] contravenes those principles by (1) secluding non-trade-secret information about algorithmic development and performance and (2) restricting competition.[26] Part III proposes a novel framework that redefines the scope of trade secret protection in the algorithmic context and revives trade secret law's early policy objectives. This Note concludes that while algorithms themselves constitute protectable trade secrets, ancillary information—such as training data, performance statistics, or descriptions of the software's methodology—does not. The disclosure of ancillary information comports with first principles and public demands for algorithmic transparency while maintaining trade secret holders' proprietary interests.

I. THE HISTORY OF TRADE SECRET LAW

A. *Early Trade Secret Law's Liability Regime*

Trade secret law developed amid disputes between employers, employees, and market competitors over the use of secret manufacturing processes.[27] The Supreme Judicial Court of Massachusetts first expounded on the doctrine in the 1868 case *Peabody v. Norfolk*,[28] in which a manufacturer of gunny cloth sued to restrain his employee from revealing the firm's secret production techniques to a competitor.[29] The court ordered an injunction against the employee to protect the manufacturer's production technique. This injunction would ensure that the value the manufacturer brought to the production process through his unique "skill and attention" would be shielded from improper use by third parties.[30] In deriving the manufacturer's interest in his trade secret from the skill and attention he invested in its development, *Peabody* recognized what courts

---

25. This Note adopts the term "ancillary information" to describe nonprotected materials related to protected algorithms. For a more detailed explanation of ancillary information, see infra notes 132–136 and accompanying text.

26. See infra section II.D (discussing how secluding information on algorithmic methodology and performance limits efforts to improve existing technologies).

27. Catherine L. Fisk, Working Knowledge: Employee Innovation and the Rise of Corporate Intellectual Property, 1800–1930, at 82 (2009) (describing how trade secret law emerged in the employment context as firms sought "to wrest control of the production process from their skilled workers").

28. 98 Mass. 452, 459 (1868).

29. Id. at 454.

30. Id. at 457.

would later term "the *labor*—the so-called 'sweat equity'—that goes into creating a work."[31] Importantly, as a practical consequence of awarding injunctive relief, *Peabody* shielded the manufacturer's valuable creation from his competitors.[32]

But secluding the manufacturer's techniques served the larger policy goal of generally encouraging "invention and commercial enterprise" for the public interest.[33] Although it guarded individuals' secrets, *Peabody* cautioned that trade secret protection must further "the advantage of the public."[34] To expand "invention and commercial enterprise,"[35] the law could not bar new innovators from examining valuable knowledge and information for purposes of improving them.[36] Indeed, early courts recognized that trade secret overprotection risked stunting innovation by secluding too much information from the public.[37] In 1908, a Michigan circuit court considered whether to extend trade secret protection to a manufacturing process that, while "limited" in use in the complainant's industry, was in "common use" in other industries.[38] The court declined to grant the innovator "exclusive use" of a process that was in "common use," cautioning that such broad protections "would foster monopoly and exclude others from the use of well-known and much-used prior devices."[39] By awarding narrow trade secret protections and taking an expansive view of non-trade-secret knowledge, the law encouraged competing innovators to build upon existing products in the market.[40]

---

31. Alcatel USA, Inc. v. DGI Techs., Inc., 166 F.3d 772, 788 (5th Cir. 1999). See *Peabody*, 98 Mass. at 457.

32. See Kapczynski, supra note 7, at 1396 (cautioning that trade secret law "can be used to prevent the dissemination of information *indefinitely*").

33. *Peabody*, 98 Mass. at 457.

34. Id.

35. Id.

36. See Robert G. Bone, A New Look at Trade Secret Law: Doctrine in Search of Justification, 86 Calif. L. Rev. 241, 284 (1998) ("Keeping information secret denies other innovators opportunities to express their creativity, deprives persons of the fruits of further research based on the secret, and forces consumers to pay higher prices.").

37. See Pamela Samuelson & Suzanne Scotchmer, The Law and Economics of Reverse Engineering, 111 Yale L.J. 1575, 1581 (2002) ("Intellectual property rights, if made too strong, may impede innovation and conflict with other economic and policy objectives.").

38. Hamilton Mfg. Co. v. Tubbs Mfg. Co., 216 F. 401, 405–06 (C.C.W.D. Mich. 1908) (describing how "machines doing the same character of work and involving the same principles found in the complainant's machines were in common use in woodworking establishments").

39. Id. at 407.

40. See Mark A. Lemley, The Surprising Virtues of Treating Trade Secrets as IP Rights, 61 Stan. L. Rev. 311, 313–14 (2008) (arguing that when applied coherently, trade secret law increases efficient collaboration and communication between parties who would otherwise be too distrustful to share information); Intell. Prop. Off., The Economic and Innovation Impacts of Trade Secrets, Gov.UK (Apr. 19, 2021), https://www.gov.uk/government/publications/economic-and-innovation-impacts-of-trade-secrets/the-economic-and-innovation-impacts-of-trade-secrets#economic-construction [https://perma.cc/3SRA-D2VN]

Trade secret law, then, faced an inherent tension. On the one hand, the doctrine safeguarded intellectual labor to encourage innovation at the individual level.[41] On the other hand, overbroad trade secret protections could prevent the improvement of products by concealing "well-known" and "much-used" processes from other innovators.[42] To balance these competing interests in secrecy and public access, the law established a liability regime that limited the scope of exclusionary rights to foster fair competition.[43]

Although it shielded secret production techniques from wrongful disclosure, *Peabody* clarified that the manufacturer "has not indeed an exclusive right to it as against the public, or against those who in good faith acquire knowledge of it."[44] Rather than establish an absolute property right in the trade secret,[45] the court conditioned its protection on the invention's value and the propriety of the employee's behavior.[46] First, the law limited injunctive relief to trade secrets made commercially "valuable" by the creator's efforts.[47] By requiring economic value, the court sought to avoid overbroad protections for general noncommercial knowledge or processes that may nonetheless benefit the public.[48] Second, the court qualified that it would "restrain a party [only] from making a disclosure of secrets communicated to him in the course of a confidential employment."[49] Rather than granting a property right against the world, *Peabody* established a liability rule that guarded valuable business secrets against parties involved in the "violation of contract and breach of confidence."[50] By restricting its jurisdiction to circumstances involving

---

(explaining how overbroad trade secret protections "restrict the acquisition of ideas" and cause "reduced innovation and lower productivity growth").

41. See supra notes 30–31 and accompanying text.

42. See *Hamilton Mfg.*, 216 F. at 407.

43. See Eric R. Claeys, The Use Requirement at Common Law and Under the Uniform Trade Secrets Act, 33 Hamline L. Rev. 583, 595 (2010) ("By refusing to recognize any property rights, trade secrecy promotes competition and consumer access, and it also frees all competitors to innovate or gather useful information by sparing them the transaction costs associated with bargaining with a right holder.").

44. Peabody v. Norfolk, 98 Mass. 452, 458 (1868).

45. Sharon K. Sandeen, The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act, 33 Hamline L. Rev. 493, 499 (2010) (describing how "courts were unwilling to find an absolute property interest in secret information").

46. See *Peabody*, 98 Mass. at 458.

47. Id. at 457.

48. See Camilla A. Hrdy, The Value in Secrecy, 91 Fordham L. Rev. 557, 559 (2022) [hereinafter Hrdy, The Value in Secrecy] (describing how the value requirement "performs an essential line-drawing function" because it "distinguishes mere secrets, which abound in human society, from trade secrets").

49. *Peabody*, 98 Mass. at 459 (quoting 2 Joseph Story, Commentaries on Equity Jurisprudence, as Administered in England and America § 952 (1836)).

50. Id. at 458.

dishonest behavior, trade secret law vindicated "interests not of property but of fair competition and commercial morality."[51]

The reverse engineering exception is a central component of trade secret law's liability regime.[52] Because liability depends on whether the defendant used unfair means to access the trade secret, trade secret law does not penalize "those who in good faith acquire knowledge."[53] Consequently, third parties may discover otherwise protected secrets as long as they do so through fair and lawful means,[54] such as reverse engineering.[55] Courts have long recognized reverse engineering as a proper method of studying public information on trade secrets to recreate or improve them.[56] For example, to reverse engineer the trade secret formula for Coca-Cola,[57] a competitor may conduct any number of experiments on the Coca-Cola product,[58] the ingredients publicly disclosed by the company,[59] or other fairly obtained information[60] to reinvent it. They may

---

51. Kapczynski, supra note 7, at 1389. In 1939, the Restatement of Torts reiterated these principles, stating that trade secret law reflected a "general duty of good faith" in the marketplace, not any "right of property in the idea." Restatement of Torts § 757 cmt. a (1939).

52. Trade secret law confines liability to misappropriation, which is narrowly defined as improper acquisition, use, or disclosure. Because reverse engineering is not a form of misappropriation, it is legal. See Jessica M. Meyers, Artificial Intelligence and Trade Secrets, Landslide, Jan.–Feb. 2019, at 17, 19 (describing how trade secret law "does not give its owner a monopoly over the subject of the trade secret" because the "information is only protected against misappropriation—improper acquisition, use, or disclosure").

53. *Peabody*, 98 Mass. at 458.

54. Bone, supra note 36, at 257 (describing how "independent discovery and reverse engineering were perfectly lawful because they did not cross the boundaries of the owner's secrecy and violate his factual exclusivity").

55. Reverse engineering is a "method for studying protected products in an attempt to develop a more thorough understanding of the relevant art in order to create superior products." Craig L. Uhrich, The Economic Espionage Act—Reverse Engineering and the Intellectual Property Public Policy, 7 Mich. Telecomm. & Tech. L. Rev. 147, 170 (2001). The Uniform Trade Secret Act defines reverse engineering as "starting with the known product and working backward to find the method by which it was developed." Unif. Trade Secrets Act § 1 cmt. (Unif. L. Comm'n 1985).

56. Samuelson & Scotchmer, supra note 37, at 1582 n.23 (describing how competitors may reverse engineer for numerous purposes, such as "learning, changing or repairing a product, providing a related service, developing a compatible product, creating a clone of the product, and improving the product"); Samuel J. LaRoque, Comment, Reverse Engineering and Trade Secrets in the Post-*Alice* World, 66 U. Kan. L. Rev. 427, 437 (2017) (describing how "courts have traditionally recognized reverse engineering as a proper means of learning trade secrets").

57. See Coca-Cola Bottling Co. of Shreveport v. Coca-Cola Co., 107 F.R.D. 288, 294 (D. Del. 1985) (holding that Coca-Cola's "secret formulae are trade secrets").

58. See id. at 291 (describing the Coca-Cola product's "tremendous market recognition").

59. See id. at 289 (describing how "most of the ingredients are public knowledge").

60. Kurt M. Saunders & Nina Golden, Skill or Secret?—The Line Between Trade Secrets and Employee General Skills and Knowledge, 15 N.Y.U. J.L. & Bus. 61, 75 (2018) (explaining how "one who independently invents or discovers information identical to

not, however, misappropriate or access the secret through unfair means,[61] such as seeking employment at Coca-Cola for purposes of publicizing the formula.[62]

The reverse engineering exception limits the scope of trade secret protection to avoid granting intellectual monopolies that would stunt fair competition and innovation.[63] In 1992, the Ninth Circuit articulated these antimonopolistic concerns when considering the lawfulness of reverse engineering computer code.[64] The court discussed how prohibitions on reverse engineering would confer on the software holder an impermissible "*de facto* monopoly over those ideas and functional concepts."[65] The Ninth Circuit determined that reverse engineering was "fair use . . . as a matter of law" in part because it was "the only way" that a competitor may "gain access" to the code.[66] Finding that competitors must enjoy some lawful means to access certain "ideas and functional concepts," the court declined to establish a monopoly over the software at issue.[67] In 1989, the Supreme Court described reverse engineering as "an essential part of innovation,"[68] recognizing that competitors must enjoy the right to lawfully reinvent trade secrets to devise "new and improved products"[69] and produce "significant advances in the field."[70] Thus, trade secret law sought to facilitate a competitive market on which competitors could reverse engineer and enhance trade secrets for the public good.[71]

---

another's trade secret, without relying on improper means to do so, is not liable for misappropriation").

61. See Meyers, supra note 52, at 19 (noting that trade secrets are protected against misappropriation).

62. Such conduct would constitute a "violation of contract and breach of confidence." Peabody v. Norfolk, 98 Mass. 452, 458 (1868).

63. Lemley, supra note 40, at 340 ("To avoid inadvertently encouraging secrecy rather than disclosure, trade secret law incorporates limits on the scope of the right, notably the defenses of independent development and reverse engineering."); see also Samuelson & Scotchmer, supra note 37, at 1625–26 ("Reverse engineering . . . may also lessen a monopoly platform provider's market power by providing application developers with an alternative means of entry . . . .").

64. See Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1526 (9th Cir. 1992).

65. Id. at 1527; see also Chi. Lock Co. v. Fanberg, 676 F.2d 400, 405 (9th Cir. 1981) (noting that the removal of the reverse engineering exception would "convert the . . . trade secret into a state-conferred monopoly akin to the absolute protection that a federal patent affords").

66. See *Sega Enters.*, 977 F.2d at 1527–28.

67. Id. at 1527.

68. Bonito Boats, Inc. v. Thunder Craft Boats, Inc, 489 U.S. 141, 160 (1989).

69. Samuelson & Scotchmer, supra note 37, at 1590; see also Uhrich, supra note 55, at 149 ("Since reverse engineering plays a significant role in the exploitation of knowledge committed to the public domain through the grant of patents and copyrights, prohibiting reverse engineering may stifle the drive to study and improve upon the existing knowledge base.").

70. See *Bonito Boats*, 489 U.S. at 160.

71. Deepa Varadarajan, Trade Secret Fair Use, 83 Fordham L. Rev. 1401, 1420 (2014) ("Scope-limiting doctrines in intellectual property law . . . reconcile owners' rights to

In conclusion, trade secret law's liability regime balanced the innovator's interest in their business secret against the public's interest in knowledge and invention. Although it protected creators' secrets, the law permitted competitors to reverse engineer products to study and improve them.[72] Because it reduced the risk of intellectual monopolies and allowed competitors to recreate and enhance existing secrets, the reverse engineering exception was "an important part of the balance implicit in trade secret law."[73]

B. *Incentives for Competition and Innovation Under the Liability Regime*

By narrowly secluding commercial secrets and broadly permitting reverse engineering, early trade secret law sought to promote fair competition and innovation for the public interest.[74] Because it incentivized efficient market behavior, the reverse engineering exception played a central role in realizing these policy objectives. First, because innovators could decide to license their trade secrets based on how easily competitors could reverse engineer them, the exception facilitated greater information sharing than would exist without it.[75] Second, by permitting competitors to lawfully enter the market, the exception advanced fair use over misappropriation.[76] Importantly, trade secret law's incentive structure achieved these outcomes only in certain circumstances, namely when reverse engineering was costly but feasible.[77]

1. *Reverse Engineering Facilitates Information Sharing.* — Trade secret law's liability rule influenced innovators to engage in efficient market decisions that minimized overinvestment and overprotection. Because the law shielded their products from misappropriation, trade secret holders could avoid "overinvesting in actual secrecy" or "mak[ing] wasteful investments in locks and fences and encryption."[78] In addition to advancing efficiency, the doctrine encouraged innovators to license rather

---

exclude with the public's interest in furthering innovation and access."); see also Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 485 (1974) (describing how "[c]ompetition is fostered and the public is not deprived of the use of valuable, if not quite patentable, invention" under trade secret law).

72. Uhrich, supra note 55, at 155 (explaining how reverse engineering permits the "study of, and improvement upon, discoveries that have been committed to the public domain").

73. Samuelson & Scotchmer, supra note 37, at 1584; see also Chi. Lock Co. v. Fanberg, 676 F.2d 400, 402–03 (9th Cir. 1982) (distinguishing trade secret law's reverse engineering exception from the "absolute" monopoly awarded by patent law).

74. Lemley, supra note 40, at 314 (arguing that trade secret law "advances the goals of innovation and promotes responsible business conduct without limiting the vigorous competition on which a market economy is based").

75. See infra section I.B.1.

76. See infra section I.B.2.

77. See infra section I.B.3.

78. Dan L. Burk, Law and Economics of Intellectual Property: In Search of First Principles, 8 Ann. Rev. L. & Soc. Sci. 397, 410 (2012).

than seclude products that competitors could otherwise easily reverse engineer.[79] Because they would lose their market share to competitors who successfully reverse engineered their products, innovators sought to maximize profits by licensing "weak" trade secrets (i.e., ones competitors could easily reverse engineer) subject to a fee and secluding "strong" trade secrets (i.e., ones that were difficult to reverse engineer).[80] In turn, if the cost of licensing a trade secret was less than the cost of reverse engineering it, competitors paid to license it.[81] Consequently, the reverse engineering exception avoided overseclusion by protecting trade secrets only as long as they were valuable enough to evade recreation. As a result, the law returned products and processes that failed to derive a competitive advantage from their secrecy to the public domain, allowing society to enjoy inventions that would otherwise be secluded.

2. *Reverse Engineering Incentivizes Fair Use.* — By permitting competitors to lawfully enter the market, this liability regime incentivized greater innovation than would otherwise exist if the law awarded no protection (i.e., underprotection) or granted a legal monopoly to the first innovator (i.e., overprotection). Without legal safeguards over their creations, people would decline to develop trade secrets because free riders could reap the benefits of their labor without consequence.[82] By shielding valuable inventions from misappropriation, trade secret law ameliorated these harms; because innovators could recoup the investment costs from trade secrets, they enjoyed legal incentives to develop those secrets.[83] Trade secret law also addressed the adverse consequences of overprotection. If the law gave innovators an absolute property right, certain products and techniques would remain secret in perpetuity, preventing competitors from reverse engineering them.[84] Consequently, by permitting third parties to profit from products that they fairly recreate, the reverse engineering exception encouraged competitors to improve existing products rather than invest in "wasteful industrial espionage" and misappropriate those products.[85] Because it vindicated trade secret

79. See Samuelson & Scotchmer, supra note 37, at 1589 (describing how innovators may allow "some measure of competition from licensees (e.g., by licensing with low royalties)" to "avoid reverse engineering by unlicensed entrants").

80. See id. (explaining how licensing permits innovators to maintain "market power" and "profit").

81. Burk, supra note 78, at 410 ("Competitors will instead license the information if the cost of a license is less than the expected cost of independently discovering or reverse engineering the information.").

82. Jonathan R. Chally, Note, The Law of Trade Secrets: Toward a More Efficient Approach, 57 Vand. L. Rev. 1269, 1270 (2004) (describing how "the law must protect commercial secrets to insure that those secrets will be developed").

83. Id. at 1274 (2004) ("Without the ability to exclude free-riders from profiting from one's idea, innovators cannot recoup experimentation costs to the extent necessary to justify the decision to innovate.").

84. See supra notes 36–40, 63–67, and accompanying text.

85. Burk, supra note 78, at 410.

owners' interest in their products until competitors reverse engineered them, trade secret law's liability rule offered market actors greater incentives to innovate than alternate regimes.

3. *Reverse Engineering Must Be Difficult but Feasible.* — But the incentives for information sharing[86] and fair use[87] disappeared when reverse engineering was either too easy or too difficult. As a consequence of the liability rule, innovators could decide to enter certain sectors of the market over others based on the ease of reverse engineering within that sector.[88] If competitors could easily and cheaply reverse engineer a product, potential innovators would decline to develop in that industry because they would capture the market only for the brief period before successful reverse engineering by others.[89] Conversely, if reverse engineering a product was virtually impossible, the first market entrant could monopolize the good, and competitors would enjoy no incentive to develop in that industry and improve existing products.[90] Consequently, trade secret law struggled to maximize innovation if reverse engineering was too easy or too difficult because innovators and competitors would enjoy fewer incentives to develop and enhance products.

In contrast, trade secret law accomplished its goals when reverse engineering was expensive but feasible. Under such conditions, trade secret holders would reap the benefits of their inventions and continue innovating because competitors would require greater time before they could reverse engineer the product.[91] And as long as reverse engineering was feasible and lucrative, competitors would nonetheless invest in those costs of reverse engineering to eventually capture the market.[92] Thus, when reverse engineering was *difficult but feasible*, trade secret law maximized the incentives for trade secret holders and competitors to innovate.

---

86. See supra section I.B.1.

87. See supra section I.B.2.

88. See Samuelson & Scotchmer, supra note 37, at 1587 n.49 ("In general, the more difficult reverse engineering is, the greater value the secret will have, the longer lead time advantage the trade secret holder will enjoy in the market, and the less incentive the holder may have to license the secret.").

89. Id. at 1652 ("When a particular means of reverse engineering makes competitive copying too cheap, easy, or rapid, innovators may be unable to recoup R&D expenses.").

90. Id. at 1613 ("[R]everse engineering of object code is generally so difficult, time-consuming, and resource-intensive that it is not an efficient way to develop competing but nonidentical programs.").

91. See J.H. Reichman, Computer Programs as Applied Scientific Know-How: Implications of Copyright Protection for Commercialized University Research, 42 Vand. L. Rev. 639, 659 (1989) ("Because this task of catching up to the originator's head start takes time, it presumably endowed traditional innovators with a period of natural lead time that enabled them to gain a foothold in the market."); Samuelson & Scotchmer, supra note 37, at 1625 (describing how incentives to develop and innovate are "generally adequate owing to the high costs and difficulties of reverse-engineering").

92. See Samuelson & Scotchmer, supra note 37, at 1587–88 (describing how a competitor or "second comer" may "compete in the same market" after successfully "reverse-engineering the innovator's product").

C. *The Haphazard Development of Trade Secret Law*

Although early courts clearly articulated trade secret law's liability rule and reverse engineering exceptions, they struggled to offer a precise definition of a trade secret itself.[93] As a result, subsequent developments in trade secret law proceeded haphazardly, state by state, as a "creature of common law."[94] The Restatement of Torts ("First Restatement"), published in 1939,[95] sought to provide a uniform definition for trade secrets from this unruly precedent.[96] Until the late 1900s, the First Restatement was "the sole authority to which most courts looked to define the scope of trade secret protection."[97] Section 757 of the First Restatement described a trade secret as "any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."[98] It instructed courts to determine whether a trade secret exists by considering:

> (1) the extent to which the information is known outside of [the] business; (2) the extent to which [the information] is known by employees and others involved in [the] business; (3) the extent of measures taken . . . to guard the secrecy of the information; (4) the value of the information to . . . competitors; (5) the amount of effort or money expended . . . in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.[99]

Despite the First Restatement's efforts to promote uniformity, trade secret law continued to develop inconsistently.[100] In turn, the 1979 Uniform Trade Secrets Act (UTSA) sought to reintroduce clarity to trade secret law.[101] Under the UTSA, a trade secret:

---

93. See, e.g., Peabody v. Norfolk, 98 Mass. 452, 458 (1868) (noting "a process of manufacture" or "medicine" as examples of protected trade secrets but not otherwise defining trade secret subject matter). The *Peabody* court acknowledged that courts had previously defined trade secret matter in only "the broadest terms." See id. at 459.

94. Camilla A. Hrdy, The General Knowledge, Skill, and Experience Paradox, 60 B.C. L. Rev. 2409, 2426 (2019) [hereinafter Hrdy, The General Knowledge].

95. Restatement of Torts § 757 cmt. b (1939).

96. Bone, supra note 36, at 247 ("The First Restatement of Torts, published in 1939, extracted a relatively clear definition and a set of liability rules from a confusing body of precedent." (footnote omitted) (citing Restatement of Torts § 757)).

97. Annemarie Bridy, Trade Secret Prices and High-Tech Devices: How Medical Device Manufacturers Are Seeking to Sustain Profits by Propertizing Prices, 17 Tex. Intell. Prop. L.J. 187, 198–99 (2009).

98. Restatement of Torts § 757 cmt. b.

99. Id.

100. Sandeen, supra note 45, at 502 (noting the "slow pace and frequently inconsistent development of the common law" following the First Restatement).

101. Deepa Varadarajan, Business Secrecy Expansion and FOIA, 68 UCLA L. Rev. 462, 470, 474–75 (2021) (describing how the National Conference of Commissioners on Uniform State Laws enacted the UTSA as a model state statute). To date, all states except New York and North Carolina have codified the UTSA. Trade Secrets Act, Unif. L. Comm'n,

> (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and
>
> (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[102]

In 1995, the Third Restatement of Unfair Competition offered another attempt to organize trade secret doctrine. The Third Restatement adopted a "sweepingly expansive articulation" of trade secret subject matter,[103] providing that a trade secret is "any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others."[104] Unlike the First Restatement, the Third Restatement did not distinguish between trade secrets and confidential yet non-trade-secret information.[105] Because the Third Restatement offered no rationale for its departure from the First Restatement, some scholars have suggested that its definition of trade secrets "lack[ed] a coherent vision."[106] Courts have thus favored the First Restatement over the Third Restatement when determining the scope of trade secrets.[107]

II. THE PROBLEM WITH MODERN APPLICATIONS OF TRADE SECRET LAW TO ALGORITHMS

A. *Inconsistent Determinations of Trade Secret Subject Matter*

The divergent views of trade secret subject matter in the Restatements and the UTSA introduced tremendous confusion in the courts.[108] As a result, the definition of trade secrets varies across state and federal law,[109]

---

https://www.uniformlaws.org/committees/community-home?CommunityKey=3a2538fb-e030-4e2d-a9e2-90373dc05792 [https://perma.cc/VS8C-M48B] (last visited Oct. 31, 2023).

102. Unif. Trade Secrets Act § 1(4) (Unif. L. Comm'n 1985).

103. Eric E. Johnson, Trade Secret Subject Matter, 33 Hamline L. Rev. 545, 552 (2010).

104. Restatement (Third) of Unfair Competition § 39 (1995).

105. Johnson, supra note 103, at 552 ("[W]hile the First Restatement carefully distinguished between trade secrets and other sorts of confidential business information, the Third Restatement concerned itself solely with trade secrets.").

106. Id. at 554.

107. Hrdy, The General Knowledge, supra note 94, at 2428 (describing how "the Third Restatement has not been as influential as other sources, with many courts instead continuing to reference the First Restatement").

108. See Johnson, supra note 103, at 556 ("Given the mixed signals sent about trade secret subject matter by blackletter sources, it should be no surprise that considerable confusion has arisen in the courts.").

109. Harry First, Trade Secrets and Antitrust Law, *in* The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research 332, 334 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011) (describing how trade secrets "now also find some definition in state statutory law" and "in federal law").

inviting inconsistent adjudication.[110] Although determining trade secret subject matter is a "terrifically confounding" exercise, the issue has received "scant attention" from scholars and courts.[111]

At minimum, common law and statutory definitions require that trade secrets are valuable.[112] But courts follow "no clear guidance" on determining the value of a trade secret.[113] While some jurisdictions determine value according to the trade secret owner's interest in keeping the invention secret,[114] others measure value based on a competitor's gain from misappropriating the product.[115] Judges also weigh the value of a trade secret relative to the competitive advantage it offers to either the innovator or their competitors.[116] Meanwhile, some courts adopt a "sweat-of-the-brow" theory,[117] which either evaluates value according to the "effort and expense" in developing the innovation[118] or the ease of reverse engineering it.[119] To make matters worse, judges often fail to inquire into a creation's value at all.[120] Although innovators carry the burden of proving economic value,[121] courts routinely assume that a product is

---

110. Johnson, supra note 103, at 558 ("The confusion found in explications of permissible subject matter is echoed in the confusion surrounding the results of trade secret lawsuits.").

111. Id. at 546; see also Hrdy, The Value in Secrecy, supra note 48, at 560 (describing the "paucity of law review articles" on the requirement that trade secrets are valuable).

112. The First Restatement notes that "the value of the information" and "the amount of effort or money expended . . . in developing the information" are relevant factors for determining if a trade secret exists. Restatement of Torts § 757 cmt. b (1939). Similarly, the UTSA requires that trade secrets derive independent economic value from their secrecy. Unif. Trade Secrets Act § 1(4)(i) (Unif. L. Comm'n 1985).

113. Johnson, supra note 103, at 557.

114. Id. ("Some courts have held that the core inquiry in determining whether information has independent economic value relates to the value placed by the plaintiff, the putative trade secret owner, on keeping the information secret from persons who could exploit it to the owner's relative disadvantage.").

115. Id. at 557–58 ("Other courts have held that information has economic value if the defendant, the putative trade secret thief, derives value from using it.").

116. Olson v. Nieman's, Ltd., 579 N.W.2d 299, 314 (Iowa 1998) (defining "economic value" in the context of Iowa Code § 550.2(4)(a) (1991) as the "value of the information to either the owner or a competitor" (quoting U.S. W. Commc'ns, Inc. v. Off. of Consumer Advoc., 498 N.W.2d 711, 714 (Iowa 1993))).

117. Johnson, supra note 103, at 558.

118. See McCallum v. Allstate Prop. & Cas. Ins. Co., 204 P.3d 944, 950 (Wash. Ct. App. 2009).

119. See Walker Mfg., Inc. v. Hoffmann, Inc., 261 F. Supp. 2d 1054, 1082 (N.D. Iowa 2003) (holding that "the ease with which the device can be 'reverse engineered' is certainly relevant to the question of whether or not the device *remains* a 'trade secret'").

120. Hrdy, The Value in Secrecy, supra note 48, at 559–60 (describing how "courts sitting in trade secret litigation have not closely scrutinized plaintiffs' assertions of independent economic value").

121. Rent Info. Tech., Inc. v. Home Depot U.S.A., Inc., 268 F. App'x 555, 558 (9th Cir. 2008) (finding that the complainant "failed to carry its burden of proving that any specific business [secrets] derive their value from not being generally known").

valuable enough based on "circumstantial evidence, such as the time, money, and effort invested in developing the information."[122]

Because courts lack a coherent test for measuring value and often fail to investigate value altogether, determinations of trade secret subject matter vary widely.[123] While some judges extend trade secret protection to business information on consumer purchases,[124] others find that such materials are not trade secrets because they lack economic value.[125] Similarly, courts disagree on whether financial data about a company's pricing and sales are sufficiently valuable to receive legal protection.[126] The trade secret status of "negative know-how"—knowledge about processes that are nonbeneficial or detrimental to the trade secret holder—varies by jurisdiction.[127] In the algorithmic context, the propriety of trade secret protection for training data remains in dispute.[128] Consequently, when courts fail to carefully scrutinize trade secret claims, they risk erroneously secluding non-trade-secret materials.[129]

---

122. Hrdy, The Value in Secrecy, supra note 48, at 560 ("Independent economic value, if it appears at all, is an afterthought, something that courts assume can be shown easily from circumstantial evidence, such as the time, money, and effort invested in developing the information.").

123. Johnson, supra note 103, at 559 (discussing inconsistent trade secret treatments of consumer, marketing, and business strategy data).

124. See Star Sci., Inc. v. Carter, 204 F.R.D. 410, 415 (S.D. Ind. 2001) (finding that data on product sales and use were trade secrets because the "information is not readily obtainable, and possesses economic value").

125. Vigoro Indus., Inc. v. Cleveland Chem. Co. of Ark., 866 F. Supp. 1150, 1164 (E.D. Ark. 1994) (declining to protect consumer purchasing data because "its independent economic value is scant").

126. Compare Whyte v. Schlage Lock Co., 125 Cal. Rptr. 2d 277, 287 (Cal. Ct. App. 2002) (finding that financial data on profit margins, production costs, and accounting information had "independent economic value because Schlage's pricing policies would be valuable to a competitor"), with United States v. IBM Corp., 67 F.R.D. 40, 49 (S.D.N.Y. 1975) (finding that the value of financial data on profits, loss, and sales to "competitors is speculative").

127. Charles Tait Graves, The Law of Negative Knowledge: A Critique, 15 Tex. Intell. Prop. L.J. 387, 392 (2007) (describing how the extension of trade secret protection over "negative information . . . is a difficult subject").

128. Compare Zabit v. Brandometry, LLC, 540 F. Supp. 3d 412, 424 (S.D.N.Y. 2021) ("[A]lthough Plaintiffs cannot lay claim to the [training] data, the algorithm and its methodology for using that data might still be protected."), with Lab. Ready, Inc. v. Williams Staffing, LLC, 149 F. Supp. 2d 398, 412 (N.D. Ill. 2001) (granting trade secrecy protection to a corporation's "models and data"). Scholars have noted that "[i]solated data as such may not necessarily have any commercial value," which "begs the question whether we should extend trade secrets protection also to databases obtained by aggregating data." Guido Noto La Diega & Cristiana Sappa, The Internet of Things (IoT) at the Intersection of Data Protection and Trade Secrets. Non-Conventional Paths to Counter Data Appropriation and Empower Consumers, 2020 Eur. J. Consumer L., 419, 440.

129. In *State v. Chun*, the New Jersey Supreme Court ordered a breathalyzer manufacturer to share its source code with an independent third party for an assessment of its scientific validity. See 943 A.2d 114, 123 (N.J. 2008). In addition to identifying errors in the software, the examination revealed that the allegedly proprietary software consisted of

B. *Barriers to Accused Parties' Right to Present a Complete Defense*

Despite the absence of a coherent test for trade secrets, courts consistently award trade secret protection to algorithms.[130] An algorithm is a computational procedure that automates decisionmaking processes by predicting future outcomes or identifying patterns from complex datasets.[131] This Note adopts the term "ancillary information" to describe all non-trade-secret information that is related to but separate from the protected algorithm.[132] Ancillary information encompasses three general categories of material: (1) summary information providing context on the algorithm's development, methodology, or performance; (2) input data used to train the algorithm; and (3) output data produced by the algorithm. Summary information offers intelligible, high-level analyses or descriptions to clarify a software's methodology and performance.[133] Broadly speaking, algorithms receive input information to calculate unique output values.[134] Output values may consist of predictions or pattern detection, such as the likelihood that a defendant will recidivate

---

general algorithms that arguably failed to meet the elements of a trade secret. See Report on Behalf of the Defendants at 14, *Chun*, 943 A.2d 114 (No. 58,879) (stating that "the code is not really unique or proprietary" because it "consists mostly of general algorithms"); see also Charles Short, Note, Guilt by Machine: The Problem of Source Code Discovery in Florida DUI Prosecutions, 61 Fla. L. Rev. 177, 190 (2009) ("The resulting examination of the code revealed that it consisted primarily of *general* algorithms and, as a result, was arguably not unique or proprietary."). *Chun* demonstrates the need for courts to strictly police overbroad trade secrecy claims over programs that are not entitled to protection.

130. See Short, supra note 129, at 189–90 (describing how courts have protected algorithms and source code as trade secrets since the 1980s).

131. See Levendowski, supra note 15, at 590 ("Most AI systems are trained using vast amounts of data and, over time, hone the ability to suss out patterns that can help humans identify anomalies or make predictions."); Surden, supra note 16, at 90 (describing how "researchers often employ machine learning methods to analyze existing data to predict the likelihood of uncertain outcomes").

132. For an explanation of why ancillary information is not a trade secret, see infra section III.C.

133. See Maayan Perel & Niva Elkin-Koren, Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement, 69 Fla. L. Rev. 181, 185 (2017) (describing the necessity of "proper tools to analyze massive amounts of data"). Summary information is crucial to clarify convoluted algorithmic operations as the sheer volume of input and output data may be so vast that they are "unintelligible" in isolation. Id.; see also Katyal, The Paradox of Source Code Secrecy, supra note 19, at 1250 (arguing that the "disclosure of source code is a deceptively simple solution to the problem of algorithmic transparency . . . because of the complexity and dynamism of machine-learning processes" (citing, among others, Frank Pasquale, The Black Box Society: The Secret Algorithms that Control Money and Information 142 (2015))); David S. Levine, Confidentiality Creep and Opportunistic Privacy, 20 Tul. J. Tech. & Intell. Prop. 11, 41 (2017) (arguing that "contextual and relational information is needed to fully assess an algorithm's function and impact").

134. See Surden, supra note 16, at 90 (describing how "machine learning algorithms may produce automated results" based on "existing data").

or reoffend.[135] Input values include existing data related to the problem or phenomenon of interest, such as a defendant's prior criminal record.[136]

Modern courts designate both algorithms and ancillary information about their development, methodology, and performance as trade secrets.[137] But because there is no coherent test for determining the trade secret status of automated software, courts risk secluding non-trade-secret materials[138] that are essential for confirming the methodology, accuracy, and fairness of otherwise inscrutable algorithms.[139] Such overprotection raises due process concerns in criminal proceedings, in which errors may produce overly punitive bail outcomes, verdicts, and sentences.[140] In light of the "competing and powerful" liberty interests[141] implicated by automated decisionmaking, algorithmic transparency is more important than ever.[142] But when defendants seek information about the accuracy and performance of criminal justice technologies,[143] the companies that own and license these programs to courts routinely object to such disclosure on the grounds that their algorithms are trade secrets.[144]

---

135. See, e.g., State v. Loomis, 881 N.W.2d 749, 753–54, 753 n.10 (Wis. 2016) (describing how a risk assessment algorithm called the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) tool is "intended to predict the general likelihood that those with a similar history of offending are either less likely or more likely to commit another crime following release from custody").

136. See, e.g., id. at 754 (describing how the "COMPAS risk assessment is based upon information gathered from the defendant's criminal file and an interview with the defendant").

137. See, e.g., GlobeRanger Corp. v. Software AG U.S., Inc., 836 F.3d 477, 491–93 (5th Cir. 2016) (extending trade secret protection to proprietary computer software); *Loomis*, 881 N.W.2d at 761 (awarding trade secret protection to the COMPAS algorithm and information related to its performance because the developer "considers COMPAS a proprietary instrument").

138. See Hrdy, The Value in Secrecy, supra note 48, at 606–07 (arguing that courts must assess the statutory elements of trade secrets "more comprehensively and consistently" to avoid granting trade secret status to mere confidential information).

139. For an explanation of how summary information may clarify algorithmic outcomes and methods, see supra note 133 and accompanying text.

140. See Wexler, Life, Liberty, and Trade Secrets, supra note 12, at 1346 ("At every stage—policing and investigations, pretrial incarceration, assessing evidence of guilt at trial, sentencing, and parole—machine learning systems and other software programs increasingly guide criminal justice outcomes.").

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

142. Wexler, Life, Liberty, and Trade Secrets, supra note 12, at 1402 (arguing that the seclusion of automated criminal justice technologies harms "anyone who is affected by a criminal justice outcome and for whom greater transparency could provide assurance that the outcome was proper").

143. See, e.g., State v. Loomis, 881 N.W.2d 749, 757 (Wis. 2016) (considering whether "the proprietary nature of COMPAS prevents [defendants] from assessing its accuracy").

144. Wexler, Life, Liberty, and Trade Secrets, supra note 12, at 1358–64 (describing how developers invoke trade secrecy protection in criminal litigation to withhold evidence on their source code, methodology, and software performance).

The seclusion of summary information about the COMPAS algorithm demonstrates these harms. Owned by commercial vendor Northpointe, COMPAS purports to calculate an individual's likelihood of "recidivism," or reoffending,[145] based on criminal records and questionnaires.[146] In 2016, the Wisconsin Supreme Court upheld Mr. Loomis's eleven-year sentence based on COMPAS's determination that he posed a high risk for general recidivism and violent recidivism.[147] Mr. Loomis appealed his sentence on the grounds that COMPAS's proprietary nature prevented him from challenging its accuracy and validity.[148] But the Wisconsin Supreme Court rejected Mr. Loomis's claims and declined to compel the disclosure of COMPAS source code or summary information, finding that Northpointe "considers COMPAS a proprietary instrument and a trade secret."[149]

Loomis raises numerous concerns about the seclusion of summary information. Given that algorithms and ancillary information are entitled to distinct legal protections, courts must independently determine the trade secret status of these materials.[150] Because the Wisconsin Supreme Court failed to differentiate between the COMPAS algorithm and its ancillary summary information, however, it withheld non-trade-secret data from interested parties.[151] The nondisclosure of summary information prevents defendants like Mr. Loomis from exercising their right to present a complete defense and challenge algorithmic decisions that implicate

---

145. Jeff Larson, Surya Mattu, Lauren Kirchner & Julia Angwin, How We Analyzed the COMPAS Recidivism Algorithm, ProPublica (May 23, 2016), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm [https://perma.cc/A86C-25CW] ("Across the nation, judges, probation and parole officers are increasingly using algorithms to assess a criminal defendant's likelihood of becoming a recidivist—a term used to describe criminals who re-offend.").

146. Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, Machine Bias, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/QK5L-CWQ6] ("Northpointe's core product is a set of scores derived from 137 questions that are either answered by defendants or pulled from criminal records."). The COMPAS questionnaire measures defendants' prior education, employment, substance use, and other factors. Equivant, Practitioner's Guide to COMPAS Core 31–32 (2019), https://www.equivant.com/wp-content/uploads/Practitioners-Guide-to-COMPAS-Core-040419.pdf [https://perma.cc/29MW-YGQ9].

147. See *Loomis*, 881 N.W.2d at 755–56, 772.

148. Id. at 753 (considering "the specific question of whether the use of a COMPAS risk assessment at sentencing 'violates a defendant's right to due process, either because the proprietary nature of COMPAS prevents defendants from challenging the COMPAS assessment's scientific validity, or because COMPAS assessments take gender into account.'" (quoting State v. Loomis, No. 2015AP157-CR, 2015 WL 5446731, at *1 (Wis. Ct. App. Sept. 17, 2015))).

149. Id. at 761.

150. For a discussion of why algorithms are entitled to trade secrecy protection while ancillary information is not, see infra section III.C.

151. See *Loomis*, 881 N.W.2d at 761 (withholding COMPAS's source code and ancillary data).

their life and liberty.[152] Indeed, the Wisconsin Court of Appeals noted this catch-22 for criminal defendants before the Wisconsin Supreme Court denied Mr. Loomis's due process claims.[153] Mr. Loomis sought to appeal his sentence on the grounds that COMPAS (1) impermissibly considered his gender[154] and (2) inaccurately assessed his "risk."[155] But to prove these claims, he required access to information about COMPAS's algorithm, its assessment of gender, and its accuracy—information barred by Northpointe's invocations of trade secret protection.[156] Considering this "lack of transparency," the Wisconsin Court of Appeals questioned how Mr. Loomis could meaningfully articulate his due process claims and "'explain how the [COMPAS] assessments work' absent access to COMPAS's underlying proprietary methodology."[157]

Yet the Wisconsin Supreme Court's refusal to share COMPAS code with Mr. Loomis reflects the failure of modern courts to closely police trade secret subject matter. Statutory and common law authorities on trade secret law all require that courts investigate the value and secrecy of an invention.[158] Despite these commands, the Wisconsin Supreme Court designated the COMPAS algorithm and its summary information as trade secrets without closely analyzing their trade secret status. Rather than inquiring into the software's value, the court relied on Northpointe's conclusory allegation that COMPAS was "a proprietary instrument and a trade secret."[159] Despite the harms of overprotection, several courts have arrived at the same outcome as *Loomis*, denying defendants' requests to access risk-assessment programs on the grounds that such programs are trade secrets.[160] Like *Loomis*, these decisions extend trade secret protection

---

152. See Charles Tait Graves & Sonia K. Katyal, From Trade Secrecy to Seclusion, 109 Geo. L.J. 1337, 1375 (2021) ("Denying source code availability makes it literally impossible for the defendant to present a full and complete defense . . . .").

153. See *Loomis*, 2015 WL 5446731, at *2 (noting that the lack of transparency in COMPAS's methodology raises potential questions of due process).

154. Id. at *3 (certifying the question of "whether a sentencing court's reliance on a COMPAS assessment runs afoul of *Harris*'s prohibition on gender-based sentencing" (cleaned up)).

155. Id. at *2 ("Loomis asserts that COMPAS assessments were developed for use in allocating corrections resources and targeting offenders' programming needs, not for the purpose of determining sentence.") Mr. Loomis argued that both grounds constituted violations of his due process rights. Id.

156. See id.

157. Id. (quoting Brief of Plaintiff-Respondent at 10, *Loomis*, 2015 WL 54467321).

158. For a discussion of the secrecy and value requirements for trade secrets, see infra section III.A.

159. State v. Loomis, 881 N.W.2d 749, 761 (Wis. 2016).

160. See Graves & Katyal, supra note 152, at 1375 ("Several other cases have followed this reasoning, concluding that source code is proprietary and therefore essentially immune from investigation by the defendant."); see also People v. Super. Ct., No. B258569, 2015 WL 139069, at *6 (Cal. Ct. App. Jan. 9, 2015) (denying a death-penalty-eligible defendant the right to examine a forensic program after determining that its source code was a trade secret); People v. Carter, No. 2573/14, 2016 WL 239708, at *1, *7 (N.Y. Sup. Ct. Jan. 12,

based on mere allegations that the technology is proprietary.[161] These opinions also fail to separately analyze the trade secret statuses of algorithms and ancillary summary information.[162] By secluding non-trade-secret information, *Loomis* and its progeny wield trade secret law as a weapon against people in the criminal legal system.

C. *Barriers to Bias Mitigation*

Algorithmic opacity not only harms defendants but also undermines third parties' efforts to mitigate technological bias and discrimination. Public interest groups play a crucial role by using publicly available data to expose algorithmic harms and unveil discriminatory outcomes in criminal sentencing,[163] housing,[164] healthcare,[165] and other technologies.[166] But trade secret protection over algorithms impedes these empirical investigations.[167] To address this problem, public interest groups often rely on a form of reverse engineering that does not require access to the source code itself.[168] Using only input and output data from previous applications of the technology, researchers can reverse engineer algorithms and

---

2016) (denying a defendant's discovery motion for the Forensic Statistical Tool because "the source code is proprietary software"); People v. Lopez, 23 N.Y.S.3d 820, 829 (N.Y. Sup. Ct. 2015) (refusing to turn over software to a defendant on the grounds that it was proprietary).

161. See Katyal, The Paradox of Source Code Secrecy, supra note 19, at 1270 (arguing that the determination of trade secret status "risks becoming somewhat circular in nature: something is secret because it is said to be secret, not because the information, in actuality, *is* secret or because its secrecy is proven with particularity").

162. See, e.g., GlobeRanger Corp. v. Software AG U.S., Inc., 836 F.3d 477, 492, 502 (5th Cir. 2016) (extending trade secrecy protection to a software and its related "documentation" based on limited evidence that "at least some portion of its . . . [software] constituted a trade secret").

163. E.g., Larson et al., supra note 145 (identifying racial bias in the COMPAS algorithm).

164. E.g., Julia Angwin, Ariana Tobin & Madeleine Varner, Facebook (Still) Letting Housing Advertisers Exclude Users by Race, ProPublica (Nov. 21, 2017), https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin (on file with the *Columbia Law Review*) (uncovering the racial bias of Facebook's algorithm for advertising housing opportunities by measuring the outputs of ProPublica's inputs into Facebook's system).

165. E.g., Obermeyer et al., supra note 13, at 448–49 (discovering that a nationwide healthcare algorithm disproportionally underestimated the health needs of Black patients).

166. E.g., Julia Angwin & Surya Mattu, Amazon Says It Puts Customers First. But Its Pricing Algorithm Doesn't, ProPublica (Sept. 20, 2016), https://www.propublica.org/article/amazon-says-it-puts-customers-first-but-its-pricing-algorithm-doesnt (on file with the *Columbia Law Review*) (simulating customer activity and examining public product listings to identify that Amazon's pricing algorithm was biased toward Amazon products).

167. See Obermeyer et al., supra note 13, at 447 ("Algorithms deployed on large scales are typically proprietary, making it difficult for independent researchers to dissect them.").

168. See Levendowski, supra note 15, at 604 ("Reverse engineering can be a critical means of examining bias in AI systems."); Obermeyer et al., supra note 13, at 447 ("Instead, researchers must work 'from the outside[]' . . . and resort to clever work-arounds such as audit studies.").

investigate their accuracy, fairness, and methodology.[169] In 2016, the investigative journalism organization ProPublica successfully reverse engineered the COMPAS algorithm using input and output information obtained from public access requests and determined that the software was racially biased.[170] Because input and output data are ancillary materials that do not constitute trade secrets,[171] reverse engineering enables members of the public to check against algorithmic unfairness without accessing proprietary software itself.[172]

The issue is that companies like Northpointe regularly claim trade secret protection over *all* materials related to their software, including non-trade-secret datasets,[173] which undermines bias-mitigation techniques that rely on reverse engineering.[174] To make matters worse, the law is ill-equipped to police overbroad trade secrecy claims. Because developers seldom voluntarily disclose their source code to the public, courts adjudicating those technologies' trade secret status lack virtually any information about them.[175] To meaningfully assess trade secrecy claims, courts may require that trade secret holders disclose their algorithms and ancillary information subject to protective orders.[176] Protective orders prevent nonparties from accessing the materials at issue to maintain the confidentiality of algorithmic information.[177] Despite these safeguards,

---

169. See Levendowski, supra note 15, at 602 ("Reverse engineering is a way of leveraging available inputs or outputs to understand the mechanics of what happens inside a black box system."). Specifically, competitors require training data and output values from previous iterations of an algorithm to reverse engineer its functions. See, e.g., Larson et al., supra note 145 (reverse engineering the COMPAS algorithm from criminal records and risk assessment scores in previous applications of the tool).

170. See Larson et al., supra note 145 (finding that Black defendants "who did not recidivate over a two-year period were nearly twice as likely to be misclassified as higher risk compared to their white counterparts"); see also infra section III.C.3 (discussing ProPublica's reverse engineering).

171. See infra section III.C.

172. See Wexler, Life, Liberty, and Trade Secrets, supra note 12, at 1374 (describing how reverse engineering "uses known inputs, outputs, and knowledge of the general function of a system but not of its internal contents or implementation").

173. See Levendowski, supra note 15, at 600 (describing how Northpointe refused to disclose COMPAS's source code or performance metrics).

174. See Obermeyer et al., supra note 13, at 447 ("Without an algorithm's training data, objective function, and prediction methodology, we can only guess as to the actual mechanisms for the important algorithmic disparities that arise.").

175. Sonia K. Katyal, Private Accountability in the Age of Artificial Intelligence, 66 UCLA L. Rev. 54, 125 (2019) [hereinafter Katyal, Private Accountability] ("[W]ithout first disclosing and examining the source code, it is impossible to know whether an algorithm even qualifies as a trade secret.").

176. See Unif. Trade Secrets Act § 5 (Unif. L. Comm'n 1985) ("[A] court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include granting protective orders in connection with discovery proceedings . . . .").

177. Wexler, Life, Liberty, and Trade Secrets, supra note 12, at 1353 (describing how "courts may issue protective orders to limit the use and distribution of trade secrets beyond the needs of the proceeding").

however, companies routinely object to examination under protective order on the grounds that the risk of inadvertent disclosure jeopardizes their proprietary interests.[178] As a result, corporate entities often take advantage of the difficulties in policing trade secret subject matter by broadly claiming protection over all algorithmic materials, "even when the underlying information may not actually qualify as a trade secret."[179] In criminal proceedings, when defendants demand access to programs that determine their verdicts and sentences, the vendors of these risk-assessment tools object that their technology is proprietary.[180] And in civil proceedings, credit reporting companies and social media powerhouses like Facebook call upon trade secret law to defend against lawsuits claiming that their algorithms are discriminatory.[181] Consequently, developers' tendency to claim trade secret protection over algorithmic materials at large, alongside courts' failure to police these broad allegations, exacerbates issues of technological opacity.

D. *Departure From First Principles*

The nondisclosure of summary data marks a profound departure from the first principles underlying early trade secret law. Public access to information on a product's performance and accuracy plays a crucial role in improving available technologies on the market.[182] When summary information exists in the public domain, consumers (e.g., courts licensing risk-assessment programs) can make informed purchases based on product qualities of accuracy and fairness.[183] As consumers identify and select

---

178. Id. at 1349–50 (noting that developers often "claim entitlements to withhold that information from criminal defendants and their attorneys, refusing to comply even with those subpoenas that seek information under a protective order and under seal").

179. Katyal, Private Accountability, supra note 175, at 125.

180. See, e.g., State v. Loomis, 881 N.W.2d 749, 761 (Wis. 2016) (declining to compel Northpointe to disclose the COMPAS algorithm based on Northpointe's objection that its technology is a protected trade secret).

181. See Mikella Hurley & Julius Adebayo, Credit Scoring in the Era of Big Data, 18 Yale J.L. & Tech. 148, 158 (2016) ("A number of emerging companies use proprietary 'machine-learning' algorithms to sift and sort through thousands of data points available for each consumer. These companies treat their machine-learning tools as closely-guarded trade secrets, making it impossible to offer a comprehensive picture of the industry."); Meghan J. Ryan, Secret Algorithms, IP Rights, and the Public Interest, 21 Nev. L.J. 61, 66 (2020) (describing how "companies such as Facebook rely on secret algorithms in their advertisement targeting, which could discriminate against certain types of individuals in critical markets like housing"); Joseph Blass, Note, Algorithmic Advertising Discrimination, 114 Nw. U. L. Rev. 415, 450 (2019) (noting that lawsuits against Facebook for discriminatory advertisement "would require inspecting the actual algorithms used by companies like Facebook—algorithms that form the basis of their revenue-raising business and are fiercely guarded trade secrets").

182. For an explanation of summary information, see supra note 133 and accompanying text.

183. Courts have directed the state to fix and declined to accept into evidence results from criminal justice technologies that yield incorrect results. In *State v. Chun*, a court-

high-quality algorithms over discriminatory software, programmers face market pressures to develop new technologies that minimize error and bias.[184] Consequently, when courts withhold summary data from the public, they stymie bias mitigation and software improvement in the industry.

Similarly, secluding input and output data disrupts incentives for competition and innovation by rendering reverse engineering functionally impossible.[185] Algorithmic development involves complex mathematical operations and data preparation processes.[186] Even when third parties do have access to relevant input and output information (which is seldom the case), reverse engineering a software system is a difficult enterprise.[187] Consequently, when the law entirely withholds input and output data from third parties, reverse engineering is near impossible,[188] allowing algorithm owners to maintain a virtual monopoly over their software.[189] This protection of intellectual monopolies

---

ordered investigation into the scientific validity of a breathalyzer technology revealed a "significant flaw in the program's source code that, in limited circumstances, can lead to an inaccurate reported BAC test result." 943 A.2d 114, 157 (N.J. 2008). The court declared that it would "reject all of the tests" if it was "without confidence in the accuracy of the individually reported results." Id. at 158; see also People v. Thompson, No. 4346/15, 2019 WL 4678813, at *1 (N.Y. Sup. Ct. Sept. 25, 2019) (unpublished table decision) (declining to use evidence produced by a forensic analysis software on the grounds that its "results were not the product of procedures generally accepted in the 'community' of DNA forensic scientists").

184. See Levendowski, supra note 15, at 601 ("Bias mitigation techniques, like reverse engineering and algorithmic accountability processes, provide a means of identifying where competitors may be able to make gains over incumbents: by rectifying a known bias.").

185. See id. at 604–06 (discussing how the nondisclosure of training data impedes reverse engineering).

186. See Katyal, The Paradox of Source Code Secrecy, supra note 19, at 1249 ("[B]ecause algorithms increasingly depend on the input of unique personal data, the outcomes may be obscure and difficult to study in a systematic capacity without access to the data."); Michael Mattioli, Disclosing Big Data, 99 Minn. L. Rev. 535, 557, 566–67 (2014) (describing how "big data" algorithms are "difficult to uncover through reverse engineering" because their training data is often aggregated from multiple sources and stripped of information that can be used to identify individuals).

187. See Katyal, The Paradox of Source Code Secrecy, supra note 19, at 1249 ("If the source code is unavailable, the only way to obtain the code is to engage in reverse engineering, but this is often difficult, costly, and restricted . . . ."); Wexler, Life, Liberty, and Trade Secrets, supra note 12, at 1374 (describing how reverse engineering is "limited by the volume and scope of known test inputs, the difficulty of testing for unforeseen circumstances, and the possibility of fraud" (footnotes omitted)).

188. Access to input and output data is necessary for reverse engineering algorithms. Katyal, The Paradox of Source Code Secrecy, supra note 19, at 1251 ("[E]ven if source code disclosure reveals some elements of a decision reached through automated processing, it cannot be fully evaluated without an accompanying investigation of the training data . . . ."). Consequently, "assertions of trade secret protection . . . remain a key obstacle for researchers and litigants seeking to test the efficacy and fairness of government algorithms and automated decision making" through reverse engineering. Id. at 1248.

189. See Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1527 (9th Cir. 1992) (finding that prohibitions on reverse engineering would confer on the software holder an

contradicts trade secret law's policy goals of encouraging competition and innovation and reflects an unprecedented shift in the doctrine.

Finally, early trade secret law originated as a means to prevent misappropriation and unfair use in the workplace, not to shield corporate entities from accountability when their technology incriminates, penalizes, or otherwise discriminates against members of the public. At first, trade secret law awarded injunctive relief to manufacturers seeking to prevent wrongful disclosure and acquisition by employees and competitors.[190] In contrast, algorithm owners now claim trade secret protection not to prevent misappropriation but to evade investigations into the fairness and accuracy of their technology by defendants and public interest groups—parties who are neither competitors nor employees.[191] These novel applications of trade secret law introduce immense confusion and invite courts to forget that the doctrine was narrowly concerned with commercial exchanges between market actors.[192] As a result, these unprecedented fact patterns increase the risk of overprotection and algorithmic opacity.[193]

III. REVISITING THE VALUE REQUIREMENT OF TRADE SECRETS

When courts fail to carefully scrutinize the boundaries of trade secret subject matter, they risk secluding information that does not qualify as a trade secret.[194] This practice withholds information necessary for defendants to challenge the accuracy, fairness, and validity of algorithms[195] and

---

impermissible "*de facto* monopoly over [the program's] ideas and functional concepts"); Chally, supra note 82, at 1274–76 ("By precluding potential competitors from entering a market, government protection of ideas creates a state-sponsored monopoly regardless of the method of protection.").

190. See, e.g., Peabody v. Norfolk, 98 Mass. 452, 459–61 (1868) (finding a manufacturer entitled to injunctive relief against misappropriation by a former employee); Tabor v. Hoffman, 23 N.E. 12, 13 (N.Y. 1889) (finding a manufacturer entitled to preventative injunctive relief against misappropriation by a competitor).

191. See, e.g., State v. Loomis, 881 N.W.2d 749, 761 (Wis. 2016) (considering the trade secret status of a risk assessment program employed against a defendant who was neither a competitor nor a former employee); see also Katyal, The Paradox of Source Code Secrecy, supra note 19, at 1247 (noting that recent defendants' motivations are "not to compete with a trade secret holder but rather to investigate a particular source of information").

192. See, e.g., *Loomis*, 881 N.W.2d at 761 (failing to consider the absence of a confidential or competitive relationship between the algorithm owner and the defendant).

193. See Robin Feldman & Charles Tait Graves, Naked Price and Pharmaceutical Trade Secret Overreach, 22 Yale J.L. & Tech. 61, 82 (2020) ("Although over broad trade secrecy assertions are not new, the problem now extends far beyond traditional civil litigation disputes between former employers and departing employees—the customary domain of trade secret law.").

194. See, e.g., *Loomis*, 881 N.W.2d at 761 (extending trade secrecy protection over the COMPAS algorithm and its ancillary information without scrutinizing the trade secret status of those materials).

195. See supra section II.B (addressing the effects on accuracy, fairness, and validity challenges).

for competitors to reverse engineer and improve existing software.[196] But such invocations of trade secret protection surpass the bounds anticipated by the doctrine.[197] To address this departure from first principles, courts and scholars must revisit the foundations of trade secret law to determine whether algorithmic materials deserve trade secret protection.[198]

A. *The Value and Secrecy Requirements of Trade Secrets*

To start, this Note identifies the principles shared across early trade secret authorities. Common law jurisdictions that follow the First Restatement adopt a multifactor balancing test that generally examines (1) the invention's investment costs and value to the creator,[199] (2) the difficulty among competitors of reverse engineering the invention,[200] and (3) the invention's secrecy.[201] States under the UTSA require that trade secrets (1) derive independent economic value from their secrecy and (2) are subject to reasonable efforts to maintain their secrecy.[202] Although they articulate different factors, these authorities share fundamental requirements that: (1) the value of the trade secret is derived from its secrecy ("value requirement"), and (2) the trade secret is indeed secret ("secrecy requirement").

Because developers routinely conceal their technology from the public,[203] algorithms and ancillary information typically satisfy the secrecy requirement. But because courts adopt conflicting approaches to assessing value[204]—or even fail to scrutinize value altogether[205]—algorithm owners routinely enjoy trade secret protection over materials that do not satisfy

196. See supra section II.C (discussing the effect on competition).

197. See supra section II.D.

198. See Fla. ex rel. Atty. Gen. v. U.S. Dep't of Health & Hum. Servs., 648 F.3d 1235, 1282, 1289 (11th Cir. 2011) (deciding to "begin with first principles" when addressing a "novel" extension of constitutional doctrine), rev'd in part, aff'd in part sub nom. NFIB v. Sebelius, 567 U.S. 519 (2012).

199. The First Restatement states that "the value of the information" and "the amount of effort or money expended . . . in developing the information" are relevant factors for determining the subject matter of trade secrets. Restatement of Torts § 757 cmt. b (1939).

200. According to the First Restatement, courts should also consider "the ease or difficulty with which the information could be properly acquired or duplicated by others" when defining trade secrets. Id.

201. The First Restatement notes the relevance of the extent to which the information is known outside the business, the extent to which those involved with the business know the information, and the extent to which measures are taken to protect the information's secrecy in defining trade secrets. See id.

202. See Unif. Trade Secrets Act § 1(4) (Unif. L. Comm'n 1985).

203. See, e.g., State v. Pickett, 246 A.3d 279, 301 (N.J. Super. Ct. App. Div. 2021) (describing how developers are "shrouding the source code and related documents in a curtain of secrecy").

204. See supra notes 113–119 and accompanying text.

205. See supra notes 120–122 and accompanying text; see also, e.g., State v. Loomis, 881 N.W.2d 749, 761 (Wis. 2016) (failing to scrutinize the COMPAS algorithm's trade secret status).

the value requirement.[206] Furthermore, developers now claim trade secret protection to evade public access efforts by parties who are neither competitors nor employees, departing from the traditional structure of misappropriation claims.[207] Because secluding algorithmic materials deviates from first principles and opposes the public's profound interest in transparency, courts must reassess the protection they award to automated programs and ancillary information. To redefine the trade secret status of algorithmic materials, this Note derives a new framework based on *Tabor v. Hoffman*,[208] an 1889 case that clarifies the value requirement.

B. *Revisiting the Value Requirement*

Currently, no coherent test or principles exist to guide courts in determining whether an invention is valuable enough to constitute a trade secret.[209] But the early case *Tabor v. Hoffman* offers key guiding principles to assess the value of particular types of inventions—specifically, ones that produce a valuable output based on an input, such as blueprints, formulas, and algorithms.[210] In the late 1800s, a manufacturer sought to restrain a competitor from using his "patterns" or blueprints for manufacturing a pump.[211] The New York Court of Appeals considered whether the patterns for the pump were valid trade secrets in light of the fact that, while the complainant guarded the patterns in his private possession,[212] he sold the pumps on the public market.[213] Because the patterns were secret, the issue for the court was whether they derived enough value to warrant trade secret protection.[214] Finding a valid secret in the patterns,[215] *Tabor* articulated a coherent set of principles for measuring value.[216]

1. *Reverse Engineering Must Be Difficult.* — *Tabor* evaluated an innovation's value based on the advantage that it offered competitors for purposes of reverse engineering. To introduce the concept of reverse

---

206. For an explanation of why ancillary information is not a trade secret, see infra section III.C.

207. See supra notes 190–193 and accompanying text.

208. 23 N.E. 12, 13 (N.Y. 1889).

209. See supra section II.A.

210. 23 N.E. 12–13. For a comparison between the materials at issue in *Tabor* and *Loomis*, see infra note 238 and accompanying text.

211. See *Tabor*, 23 N.E. at 12 (discussing whether the plaintiff could bar the defendant from copying a secret blueprint plan for producing the plaintiff's pump technology).

212. Id. at 12 (describing how even though the pump technology was public, the plaintiff devoted considerable efforts to keeping the patterns secret).

213. Id. (describing how "the plaintiff had placed the perfected pump upon the market").

214. See id. at 13 ("As more could be learned by measuring the patterns, than could be learned by measuring the component parts of the pump, was there not a secret that belonged to the discoverer . . . ?").

215. Id. (holding that the "patterns were a secret device").

216. Id. at 12 (determining that the patterns "greatly aided, if they were not indispensable, in the manufacture of the pumps" through the logic of reverse engineering).

engineering, the court presented a hypothetical involving "a secret formula for compounding medicines":[217]

> If a valuable medicine, not protected by patent, is put upon the market, any one may, if [they] can by chemical analysis and a series of experiments, or by any other use of the medicine itself, aided by [their] own resources only, discover the ingredients and their proportions. If [they] thus find[] out the secret of the proprietor, [they] may use it to any extent that [they] desire[] without danger of interference by the courts.[218]

First, the court described reverse engineering as a lawful method of competition, stating that a competitor may "use [the medicine] to any extent that [they] desire[]" as long as they discover its formula through "chemical analysis," "experiments," or "any other use of the medicine."[219] Next, the court determined that the formula was a valuable invention deserving of trade secret protection[220] because it would be difficult for competitors to reverse engineer the medicine without its guidance. Without the formula, competitors could recreate the medicine only by conducting "chemical analysis and a series of experiments" on "ingredients."[221] In other words, the formula derived value from its secrecy because, had it been public knowledge, competitors could have reaped its benefits without investing in the costs and labor of reverse engineering.

Extending this reasoning to the materials at issue, the court concluded that the patterns were also valuable secrets because reverse engineering the pump from "brass or iron" materials[222] would be difficult, requiring a "series of experiments, involving the expenditure of both time and money."[223] Just as the formula specified "the ingredients and their proportions" for "valuable medicine,"[224] the patterns "greatly aided, if they were not indispensable, in the manufacture of the pumps."[225] Both inventions were thus entitled to protection.

Through the logic of reverse engineering, *Tabor* presents a key principle for measuring value: An innovation is valuable if its absence makes it difficult for competitors to reverse engineer its output from its component parts. Furthermore, because the court's protection turned on the complexity of the "experiments" and "expenditure" involved in reverse

---

217. Id. at 13.

218. Id.

219. See id.

220. See id. ("The courts have frequently restrained persons who have learned a secret formula for compounding medicines . . . while in the employment of the proprietor, from using it themselves or imparting it to others to his injury . . . .").

221. Id.

222. Id. at 12 (describing how "[t]he pump consists of many different pieces, the most of which are made by running melted brass or iron in a mould").

223. Id. at 13.

224. Id.

225. Id. at 12.

engineering, the decision clarifies a corollary proposition: An invention is not valuable if competitors can easily reverse engineer its output from its component parts alone.

These concepts of value comport with first principles by conditioning trade secret protection on the ease with which competitors can reverse engineer a product. *Tabor*'s key principle—that a creation is valuable only until competitors reverse engineer it—resists awarding intellectual monopolies and secluding information into perpetuity.[226] And the corollary principle—that trade secret law does not protect inventions when competitors can easily recreate them—avoids withholding general, noncompetitive knowledge, which may nonetheless benefit the public.[227] Together, these concepts restrain the parameters of trade secret subject matter and encourage innovation and market improvement by inviting third parties to lawfully profit when they reverse engineer more valuable products.[228] In doing so, these principles uphold trade secret law's policy objectives of promoting fair competition and innovation.[229]

2. *Reverse Engineering Must Be Feasible.* — Unlike the patterns, the pump and its component parts did not receive trade secret protection.[230] The court reasoned that the pump did not derive its value from its secrecy because competitors could access it in the public domain.[231] The component parts of the pump similarly derived no value from their secrecy because they constituted basic "brass or iron" materials that competitors could fairly use to reverse engineer the pump.[232] Due to these structural differences between the invention, its output, and its component parts, the court identified a valid trade secret only in the patterns.

The pump and its component parts also did not receive trade secret protection because secluding them would frustrate reverse engineering.[233] By permitting competitors to reverse engineer the patterns through

226. See supra notes 63–67.

227. See supra note 48 and accompanying text.

228. See supra notes 68–71, 85, 92, and accompanying text.

229. These principles also comport with the practices of many modern courts. Consistent with the first principle, some jurisdictions find that "the ease with which the device can be 'reverse engineered' is certainly relevant to the question of whether or not the device *remains* a 'trade secret.'" See Walker Mfg. v. Hoffmann, Inc., 261 F. Supp. 2d 1054, 1082 (N.D. Iowa 2003). Similarly, the second principle aligns with requirements that trade secrets are neither "readily ascertainable," Unif. Trade Secrets Act § 1(4) (Unif. L. Comm'n 1985), nor "readily duplicated without considerable time, effort, or expense," Stenstrom Petrol. Servs. Grp., Inc. v. Mesch, 874 N.E.2d 959, 972 (Ill. App. Ct. 2007).

230. *Tabor*, 23 N.E. at 12 (limiting trade secret protection to the patterns for the pump).

231. See id. ("As the plaintiff had placed the perfected pump upon the market, without obtaining the protection of the patent laws, he thereby published that invention to the world, and no longer had any exclusive property therein.").

232. Id. at 12–13 (describing how competitors may reverse engineer the pump by engaging in a "series of experiments, involving the expenditure of both time and money" upon the "brass or iron" pieces that compose the pump).

233. See id. at 13. For a discussion of the barriers to reverse engineering algorithms when competitors lack access to input data, see supra notes 185–189 and accompanying text.

"chemical analysis and a series of experiments," the *Tabor* court anticipated that competitors could access the "component parts" necessary for conducting those experiments.[234] Similarly, when stating that competitors could reverse engineer the patterns by "any other use of the [product] itself," the court assumed that the pump would be available in the public domain for competitors to fairly reference, study, and deconstruct.[235] Thus, implicit in the design of reverse engineering was the expectation that trade secret law would not obscure the product and its component parts from competitors. As a result, *Tabor* reveals an additional rule for defining the parameters of trade secret subject matter: The materials necessary for competitors to fairly reverse engineer a valuable invention are not themselves trade secrets.

This element upholds the first principles of trade secret law by effectuating the reverse engineering exception. Without this requirement—that the materials necessary for reverse engineering are public—reverse engineering would be impossible in certain circumstances, and trade secret holders could monopolize their creations.[236] This rule thus protects the fundamental design of trade secret law by ensuring that reverse engineering is always possible.[237]

3. *Three-Element Framework.* — *Tabor* is a paragon case to guide courts in determining the trade secret status of software like COMPAS because the patterns at issue structurally resemble algorithms; importantly, the patterns and algorithms both produce valuable output from a given input.[238] The opinion clarifies that for creations to constitute valuable secrets, it must be difficult[239]—but not impossible[240]—for competitors to reverse engineer them. In light of *Tabor*, this Note derives the following elements for determining whether innovations similar to the patterns (i.e., blueprints, formulas, or algorithms that produce an output from a given input) satisfy the value requirement:[241]

1. An invention is a valuable trade secret if it is difficult for competitors to reverse engineer its output from component parts.

2. An invention is not a valuable trade secret if competitors can easily reverse engineer its output from component parts.

---

234. See *Tabor*, 23 N.E. at 13.

235. See id.

236. See supra notes 63–67 and accompanying text.

237. See supra notes 68–71, 85, 92, and accompanying text.

238. The patterns and algorithms are inventions of similar design. In *Tabor*, the patterns (i.e., the innovation) produced a pump (i.e., the output) from brass or iron component parts (i.e., the inputs). See *Tabor*, 23 N.E. at 12. Similarly, algorithms like COMPAS (i.e., the innovation) produce risk scores (i.e., the output) from training data (i.e., the inputs). See State v. Loomis, 881 N.W.2d 749, 761 (Wis. 2016).

239. See supra section III.B.1.

240. See supra section III.B.2.

241. To constitute a trade secret, the invention must also satisfy the secrecy requirement. See supra section III.A.

3. The materials necessary for competitors to reverse engineer a valuable invention are not themselves trade secrets.

C. *Reconsidering Algorithmic Materials*

This framework clarifies the parameters of trade secret subject matter in the algorithmic context. Like the medicinal formula and patterns at issue in *Tabor*, algorithms are secret inventions that produce an output (i.e., predictions of future recidivism) from an input (i.e., criminal records).[242] By measuring value through the logic of reverse engineering, *Tabor* guides courts to separate trade secret from non-trade-secret information when developers seek broad protection for algorithmic materials.[243] To demonstrate, this Note revisits the COMPAS algorithm and ancillary information under its three-element framework.

1. *COMPAS Algorithm.* — COMPAS's source code falls squarely within this Note's definition of trade secrets. To meet the value requirement, an invention's output must be difficult but not impossible to reverse engineer.[244] Because of their complex development and methodology, algorithmic functions are costly and challenging to reverse engineer from their component parts.[245] Algorithmic source code, then, satisfies the value requirement of trade secrets. As long as creators protect their programs from wrongful disclosure in satisfaction of the secrecy requirement, trade secret law will protect source code until competitors reverse engineer them.[246] The COMPAS software is thus a valid secret under this Note's framework.[247]

---

242. See supra note 238 and accompanying text.

243. See supra notes 233–235 and accompanying text; see also Katyal, Private Accountability, supra note 175, at 125 (cautioning that corporate entities often claim overbroad assertions of trade secrecy status over their algorithms and related information).

244. See supra section III.B.2.

245. See Kapczynski, supra note 7, at 1410 ("The 'black boxes' created by AI . . . make reverse engineering more difficult . . . ."); Perel & Elkin-Koren, supra note 133, at 185 (describing how an algorithm's "mathematical complexity and learning capacities make it impenetrable").

246. For a description of reverse engineering in *Tabor*, see supra text accompanying notes 217–221.

247. Although this Note does not object to the trade secret status of source code, it maintains that ancillary information should not receive trade secret protection in an effort to further algorithmic transparency. The disclosure of ancillary information is crucial because access to the source code in isolation may not elucidate algorithmic operations and performance. See Katyal, The Paradox of Source Code Secrecy, supra note 19, at 1249 (arguing that "simply reading the code does not make it interpretable without the ability to plug in data and see how the algorithm actually functions"); Levine, supra note 133, at 40 ("Public access to an algorithm's source code does not guarantee that the public will have the resources and knowledge needed in order to understand it, scrutinize it, or even care."); Anupam Chander, The Racist Algorithm?, 115 Mich. L. Rev. 1023, 1024–25 (2017) (reviewing Frank Pasquale, The Black Box Society: The Secret Algorithms that Control Money and Information (2015)) (arguing that developers must provide "transparency of inputs and results" for the public to determine whether "the algorithm is generating discriminatory impact" (emphasis omitted)).

2. *Summary Information.* — Under this Note's proposed framework, an invention is not valuable if competitors can easily reverse engineer its output from its component parts.[248] Unlike the patterns in *Tabor*, which were derived from "experiments" and "expenditure of both time and money,"[249] summary information is readily calculated from output data. Developers may determine a software's accuracy across different categories and groups by analyzing algorithmic output alone.[250] Because summary information is either "readily ascertainable" or easily reverse engineered, it is not a trade secret.[251]

This determination avoids secluding beneficial summary information from the public. Access to intelligible information on algorithmic performance enables consumers to identify high-quality software and competitors to create new technologies that minimize discriminatory outcomes.[252] Because it improves the software marketplace, classifying summary information as non-trade-secret material comports with first principles.

Access to summary information also protects accused parties' right to defend their liberty. Mr. Loomis challenged the Wisconsin Supreme Court's consideration of automated risk assessments on the grounds that (1) COMPAS's proprietary nature prevented him from assessing its scientific validity, and (2) COMPAS impermissibly considered gender in its calculation of risk scores.[253] Because the court refused to compel Northpointe to share summary information on the algorithm's accuracy or analysis of gender, however, Mr. Loomis could not offer empirical bases to support his claims. As a result, he was unable to effectively appeal his sentence.[254] After the court's unfavorable ruling against Mr. Loomis, ProPublica reverse engineered the COMPAS algorithm and determined that the software was racially biased.[255] ProPublica's findings suggest that

---

248. See supra section III.B.3.

249. See Tabor v. Hoffman, 23 N.E. 12, 13 (N.Y. 1889).

250. For example, ProPublica reverse engineered summary information on COMPAS's overall accuracy and accuracy by race and gender using risk scores (i.e., output data) and criminal and incarceration records (i.e., input data). See Larson et al., supra note 145.

251. See Fin. Info. Techs., LLC v. iControl Sys., USA, LLC, 21 F.4th 1267, 1273 (11th Cir. 2021) (stating that "aspects of computer software that *are* readily ascertainable don't qualify" as trade secrets).

252. See supra section II.C.

253. State v. Loomis, 881 N.W.2d 749, 753 (Wis. 2016).

254. See Wexler, Life, Liberty, and Trade Secrets, supra note 12, at 1353 (arguing that trade secret evidentiary privilege should not exist in criminal proceedings because it bars defendants from challenging the validity of algorithms and defending their liberties); Alyssa M. Carlson, Note, The Need for Transparency in the Age of Predictive Sentencing Algorithms, 103 Iowa L. Rev. 303, 306 (2017) (objecting to court reliance on algorithmic risk scores as "defendants have no way of validating the accuracy of the formulas").

255. See Larson et al., supra note 145 (finding that the COMPAS algorithm misclassified Black defendants as posing a high risk for recidivism almost two times more often than white defendants); see also infra section III.C.3 (discussing ProPublica's reverse engineering).

court-ordered disclosure of summary information would have called into question COMPAS's accuracy and fairness. Had the court permitted Mr. Loomis to access this evidence, he may have successfully appealed his sentence on his two initial grounds and the additional ground that the software impermissibly considered race.[256] The ProPublica investigation demonstrates how people like Mr. Loomis can meaningfully challenge the validity and propriety of risk assessment tools when courts decline to extend trade secret protection to summary information.[257] Furthermore, given that ProPublica's analysis did not require access to COMPAS source code, courts may preserve the proprietary interests of developers by limiting disclosure to summary information and maintaining trade secret protection over algorithms.[258]

3. *Input and Output Information.* — Like summary information, input and output information fall outside the scope of trade secret protection. *Tabor* clarifies that trade secret law may not seclude materials necessary for competitors to fairly reverse engineer a valuable invention.[259] The input data upon which developers train their programs are component parts of the algorithm necessary for its reverse engineering.[260] Output information is the product generated from each iteration of the algorithm.[261] Like input information, algorithmic outputs are not entitled to protection because competitors must reference them for purposes of reverse engineering.[262]

The classification of input and output information as non-trade-secrets aligns with trade secret law's policy objective. Algorithms are distinct from other trade secrets in that they are extremely difficult to reverse engineer even if competitors have access to relevant inputs and

256. ProPublica's analysis also revealed that (1) the COMPAS algorithm was accurate only 63.6% of the time, and (2) female defendants were more likely to receive higher risk scores than male defendants despite "their lower levels of criminality overall." See Larson et al., supra note 145. These findings support Loomis's initial claims that COMPAS was inaccurate and impermissibly considered gender.

257. In 2016, the Maryland Court of Special Appeals recognized the need for courts to access intelligible algorithmic information when evaluating claims of constitutional deprivations. See State v. Andrews, 134 A.3d 324, 338–39 (Md. Ct. Spec. App. 2016) (finding that courts must analyze "the functionality of the surveillance device and the range of information potentially revealed by its use . . . to make the necessary constitutional appraisal"). The court rejected that algorithms' proprietary nature may bar courts from accessing this valuable information. See id. at 338 ("We observe that such an extensive prohibition on disclosure of information to the court . . . prevents the court from exercising its fundamental duties under the Constitution.").

258. See Graves & Katyal, supra note 152, at 1415–16 ("[O]btaining information necessary to understand such decisionmaking may not require disclosure of actual algorithms . . . .").

259. See supra section III.B.3.

260. For a description of inputs, see supra note 134, 136, and accompanying text.

261. For a description of outputs, see supra note 134–135 and accompanying text.

262. For a discussion of *Tabor*'s assumption that inputs and outputs are not trade secrets, see supra text accompanying notes 233–237.

outputs.[263] Should input and output data receive trade secret protection, the first developer of a software would hold a monopoly over the program because it would be virtually impossible for competitors to reverse engineer this technology.[264] But trade secret law never intended to grant enduring intellectual monopolies.[265] Instead, early courts assumed that reverse engineering would be a feasible yet difficult enterprise.[266] In light of this departure from first principles, courts must refrain from protecting input and output data as trade secrets.

The decision to not seclude input or output information also reduces algorithmic discrimination. In 2016, ProPublica reverse engineered the COMPAS program to identify and mitigate bias. The journal filed public record requests to obtain input data (criminal histories and incarceration records) and output data (risk scores for more than 11,000 defendants) from previous iterations of the software.[267] From these inputs and outputs, ProPublica reverse engineered COMPAS and calculated summary information that elucidated the program's methodology and performance.[268] The analysis revealed that COMPAS yielded an accuracy rate of approximately sixty-four percent and was twice as likely to wrongly predict that Black defendants would likely reoffend as compared to white defendants.[269] From these results, ProPublica concluded that COMPAS adopted biased racial predictors.[270]

The reverse engineering of the COMPAS tool comports with first principles by exposing algorithmic harms to market actors. By filing public records requests, ProPublica accessed input and output data (which this Note categorizes as non-trade-secret) to replicate COMPAS's functions.

---

263. Jeanne C. Fromer, Machines as the New Oompa-Loompas: Trade Secrecy, the Cloud, Machine Learning, and Automation, 94 N.Y.U. L. Rev. 706, 718 (2019) (arguing that advances in artificial intelligence have strengthened trade secret law by technically undermining "independent discovery, reverse engineering, and the free use of an employee's general knowledge and skill").

264. For an explanation of why secluding input and output data renders reverse engineering functionally impossible, see supra notes 185–189 and accompanying text.

265. See supra notes 36–40, 63–67, and accompanying text.

266. For an analysis of the disincentives to innovate when reverse engineering is easy or impossible, see supra section I.B.3.

267. See Larson et al., supra note 145.

268. See id. ("To test racial disparities in the score controlling for other factors, we created a logistic regression model that considered race, age, criminal history, future recidivism, charge degree, gender and age. We used those factors to model the odds of getting a higher COMPAS score."); see also Levendowski, supra note 15, at 600 ("Armed with COMPAS risk scores and a dataset built from those individuals' criminal records, ProPublica reverse engineered which characteristics caused the COMPAS algorithm to predict higher recidivism risk scores.").

269. Larson et al., supra note 145 (calculating an overall accuracy rate of 63.6% and finding that the COMPAS algorithm was "nearly twice as likely" to misclassify Black defendants compared to white defendants).

270. Levendowski, supra note 15, at 601 (describing how, "based on ProPublica's testing, the scores were also racist").

The journal's investigation then yielded summary information (also envisioned by this Note as non-trade-secret) that unveiled the program's error rate and biased performance. Because ProPublica's analysis revealed crucial summary information to consumers and competitors, it enabled the market to trade on key product features—such as accuracy and fairness—that may improve the quality of algorithms.[271]

D. *Balancing Proprietary Interests With Calls for Algorithmic Transparency*

The conclusion that trade secret law does not protect ancillary information furthers transparency efforts and upholds first principles while maintaining developers' proprietary interests. At a minimum, trade secret law should not bar defendants from scrutinizing the accuracy of risk assessment programs[272] or prohibit competitors or public interest groups from obtaining input and output data necessary for reverse engineering.[273] Outside of trade secret law, program developers already benefit from statutory and common law protections over ancillary information. Courts routinely issue protective orders to protect the confidentiality of disclosed materials,[274] and public access laws like the Freedom of Information Act (FOIA) exempt government agencies from disclosing information in numerous circumstances, such as when data implicate national security interests.[275] Statutes like the Health Insurance Portability and Accountability Act (HIPAA) impose heightened data security protections over certain types of personal information that limit third-party access.[276] Consequently, even without trade secret protection, sensitive input data receives robust safeguards.

Even if ancillary information enters the public domain, source code will continue to receive legal protection.[277] Since the nineteenth century, courts have granted trade secret status to hidden blueprints or formulas for a product even though the product and its component parts were

---

271. Id. at 609 ("A newcomer may be motivated to create an AI system without the race and gender biases of systems from the incumbent AI creators.").

272. See supra section III.C.2.

273. See supra section III.C.3.

274. See, e.g., Flores v. Stanford, No. 18 Civ. 02468, 2021 WL 4441614, at *1 (S.D.N.Y. Sept. 28, 2021) (ordering that Northpointe produce the underlying data and analytics of the COMPAS algorithm subject to a protective order); see also Wexler, Life, Liberty, and Trade Secrets, supra note 12, at 1429 (arguing that "narrow criminal discovery and subpoena powers combined with protective orders should suffice to safeguard the interests of trade secret owners to the full extent reasonable").

275. See, e.g., 5 U.S.C. § 552(b) (2018) (exempting nine categories of data from disclosure requirements).

276. HIPAA requires that health care providers implement safeguards to maintain the confidentiality of patient information. 42 U.S.C. § 1320d-2(d)(2) (2018). In turn, FOIA exempts the disclosure of health information protected by HIPAA. 5 U.S.C. § 552(b)(3) (permitting agencies to withhold matters "specifically exempted from disclosure by statute").

277. See Tabor v. Hoffman, 23 N.E. 12, 13 (N.Y. 1889) (clarifying that the public nature of an invention's inputs and outputs do not deprive the trade secret status of the invention itself).

publicly available.[278] Furthermore, the right of competitors to fairly reverse engineer software from public ancillary data will "not typically threaten an innovative manufacturer" due to the "costliness of reverse engineering."[279] Given the complexity of algorithmic development and execution, reverse engineering will remain difficult even when competitors have access to input and output information.[280] Sophisticated programs will enjoy extended periods of protection because competitors can reverse engineer those algorithms only if they invest in high development costs.[281] The law and market will thus continue to safeguard programs deserving of trade secret status.

Lastly, the treatment of ancillary information as non-trade-secret aligns with new efforts by courts to answer calls for algorithmic transparency. Recently, judges have ordered companies to disclose their source code under protective order after defendants questioned the validity of criminal justice software.[282] One investigation revealed that certain breathalyzer technology contained a "significant flaw"[283] and consisted of general algorithms that arguably failed to meet the elements of a trade secret.[284] Courts frequently note that access to source code, summary information, and other "raw materials" is "integral to the building of an effective

278. See AirFacts, Inc. v. de Amezaga, 909 F.3d 84, 96 (4th Cir. 2018) (holding that "a trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain" as long as the unique combination "affords a competitive advantage and is a protectable secret" (quoting Imperial Chem. Indus. v. Nat'l Distillers & Chem. Corp., 342 F.2d 737, 742 (2d Cir. 1965))); Coca-Cola Bottling Co. of Shreveport v. Coca-Cola Co., 107 F.R.D. 288, 289, 291 (D. Del. 1985) (finding that the "tremendous market recognition" of the Coca-Cola product did not implicate the trade secret status of its formula "kept in a security vault"); *Tabor*, 23 N.E. at 13 (holding that the "patterns were a secret device that was not disclosed by the publication of the pump").

279. Samuelson & Scotchmer, supra note 37, at 1586; see also *Tabor*, 23 N.E. at 13 (describing the investment costs that prevent competitors from easily reverse engineering valuable trade secrets).

280. See supra notes 185–189 and accompanying text for a discussion of the unique difficulties in reverse engineering algorithms.

281. See Rycoline Prod., Inc. v. Walsh, 756 A.2d 1047, 1055 (N.J. Super. Ct. App. Div. 2000) ("The more difficult, time consuming and costly it would be to develop the product, the less likely it can be considered to be 'reverse engineerable.'"); McClary v. Hubbard, 122 A. 469, 473 (Vt. 1923) ("The simpler and commoner the principles entering into the combination constituting a secret device are, the more likely is the device to be discovered and copied or reproduced."); see also Reichman, supra note 91, at 659 (arguing that reverse engineering does not undermine the profits of the "first on the market" as third parties must also establish themselves on the market through reliable production and marketing strategies).

282. See, e.g., Flores v. Stanford, No. 18 Civ. 02468, 2021 WL 4441614, at *1 (S.D.N.Y. Sept. 28, 2021) (requiring the disclosure of the COMPAS tool's regression models and training data to determine whether the algorithm overpenalizes juveniles); State v. Chun, 943 A.2d 114, 123 (N.J. 2008) (ordering a breathalyzer manufacturer to share its source code with an independent third party for an assessment of its scientific validity); State v. Pickett, 246 A.3d 279, 279 (N.J. Super. Ct. App. Div. 2021) (permitting a defendant to access the source code and documentation of a forensic software for purposes of challenging the technology's validity).

283. *Chun*, 943 A.2d at 157.

284. See supra note 129 and accompanying text.

defense."[285] Recently, a federal district court in New York ordered that Northpointe produce the underlying data and methodology of COMPAS subject to a protective order.[286] These decisions illustrate contemporary courts' willingness to address opacity concerns by ordering companies to disclose their source code, summary information, and input and output data. Furthermore, given that these court-ordered investigations have yet to divulge the secrecy of the software in question,[287] limited disclosure regimes—such as the framework adopted by this Note—achieve algorithmic transparency goals without jeopardizing proprietary interests.

CONCLUSION

Rather than seclude proprietary information, early trade secret law protected a public market of ideas and creations where "competition reign[ed]."[288] But recent invocations of trade secret law to conceal risk assessment algorithms and their ancillary information contravene these first principles.[289] Such safeguards prevent accused parties from defending their liberty, competitors from improving existing programs, and public interest groups from mitigating algorithmic bias.[290] To remedy this shortcoming, this Note argues that trade secret law does not prevent the disclosure of algorithmic summary information to defendants like Mr. Loomis or of input and output data to public interest groups. ProPublica's successful reverse engineering of COMPAS illustrates how public access to ancillary information furthers algorithmic transparency while still maintaining the proprietary interests of trade secret holders.[291] By meaningfully policing the trade secret status of algorithmic materials, courts can address public demands for algorithmic fairness and align the doctrine with its first principles.

---

285. See, e.g., *Pickett*, 246 A.3d at 299 (internal quotation marks omitted) (quoting State ex rel. A.B., 99 A.3d 782, 790 (N.J. 2014)).

286. See *Flores*, 2021 WL 4441614, at *1 (requiring the disclosure of "the normative dataset used to create and normalize COMPAS" (i.e., ancillary input data) and "the regression models for two COMPAS 'scales': (a) the General Recidivism Risk Scale, and (b) the Violent Recidivism Risk Scale" (i.e., the algorithm)). The court compelled this disclosure to determine "how or whether COMPAS considers the diminished culpability of juveniles and the hallmark features of youth." Id. (quoting Second Amended Complaint at 54, *Flores*, 2018 WL 10626399).

287. See, e.g., id. at *4 (finding that expert review of compelled materials "is paramount to Plaintiffs' prosecution of this case" and disclosure "poses minimal risk of competitive injury in light of the Protective Orders"); *Chun*, 943 A.2d at 123 (designating "an independent software house to review the source code" to protect its secrecy); *Pickett*, 246 A.3d at 283–84 ("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.").

288. Kapczynski, supra note 7, at 1390.

289. See supra section II.D.

290. See supra sections II.B–.C.

291. Levendowski, supra note 15, at 599 ("ProPublica's groundbreaking exposé on the black box algorithm behind Northpointe's COMPAS algorithm has quickly become a canonical example of using both techniques to reveal and interrogate bias.").