ARTICLE

ELEVATING CORPORATE PROFITS OVER INDIVIDUAL LIBERTY:

COMPARING AI TRADE SECRET PRIVILEGE IN CRIMINAL PROCEEDINGS WITH PATENT LITIGATION

*Andrew C. Michaels**

INTRODUCTION

Various courts across the country have been using privately developed artificial intelligence (AI) tools as aids in criminal proceedings. For example, AI tools purport to predict the risk that a defendant will be a recidivist, with a higher risk generally

*Assistant Professor of Law, University of Houston Law Center. This project was supported by the Community Responsive Algorithms for Social Accountability (CRASA) award funded by the National Science Foundation (NSF) (Award #2131504), in conjunction with team members Ryan Kennedy, Lydia Tiede, and Ioannis Kakadiaris. The author thanks Daria Adler and Bill Bandy for helpful research assistance related to this project.

weighing in favor of a longer criminal sentence. Like AI generally, these tools are often something of a black box, with not much being known about how they work or even the factors they look at in making their risk assessments. Concerns have been raised and some evidence suggests that these tools may be biased against certain racial minority groups.

When evidence or recommendations from these tools are introduced in proceedings against a criminal defendant, the defendant often will understandably seek disclosure of technical information as to how the tools work and what factors the tools are relying upon, so as to be able to advance a rebuttal or challenge to the AI tool's recommendations. Yet the private companies that create and own these tools will often refuse to provide such information, claiming that it is a proprietary trade secret and is privileged from discovery. Courts often honor such claims of trade secret privilege while nevertheless considering the output from these AI tools without requiring further disclosure of information.

This brief essay will contribute to the literature primarily by highlighting a comparison with claims of trade secret privilege in patent litigation. Plaintiffs asserting claims of patent infringement often seek discovery into the defendant's source code to find evidence confirming infringement of the patent claims, and the defendant will often seek to block such discovery by claiming that the source code is a valuable trade secret. But in that context, courts will often compel the requested discovery despite the claims of trade secret privilege, usually under a protective order to limit the possibility of further dissemination of the trade secret.

If anything, the case for discovery into trade secret protected information should seemingly be stronger, not weaker, in the criminal context as compared with the patent litigation context. In the criminal context, the party seeking discovery is threatened with the loss of their liberty, rather than the mere inability to prove patent infringement. Moreover, the risk to the party claiming trade secret privilege seems lower in the criminal context, in that the average criminal defendant would generally be in no position to use the disclosed information to the competitive disadvantage of the trade secret holder, as compared with a patentee plaintiff who may well be a business competitor of the trade secret holder. For similar reasons, the policies underlying trade secret law counsel more strongly in favor of refusing to order discovery in the patent litigation context as compared with the criminal context.

But perversely, claims of trade secret privilege tend to be honored more often in the criminal context as compared with the patent litigation context. This essay explores this anomaly as

follows. Part I provides some background on the use of AI risk assessment tools and the attendant claims of trade secret privilege in the criminal context. Part II discusses claims of trade secret privilege in the patent litigation context. Part III evaluates claims of trade secret privilege in light of the purposes of trade secret law. The essay then concludes by comparing arguments in favor of privilege versus disclosure between the two contexts, offering some recommendations for reform suggested by this analysis.

I. TRADE SECRET PRIVILEGE FOR AI TOOLS IN CRIMINAL PROCEEDINGS

In various cases where AI tools have been used against a criminal defendant, courts have honored claims of trade secrecy and refused to compel the disclosure of information about the tool requested by the criminal defendant. This has already been well documented in the literature, such as by Professor Rebecca Wexler, who explains that developers "often assert that details about how their tools function are trade secrets," and as a result "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."[1]

Perhaps the most commonly used and most discussed AI tool in criminal proceedings is the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) algorithm which was developed by the Northpointe Institute for Public Management.[2] This tool is used in criminal sentencing, and as explained by Professor Hannah Bloch-Wehba, "weighs a number of factors, such as criminal history, education, employment, age, and substance abuse history," to generate a "risk score" which is "intended to predict the likelihood of pretrial recidivism, general recidivism, and violent recidivism."[3]

The use of AI tools such as COMPAS is controversial. On the positive side, these tools purportedly are able to predict the risk of recidivism more accurately and consistently than the personal intuitions of the various judges who engage in criminal sentencing. But these tools have some serious drawbacks. Inappropriately and

---

1. Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1349-50 (2018).

2. *See generally* State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

3. Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1289 (2020).

unfairly, they use generalizations from group characteristics to form conclusions against individual criminal defendants.[4]

For example, if living in a certain zip-code happens to correlate with increased risk of recidivism, the algorithm may increase the defendant's risk score merely based on that. But this seems unfair and inappropriate because there should be nothing at all worthy of condemnation (let alone increased jailtime) about merely living in a certain zip-code.

A computer scientist might think that if using the group characteristic results in more accurate risk scores on the aggregate, it should be used, but a lawyer or judge should recognize a fairness issue here, as would the individual defendant being penalized for their group characteristics. Yet our societal infatuation with technology seems to be resulting in these fairness concerns being swept under the rug in many cases.

Particularly troubling, as has been discussed and debated in the literature, a ProPublica study "found through statistical analysis that black defendants evaluated by COMPAS tools were more likely to be incorrectly labeled as higher risk without committing a future crime in the requisite time period, as compared with white defendants who were more likely to be incorrectly labeled as lower risk but actually committed crimes in the same time period."[5] Obviously, lengthening sentences based on group characteristics such as race, over which the individual has no control, raises salient fairness and potential constitutional due process concerns.[6]

In order to challenge the inappropriate application of group characteristics to their personal situation, a criminal defendant would need to know some technical details about how the AI tool works and what characteristics it is relying on, both in general and as applied to their particular situation. Yet criminal defendants can be impeded in challenging their risk assessment scores by claims of trade secrecy.[7]

In evaluating claims of trade secret privilege, courts generally weigh the risk of harm from disclosure against the need for the

---

4. *See generally* KATHERINE B. FORREST, WHEN MACHINES CAN BE JUDGE, JURY, AND EXECUTIONER: JUSTICE IN THE AGE OF ARTIFICIAL INTELLIGENCE (2021).

5. Jessica M. Eaglin, *Constructing Recidivism Risk*, 67 EMORY L. J. 59, 96 (2017) (citing Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016)).

6. *See, e.g.*, Michael Brenner et. al., *Constitutional Dimensions of Predictive Algorithms in Criminal Justice*, 55 HARV. C.R.-C.L. L. REV. 267, 287-89 (2020).

7. *See* Wexler, *supra* note 1, at 1354 ("A New York inmate was denied parole because of a flawed risk assessment score; he discovered an error in the input data used to generate his score but could not prove the significance of that error because the developer considers the weights of input variables to be trade secrets."); *id.* at 1369-70.

information.[8] While courts will generally grant discovery of trade secrets subject to a protective order in civil cases, courts frequently deny discovery into trade secrets altogether in criminal cases.[9] Oddly, courts in the criminal context seem to presume that any disclosure, even under a protective order, will lead to business harm to the trade secret holder through eventual disclosure of the trade secret to business competitors of the trade secret holder.[10] The oddity of this presumption is highlighted when contrasted with the patent litigation context, where courts are often more skeptical as to the likelihood that disclosure under a protective order will cause any business harm.[11]

II. TRADE SECRET PRIVILEGE IN PATENT LITIGATION

The issue of trade secret privilege arises frequently in patent litigation. Often, for example, the plaintiff patent holder requests to examine the defendant's source code to find evidence supporting the assertion that the defendant is in fact infringing the patent claims, and the defendant attempts to shield its source code from disclosure by claiming trade secrecy.[12] As the court observed in the high stakes "smart phone wars" between Apple and Samsung: "In a typical patent infringement case involving computer software, few tasks excite a defendant less than a requirement that it produce source code" as "[e]ngineers and management howl at the notion of providing strangers, and especially a fierce competitor, access to the crown jewels."[13]

As that court explained, "source code production is disruptive, expensive, and fraught with monumental opportunities to screw

---

8. *Id.* at 1396 (citing Bridgestone/Firestone, Inc. v. Superior Court, 9 Cal. Rptr. 2d 709, 713 (Ct. App. 1992)).

9. *See id.* at 1401 (citing Edward J. Imwinkelried, *Computer Source Code: A Source of the Growing Controversy over the Reliability of Automated Forensic Techniques*, 66 DEPAUL L. REV. 97, 99-101 (2016)).

10. *Id.* at 1415-16.

11. *See, e.g.*, In re Subpoena to Third Party Sentieon, Inc., 2022 U.S. Dist. LEXIS 220216 (N.D. Cal. Dec. 6, 2022) ("The Court agrees with Invitae that the protective order provides sufficient protections for Sentieon's source code."); MVS Studio, Inc. v. Bingo Bean, LLC, 2011 U.S. Dist. LEXIS 157127, *6 (C.D. Cal. June 24, 2011) ("Here, the risk of competitive harm to Defendants can be minimized in two ways by the issuance of a protective order.").

12. *See, e.g.,* Drone Techs., Inc. v. Parrot S.A., 838 F.3d 1283, 1300 n. 13 (Fed. Cir. 2016) ("[I]t is well recognized among lower courts that source code requires additional protections to prevent improper disclosure because it is often a company's most sensitive and most valuable property.") (citing Via Vadis Controlling GmbH v. Skype, Inc., No. 12-MC-193-RGA, 2013 WL 836313, at *3 (D. Del. Feb. 21, 2013)).

13. *See, e.g.*, Apple Inc. v. Samsung Elecs. Co., 2012 U.S. Dist. LEXIS 62971, *10 (N.D. Cal. May 4, 2012).

up," as it raises questions such as who gets to see the code, what format must the code be produced in, what examination tools are required, etc.[14] Nevertheless, the court stated, "subject to the proportionality and burden considerations imposed by Fed. R. Civ. P. 26, when a patentee requests source code for one or more accused products, a defendant must produce it."[15]

Source code is often kept as a trade secret, so in deciding whether and the degree to which to compel the defendant to produce source code, courts will generally weigh the plaintiff's need for disclosure in order to prove their case, against the risk that disclosure may cause competitive harm to the defendant.[16] But the risk of competitive harm to the defendant can be minimized by the use a protective order limiting access to the source code, and by imposing penalties for violation of the protective order sufficient to deter such violations.[17] As such, despite the fact that plaintiffs and defendants in patent litigation are often business competitors, generally disclosure of trade secret source code will be ordered when relevant and necessary, subject to the limitations of a protective order.[18]

In contrast to the context of criminal law, courts in the civil patent litigation context have recognized that "litigators have ready-made tools at their disposal to address the merit of software-related disputes while ensuring that the source code remains protected and yet disclosed in a litigation dispute."[19] For example, one standard provision in a protective order in the patent litigation context is to require "the producing party to make source code

---

14. *Id.* at *11.

15. *Id.*

16. *See, e.g.*, MVS Studio, *supra* note 11, at *5-6 (C.D. Cal. June 24, 2011) ("[T]he risk that protection of Defendants' trade secrets will impair Plaintiffs' ability to litigate their claims must be weighed against the risk to Defendants that they may suffer competitive harm if the source code is used for non-litigation purposes.") (citing Brown Bag Software v. Symantec Corp., 960 F.2d 1465, 1470 (9th Cir. 1992)).

17. *See id.* at *6-9 ("Accordingly, the protective order shall provide that any party proven to have violated the terms thereof shall voluntarily dismiss their claims with prejudice.").

18. *See, e.g.*, Fleming v. Escort, Inc., 2010 U.S. Dist. LEXIS 101938, at *6 (D. Idaho Sept. 24, 2010) ("While the source code is obviously highly sensitive trade secret material, the Declaration of Dr. Schmidt persuades the Court that the redactions could be important, and the Protective Order assures the Court that Escort's secrets will be protected.").

19. Thales Visionix, Inc. v. United States, 149 Fed. Cl. 38, 48 (Ct. Fed. Cl. 2020) (quoting Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183, 1275-76 (2019)).

available for inspection on a standalone computer with visual monitoring by the producing party."[20]

Given these protections, "there is no elevated standard when seeking the discovery of source code," at least not in the civil context of patent litigation.[21] Courts in the criminal context would do well to recognize as well that source code and other technical information can be adequately protected while still being discoverable in litigation.

III. PURPOSES OF TRADE SECRET LAW

An examination of the purposes of trade secret law provides further reason to question the propriety of trade secret privilege for AI risk assessment tools in the criminal context.

Unlike other types of intellectual property, trade secrets generally provide only *in personam* rights against particular individuals, rather than *in rem* rights against the world. Generally, a claim for trade secret misappropriation can only lie against one who has acquired a duty to keep the information secret or acquired it by improper means.[22]

Thus, the legal status of information as a trade secret is qualified; it only provides a cause of action for misappropriation against certain legal persons with some obligation to keep the information secret and does not necessarily provide a right to keep the information secret from criminal defendants who have their liberty threatened by the use and secrecy of this information. When certain information is being used with the trade secret holder's consent to threaten an individual's liberty, a trade secret holder should forfeit the right to keep that information secret from the individual whose liberty is being threatened.

Trade secret law grew out of the common law of unfair competition and its purposes are not entirely clear. One purpose is to provide incentives to innovate by providing some degree of protection for innovative efforts that are the subject of reasonable efforts to keep secret.[23] Another purpose is to discourage companies from

---

20. LoganTree LP v. Garmin Int'l, Inc., 339 F.R.D. 171, 175-176 (D. Kan. 2021) (calling such a provision "fairly standard in a patent infringement case to protect the highly proprietary and often trade secret nature of source code").

21. *Thales*, 149 Fed. Cl. At 48 (citing Baron Servs., Inc. v. Media Weather Innovations LLC, 717 F.3d 907, 913 n.9 (Fed. Cir. 2013)).

22. *See, e.g.*, Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241 (1998); Uniform Trade Secrets Act § 1 (1985).

23. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481-82 (1974) ("The maintenance of standards of commercial ethics and the encouragement of invention are the broadly stated policies behind trade secret law.").

wastefully expending resources to protect proprietary information against any possible form of espionage.[24] Yet another purpose is to uphold certain standards of fairness and commercial morality.[25]

Claims of trade secret privilege for AI tools in the criminal context do not seem to further any of these goals. One reason is that AI tools are not easy to recreate even with some opportunity to examine technical details of the AI, due to the black box nature of AI.[26] It thus seems unlikely that an expert who has the opportunity to examine technical details of an AI risk assessment tool in the criminal context would as a result have the ability to create a competing product, even setting aside the fact that this would likely be in violation of any protective order imposed by the court.

Since AI is by its very nature difficult to recreate, it also seems unlikely that companies would engage in wasteful efforts to make such recreation more difficult merely because they know that they may need to disclose technical details subject to a protective order in criminal proceedings. And it seems even more of a stretch to suggest that the prospect of such disclosure would discourage the creation of such tools altogether.

Moreover, as noted earlier, much of trade secret law is rooted in norms about fairness, and fairness would seem to counsel strongly against a trade secret privilege in the criminal context, as doing so in a sense elevates the business needs of the AI tool proprietor over the personal liberty of the criminal defendant which is threatened by the use and secrecy of the AI tool.[27] Simply put, depriving a criminal defendant of their liberty based in part on the recommendation of an AI tool that they do not have the opportunity to examine hardly seems fair.

CONCLUSION

The greater willingness of courts to order the disclosure of trade secrets in patent litigation as compared with criminal proceedings is perverse. The general approach in both contexts is to

---

24. E.I. Dupont Denemours & Co, Inc. v. Rolfe Christopher, 431 F.2d 1012 (5th Cir. 1970) ("Our tolerance of the espionage game must cease when the protections required to prevent another's spying cost so much that the spirit of inventiveness is dampened.").

25. *See id.* at 1015 ("the undoubted tendency of the law has been to recognize and enforce higher standards of commercial morality in the business world" (quoting Hyde Corp. v. Huffines 314 S.W.2d 763 (1958)).

26. *See* Frank Pasquale, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

27. *See* Bone, *supra* note 22, at 245 ("judges seem to view trade secret law as a relatively open-ended delegation of authority to police the morality of commercial relationships").

balance the potential business harm to the trade secret holder against the relevance of and need for the information. On both scores, that the balance should favor disclosure more strongly in the criminal context.

Potential business harm from disclosure would seem to be much higher in the patent litigation context, where the parties are often competing businesses. A company that holds patents related to the defendant's business would in general be fairly capable of using the defendant's trade secrets in business competition against the defendant. By contrast, a run of the mill criminal defendant seems quite unlikely to set up a competing risk assessment tool business. The concern may be somewhat greater if the defendant is able to hire an expert to help make sense of the disclosed trade secrets, as the expert may be in a better position to use such information competitively. But this concern would still seem to be no greater than in the patent litigation contexts and can be mitigated through the use of a protective order. On the other side of the ledger, the potential harm to the party requesting disclosure is qualitatively of a different magnitude and more dire the criminal context, where the defendant is threatened with the loss of their personal liberty. By contrast, a patent holder is merely threatened with having a more difficult time making out their claim for patent infringement.

Yet somehow, courts have found the balance to come out in favor of disclosure more often in patent litigation than in criminal proceedings. One explanation for this apparent paradox might be the vastly greater resources available in high stakes patent litigation, where litigants hire armies of attorneys and expert witnesses who are able to work through the complex issues of the protective order and the details of source code examination. The average criminal defendant certainly does not have the resources to finance such extravagance.

But given that the defendant's liberty is at stake, the burden should fall on the algorithmic proprietor to disclose the workings of their product sufficient to allow the defendant fair opportunity to challenge its use. The algorithmic proprietor is in a far better position to finance such disclosure and can benefit from economies of scale in finding ways to disclose sufficient information in the many criminal cases where its algorithm is used. It should not be too difficult for the proprietor to disclose sufficient enlightening technical details without threatening its business by disclosing entirely how its algorithm was created.

Courts could simply say that these tools will not be used unless their technical details are adequately disclosed to defendants.

Given the fairness and potential constitutional issues with these tools, especially when technical details are not made transparent, this should not be a difficult thing for courts to require. This should threaten the business model of the algorithmic proprietors sufficiently to incentivize them to find a way to provide adequate transparency. Until they do so, courts could just go back to sentencing the old-fashioned way.

Requiring technical disclosure would enhance the accountability of algorithms in the criminal context and thus ultimately improve their reliability and fairness. The justice system should stop allowing companies that are unwilling to be held accountable through technical disclosure to use their algorithms to deprive criminal defendants of their liberty.