SMU Law Review Forum

Volume 76 Article 1

2023

Who Framed Roger Rabbit? Probably the Secret Codes

Jian Micah De Jesus
Southern Methodist University, Dedman School of Law

Recommended Citation

Jian Micah De Jesus, *Who Framed Roger Rabbit? Probably the Secret Codes*, 76 SMU L. REV. F. 1 (2023)

SMU Law Review Forum

Volume 76 March 2023 1-27

WHO FRAMED ROGER RABBIT? PROBABLY THE SECRET CODES!

Jian Micah De Jesus[*]

ABSTRACT

Roger Rabbit was falsely accused of murdering Marvin Acme, the owner of Toontown, after photos revealed Acme's alleged affair with Roger's wife. A few snapshots, while seemingly harmless, brought a 104-minute journey into uncovering the truth and scandal behind the murder and proving Roger's innocence. And while the camera that took the photos was not necessarily a criminal justice technology that framed Roger Rabbit, there are real-life cases where a DNA software or a breathalyzer has negatively affected many defendants. Despite the proven usefulness of these technologies, it is not a perfect method in accusing and convicting defendants. The criminal justice system, however, might disagree. Yet, there are many occasions where technology has wrongfully accused an individual, and its lack of source code transparency has created a roadblock for defense counsel.

That roadblock is known as the trade secret privilege. When defense counsel seeks access to source code information to determine the accuracy and reliability of a technology's data outputs, the owners of these technologies claim "trade secret." By claiming that privilege, trade secret holders are exercising their intellectual property right to refuse disclosure of their technologies' secret information. But at what cost?

DOI: https://doi.org/10.25172/slrf.76.1.1

[*] J.D. Candidate, SMU Dedman School of Law, May 2023; B.A. Psychology, Florida International University, April 2019. The author is immensely grateful for Jesus, who was sent by God and who bore false testimony and the punishment of iniquity to bring abundant life and healing to all who believe (Isaiah 53). The author also wants to thank her family for all their love and encouragement. She wouldn't be where she is today if it weren't for their wisdom, guidance, and support. And, finally, the author is thankful for her friends, who have continually shown her what honor, humility, and forgiveness to one another look like.

In early 2021, California Representative Mark Takano gave criminal defendants a glimpse of what the end of this seemingly absolute privilege could look like. That hopeful future clothes itself in the form of H.R. 2438, which would regulate admissibility of trade secret information and place a ban on claiming the privilege in criminal proceedings. And the bill's future may be solidified if Congress chooses to pass this bill, which it should. This Comment argues the lives and constitutional rights of defendants outweigh the protection of intellectual property in the criminal justice context. By evaluating the policy reasons favoring criminal defendants and considering the importance of trade secret rights, this Comment argues why H.R. 2438 should be passed to keep criminal justice technologies accountable and to ensure the liberty of innocent individuals.

TABLE OF CONTENTS

I. INTRODUCTION....................3
II. TRADE SECRET PRIVILEGE'S JOURNEY INTO THE COURTS 4
A. WHAT IS A TRADE SECRET? 4
B. HISTORY OF TRADE SECRET PRIVILEGE IN COURTS 7
C. DOES THE PRIVILEGE "TEND TO CONCEAL FRAUD OR OTHERWISE WORK INJUSTICE"?....................9
III. IS IT WORTH PROTECTING TRADE SECRETS AT THE EXPENSE OF CRIMINAL DEFENDANTS?....................10
A. HOW COURTS HAVE BEEN APPLYING TRADE SECRET PRIVILEGE RULES 10
B. TRADE SECRET HOLDERS: "OUR PRIVILEGE SHOULD STAY"12
C. CRIMINAL DEFENDANTS: "OUR CONSTITUTIONAL RIGHTS ARE VIOLATED" 14
IV. H.R. 2438 TO THE RESCUE?....................18
A. THE LACK OF ACCOUNTABILITY IN CRIMINAL JUSTICE TECHNOLOGIES....................18
B. ACCESS TO PROPRIETARY INFORMATION OUTWEIGHS THE NEED TO KEEP PRIVILEGE....................20
C. H.R. 2438 SEEKS TO PROTECT THE CRIMINAL DEFENDANTS 22
V. CONCLUSION....................26

I. INTRODUCTION

Robert Williams, then a forty-two-year-old father of two, was identified as a suspect by facial recognition software and was afterwards arrested "on his front lawn in front of his [family]."[1] In the police interrogation room, Williams claimed that he was not the same person the police thought he was, he stated: "When I look at the picture of the guy, I just see a big Black guy. I don't see a resemblance. I don't think he looks like me at all."[2] In response, the detective said, "So I guess the computer got it wrong, too."[3]

Williams's case is but one of many cases where technology has negatively affected the lives of innocent people.[4] Williams's situation illustrates "someone being wrongfully arrested based on a false hit produced by facial recognition technology"; in fact, when he was arrested, the police failed to ask Williams any questions, rather, the police immediately chose to believe the technology as accurate and true.[5] Thankfully, Williams's case was dismissed, despite Williams being detained for thirty hours based on inaccurate results.[6] But there are many people who were not as fortunate.[7] Some have not only been falsely identified but have been falsely convicted and put in prison or on death row.[8]

While technology has helped individuals in various areas from medicine to business to education, and even in the criminal justice system, it is not perfect.[9] In the criminal justice context, "forensic technology can be faulty . . . and can reflect the biases of the software engineers and scientists who created it."[10] When the life, liberty, and property of an individual are at stake, the criminal justice system should not be satisfied with whatever results the technology yields. The criminal justice system should assess and analyze the technology itself to ensure the accuracy and reliability of its output before letting innocent people pay the price for crimes committed by others. A way to ensure the accuracy of criminal justice technologies is through "examin[ing] its source code for bias and inaccuracy."[11] Unfortunately, companies and third party inventors typically preclude disclosure of this proprietary information and claim trade

[1] Bobby Allyn, *'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man*, NPR (June 24, 2020, 8:00 AM), https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig [https://perma.cc/3XCD-YTZK].

[2] *Id.*

[3] *Id.*

[4]. *See id.*; *see also* Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, WIRED (Mar. 7, 2022, 7:00 AM), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/ [https://perma.cc/J4FE-N6XP].

[5] *See* Allyn, *supra* note 1.

[6] *See id.*

[7] *See, e.g.*, Tribune News Service, *Convicted by Software? Not So Fast, Says Lawmaker*, INDUSTRY INSIDER (July 16, 2020), https://insider.govtech.com/california/news/convicted-by-software-not-so-fast-says-lawmaker.html [https://perma.cc/5ZMA-KCSN].

[8] *See id.*

[9] *See id.*

[10] *See id.*

[11] *See id.*

secret privilege in court.[12] By claiming source code information as a protected trade secret, the criminal justice technologies and programs used "cannot be examined or tested by lawyers for defendants"; in effect, criminal defendants are deprived of their constitutional rights and human liberty.[13] But there may be hope. A potential solution to this problem is for Congress to pass H.R. 2438, or the Justice in Forensic Algorithms Act of 2021, which seeks to regulate criminal justice technologies used against criminal defendants.

The purpose of this Comment is to (1) establish how trade secret privilege came into existence in United States criminal proceedings, (2) illustrate the use of trade secret privilege in American courts, and (3) argue in favor of passing H.R. 2438 to ensure protection of the lives and liberties of criminal defendants. To do this, Part II investigates the history of trade secret law, its evolution in American civil and criminal courts, and the establishment of the trade secret privilege to prevent disclosure of the proprietary information in court proceedings. Part III explores the application of the rules and laws regarding trade secret privilege in trial, and further considers the arguments and perspectives of trade secret privilege from the point of view of the trade secret holder and the criminal defendant. Finally, Part IV argues that Congress should pass H.R. 2438, which warrants disclosure of criminal justice technologies' confidential information in criminal court proceedings because of the technologies' lack of accountability without disclosure and the need to protect the constitutional rights and liberties of criminal defendants as a matter of public policy.

II. TRADE SECRET PRIVILEGE'S JOURNEY INTO THE COURTS

A. WHAT IS A TRADE SECRET?

From Google's search algorithm to the Coca-Cola formula to the fictitious Krabby Patty ingredients, trade secret law has existed for the purpose of protecting the products of inventors and creators from the public and their competitors.[14] Prior to its modern understanding and application in the United States, trade secret law was first recognized in the 1817 English case, *Newbery v. James*,[15] which held that neither an injunction nor specific performance should be awarded for disclosing a trade secret.[16] Twenty years later, trade secret law debuted in the United States in the case of *Vickery v. Welch*,[17] which involved a chocolatier and his "art or secret manner of making chocolate and all information

[12] *See id.*

[13] *See id.*

[14] *See* Michael J. Kasdan, Kevin M. Smith & Benjamin Daniels, *Trade Secrets: What You Need to Know*, NAT'L L. REV. (Dec. 12, 2019), https://www.natlawreview.com/article/trade-secrets-what-you-need-to-know#:~:text=With%20its%20broad%20definition%20of,%2C%20trademark%2C%20or%20copyright%20law [https://perma.cc/RV47-567A].

[15] Newbery v. James (1817) 35 Eng. Rep. 1011; 2 Mer. 446, 446.

[16] *See* Bernard C. Steiner, *Trade Secrets*, 14 YALE L.J. 374, 374 n.3 (1905).

[17] 36 Mass. 523, 523 (1837).

pertaining to his said manner of making chocolate."[18] The *Vickery* court found that the new owner of Welch's business (i.e., Vickery himself) owned the exclusive right to Welch's trade secret, and that Welch breached his sales contract with Vickery by disclosing the trade secret to others.[19] The *Vickery* holding illustrated what most early courts did in trade secret cases: it refused to "find an absolute property interest in secret information."[20] As a result, early courts based holdings on breaches of confidentiality and trust.[21] In 1963, Mathias Correa further found that while "the 'protection' of trade secrets" appears "to define what the term 'trade secret' actually means" and "to imply the existence of some sort of property"—therefore suggesting that it "ought to be defin[ed] as such"—in reality, "however, this is rarely the case."[22] Using contract law to make determinations in trade secret issues gave early courts the ability to "impose liability on individuals or companies . . . because breach of contract and breach of trust were well-recognized wrongs."[23]

From the *Vickery* case and on, trade secret law developed in the United States through the "principles of law and equity first developed by English courts."[24] Early courts faced difficulties in making determinations on trade secret issues (from the existence of a trade secret to the extent of the duty of confidentiality), but the common law came to the rescue.[25] American trade secret law was birthed out of contracts and torts, where common law courts looked at "breach[es] of confidence, breach[es] of confidential relationship, common law misappropriation, unfair competition, unjust enrichment, and torts [of] . . . trespass or unauthorized access to a plaintiff's property."[26] In 2006, the Seventh Circuit held that "[a] trade secret is really just a piece of information . . . that the holder tries to keep secret by executing confidentiality agreements . . . and by hiding the information . . . and other means of concealment, so that the only way the secret can be unmasked is by a breach of contract or a tort."[27]

While contracts and common law torts have helped keep courts afloat in making decisions in trade secret cases, it was only after the Uniform Law Commission (ULC) promulgated the Uniform Trade Secrets Act (UTSA) in 1979, amended in 1985, that some consensus on trade secret law was reached among the adopting states.[28] Further, the issuance of the UTSA was "the first

[18] *Id.* at 525.

[19] *Id.* at 525–27.

[20] Sharon 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).

[21] *Id.*

[22] *Id.* at 520 (quoting Mathias Correa, *Protection of Trade Secrets*, 1963 BUS. LAW. 531 (1963)).

[23] *Id.* at 499.

[24] *Id.* at 498.

[25] *See id.* at 499–501.

[26] BRIAN T. YEH, CONG. RSCH. SERV., R43714, PROTECTION OF TRADE SECRETS: OVERVIEW OF CURRENT LAW AND LEGISLATION 5 (2016) (footnote omitted).

[27] *Id.* at 2 (quoting ConFold Pac. v. Polaris Indus., 433 F.3d 952, 959 (7th Cir. 2006)).

[28] *See* Robert G. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803, 1805 (2014); *Trade secret*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/trade_secret# [https://perma.cc/V5C8-QKN4].

comprehensive effort to codify the law of trade secrets protection, incorporating the major common law principles while filling gaps left by the courts."[29] In fact, the UTSA bears some resemblance to its tort law counterpart.[30] For example, the Restatement of Torts § 757 states, "A trade secret may consist of 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."[31] Even further, UTSA § 1(4) defines a trade secret as information that:

> (i) derives independent economic value . . . from not being generally known . . . 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 [reasonable] efforts . . . to maintain its secrecy.[32]

The common denominator between both provisions is the economic value derived from the privilege of owning a trade secret, which is one of the three major requirements found throughout the states who have adopted the UTSA.[33] In fact, if information satisfies the following three requirements it may qualify as a trade secret that would warrant an exclusive right and protection to the information: "(1) the information must be secret; (2) it must derive economic value as a result of being kept secret; and (3) it must be the subject of reasonable efforts to maintain its secrecy."[34] Further, for the holder of a trade secret to enforce its intellectual property rights, another individual must have misappropriated or stolen the information as a result of "breaching a duty of confidence, violating an independent legal norm, or using some other 'improper means'" of procurement.[35] Moreover, another resemblance between the UTSA and the Restatement of Torts is liability, where misappropriation under the UTSA is based on (1) "acquisition" of the secret "by a person who knows or has reason to know that the secret was acquired by improper means;" (2) "disclosure or use" of the secret "without consent"; and (3) the person "knew or had reason to know that" the information was secret and "knowledge of it had been acquired by accident or mistake."[36]

Despite some apparent similarities between the Restatement and the UTSA, forty-seven states still chose to accept a form or some variation of the UTSA to deal specifically with trade secret issues.[37] States may have decided to adopt the

[29] YEH, *supra* note 26, at 6 (footnote omitted).

[30] *Compare* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. L. INST. 1939), *with* UNIF. TRADE SECRETS ACT § 1(4) (amended 1985) (UNIF. L. COMM'N 1985).

[31] RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. L. INST. 1939).

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

[33] *See* Bone, *supra* note 28.

[34] *See id.* (footnote omitted).

[35] *See id.*

[36] UNIF. TRADE SECRETS ACT § 1(2) (amended 1985) (UNIF. L. COMM'N 1985); *see* Sandeen, *supra* note 21, at 501 ("(1) [D]iscovery by improper means; (2) acquisition of the secret by a third party with notice of the fact of secrecy and the duty of confidentiality; and (3) acquisition of the secret with notice of the fact of secrecy and knowledge that it was disclosed by mistake.").

[37] *See* Bone, *supra* note 28.

UTSA because it improved upon the Restatement of Torts by (1) refining the definition of trade secret; (2) warranting protection to those that meet the requirements; (3) compelling the "claimant to prove both the existence of a trade secret one or more acts of misappropriation;" (4) simplifying the remedies available; (5) "recogniz[ing] the value of protective orders during trade secret litigation;" and (6) replacing "common law causes of action designed to provide remedies for the misuse of business information."[38] Thus, the states' adoption of the UTSA left behind the era of utilizing the Restatement of Torts as "the primary source for" interpreting and understanding "the purpose and meaning of trade secret law in the United States."[39]

B. HISTORY OF TRADE SECRET PRIVILEGE IN COURTS

Trade secret privilege exists in court proceedings to protect secret information from public disclosure; in essence, the privilege detaches a trade secret holder's obligation to produce such information during the discovery phase.[40] More specifically, courts look to whether revealing the trade secret would create "substantial financial harm," and based upon the court's determination, it may "either decline to share the information with the opposing party or allow the opposing party access to the information under a protective or sealed order."[41] For example, the Florida Legislature has promulgated a rule regarding trade secret privilege granting a holder a right "to refuse to disclose, and to prevent other persons from disclosing," so long as the purpose of concealment is not for fraud or injustice. And if a court determines disclosure is warranted, then the court must invoke "protective measures that the interests of the holder of the privilege . . . require."[42]

The drafters of the First Restatement of Torts added provisions for trade secrets in attempts to resolve issues they identified, such as "whether and to what extent a privilege to disclose or use another's trade secret exists."[43] Further, early courts found that trade secret holders have a privilege to refuse disclosure of their information because of the enforceability of the holders' intellectual property right.[44] For example, a court noted:

> [It was] strongly impressed that it would be inequitable to force the witness to make the disclosure called for . . . . If these questions must be answered, every manufacturer will be at the mercy of anyone who desires to extort

[38] Sandeen, *supra* note 21, at 520.

[39] *Id.* at 502.

[40] *See* Mavrick Law Firm, *Trade Secret Litigation: Invoking the Trade Secret Privilege to Resist Production During Discovery*, FLA. BUS. LITIG. L. BLOG (Dec. 11, 2017) [hereinafter *Trade Secret Litigation*], https://www.mavricklaw.com/blog/trade-secret-litigation-invoking-trade-secret-privilege-resist-production-discovery/ [https://perma.cc/2AD4-N4M9].

[41] Jason Tashea, *Trade Secret Privilege is Bad for Criminal Justice*, A.B.A. J. (July 30, 2019, 6:30 AM), https://www.abajournal.com/lawscribbler/article/trade-secret-privilege-is-bad-for-criminal-justice [https://perma.cc/3552-CTTE].

[42] *See Trade Secret Litigation*, *supra* note 40.

[43] *See* Sandeen, *supra* note 21, at 501.

[44] *See, e.g.*, Crocker-Wheeler Co. v. Bullock, 134 F. 241, 246–47 (C.C.S.D. Ohio 1904).

> from him an account of his process, for an attempt to restrain an infringer would result in the disclosure of all that makes the invention valuable.[45]

Therefore, during discovery, courts typically find the existence of a privilege that will not subject a trade secret holder to disclosure of his or her protected information. To make the determination of whether information is a trade secret that warrants protection, the Federal Rules of Evidence and the United States Constitution provide guidance as to the admissibility of a trade secret in court proceedings. Legal scholars have focused on the issue of an information's relevancy to the case at hand, articulating that "[d]isclosure of trade secrets . . . is apt to be required where the matter sought appears relevant to the issues in controversy."[46] According to the Federal Rules of Evidence, evidence is relevant if it "(a) has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action."[47] Further, under the Federal Rules of Evidence Rule 402, relevant evidence is generally admissible unless otherwise provided in "the United States Constitution; a federal statute; these rules; or other rules prescribed by the Supreme Court."[48] In summary, the Federal Rules of Evidence provide a low standard for admissibility of evidence through the "any tendency" standard.[49] Evidence, however, may not be admitted if its "probative value is substantially outweighed by a danger of . . . unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence."[50]

When establishing the protected information's relevancy, or any evidence for that matter, "the examining party has the burden" of showing the information's "relevance to the subject matter of the action, rather than relevancy to the precise issues presented."[51] In making the relevancy determination, courts consider various factors, such as "the importance of the disclosure to the issue in controversy, and whether the examining party and the deponent are competitors."[52] Further, courts "weigh the discovering party's need, under relevancy standards, and the discovered party's trade secret entitlements" when determining disclosure.[53] While Roger Milgrim discusses trade secret relevancy in the context of civil proceedings, courts typically apply the privilege of trade secrets invoked in civil courts to criminal proceedings.[54]

However, in the criminal context, the Federal Rules of Criminal Procedure contain discovery rules regarding protected information.[55] For instance, Rule 16

[45] *The Privilege of a Witness to Refuse to Disclose Trade Secrets*, 3 MICH. L. REV. 565, 568 (1905) (quoting Moxie Nerve-Food Co. v. Beach, 35 Fed. Rep. 465, 466 (C.C.D. Mass. 1888)).

[46] 4 MILGRIM ON TRADE SECRETS § 14.02 (2022).

[47] FED. R. EVID. 401.

[48] FED. R. EVID. 402.

[49] FED. R. EVID. 401.

[50] FED. R. EVID. 403.

[51] *See* MILGRIM, *supra* note 46 (footnote omitted).

[52] *See id.* (footnote omitted).

[53] *Id.* (footnote omitted).

[54] *See* Tashea, *supra* note 41.

[55] *See* FED. R. CRIM. P. 16.

requires disclosure of information to the defendant at the defendant's request, and "the court may, for good cause, deny, restrict, or defer discovery or inspection . . . ."[56] The relevancy of protected information and its admissibility in court, which again is subject to certain limitations as provided by precedent and federal and state rules, appear to stem from the policy rationale behind the existence of trade secret law: to protect proprietary information for economic reasons.[57] Courts should consider whether disclosure of the information, with or without protective orders, would harm the trade secret holder and their exclusive right to the information.

C. DOES THE PRIVILEGE "TEND TO CONCEAL FRAUD OR OTHERWISE WORK INJUSTICE"?

Precedent and policy have revealed that trade secret holders are afforded a privilege and protection for their secret information.[58] But that privilege is not absolute.[59] Trade secret holders are not necessarily able to argue for privilege as a means for not disclosing; in fact, if holders were afforded absolute protection of their information, then that may abuse and ultimately harm defendants.[60] Instead, "the law provides for limited protection . . . if the information sought is shown to be relevant and necessary."[61] In trade secret cases, for example, disclosure is warranted for the following reasons: (1) to "permit the trier of fact to evaluate and decide the factual issues," (2) to "lay the foundation for drafting an equitable decree with such specificity that conduct which would violate the decree is clearly described," and (3) to comply with a statute or for equitable purposes.[62] Further, trade secret holders may invoke their privilege for purposes of "prevent[ing] other persons from disclos[ure] . . . if the allowance of the privilege will not tend to conceal fraud or otherwise work injustice."[63]

Unbeknownst to most opponents of trade secret disclosure, the disclosure of a trade secret during the discovery process "does not conflict with, or terminate, property rights in them" because courts provide certain "protections as are necessary to preserve the property."[64] This is because court proceedings impose a duty upon every individual "to assist in the administration of justice."[65]

[56] *See id.*

[57] *See* MILGRIM, *supra* note 46.

[58] *See id.*

[59] *Id.*

[60] Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1383–84 (2018).

[61] KENNETH S. BROUN, EVIDENTIARY PRIVILEGES IN FEDERAL COURTS: SURVEY RULES 83 (2015); *see* Am. Tobacco Co. v. Evans, 508 So. 2d 1057, 1061 (Miss. 1987); *see also In re* Cont'l Gen. Tire, Inc., 979 S.W.2d 609, 612 (Tex. 1998).

[62] *See* MILGRIM, *supra* note 46.

[63] BROUN, *supra* note 61.

[64] *See* MILGRIM, *supra* note 46.

[65] *Id.*

Therefore, protective orders may be granted to protect the interests of the trade secret holder while still giving defendants an opportunity to make their case.[66]

In civil proceedings, courts may, for good cause, "order discovery of any matter relevant to the subject matter," such as trade secrets or any other confidential information.[67] Again, even if discovery is warranted, courts may provide protective orders, which stem from the need to protect the economic value and exclusive rights of trade secret holders.[68] Similarly, in the criminal context, courts may warrant disclosure and order protections for the benefit of the trade secret holder.[69] However, with a trade secret holder's failure to disclose its information, a court may order for the discovery or "enter any other order that is just under the circumstances."[70]

In the constitutional context, the Confrontation Clause of the Sixth Amendment provides that "the accused shall enjoy the right . . . to be confronted with the witnesses against him[,]" among other things.[71] The Confrontation Clause applies to criminal cases and grants a defendant the right to cross-examine their accusers, where out-of-court statements are admissible for purposes of litigation if the primary purpose of the statement was made towards an ongoing emergency.[72] As such, for trade secret information used to support a criminal defendant's liability, the information posits itself to be an out-of-court statement that should require courts to allow defendants to cross-examine the statements made against them.

III. IS IT WORTH PROTECTING TRADE SECRETS AT THE EXPENSE OF CRIMINAL DEFENDANTS?

A. HOW COURTS HAVE BEEN APPLYING TRADE SECRET PRIVILEGE RULES

Courts, through policy reasonings, rules, and precedents, have protected trade secret holders from the loss of their secret information.[73] Courts have done so through invoking rules that tend to place trade secrets and the rights and privileges associated with the information above a full disclosure to criminal defendants for purposes of court proceedings.[74] In fact, the Advisory Committee's Note for the Federal Rules of Evidence observed, "The need for accommodation between protecting trade secrets, on the one hand, and eliciting

[66] *See* Christian Chessman, Note, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CALIF. L. REV. 179, 213 (2017).

[67] *See* FED. R. CIV. P. 26(b)(1) advisory committee's note to 2000 amendment.

[68] *See generally* FED. R. CIV. P. 26(c).

[69] *See* FED. R. CRIM. P. 16(b), (d).

[70] FED. R. CRIM. P. 16(d)(2)(D).

[71] U.S. CONST. amend. VI.

[72] *See id.*; *see, e.g.*, Davis v. Washington, 547 U.S. 813, 821 (2006); Crawford v. Washington, 541 U.S. 36, 42 (2004); Olden v. Kentucky, 488 U.S. 227, 231 (1988).

[73] *See* Wexler, *supra* note 60, at 1377.

[74] *Id.*

facts required for full and fair presentation of a case, on the other hand, is apparent."[75]

In Texas, evidentiary rules have sought to address the issue of trade secret privilege in court proceedings.[76] Under Texas Rules of Evidence 507:

> (a) A person has a privilege to refuse to disclose and to prevent other persons from disclosing a trade secret owned by the person, unless the court finds that nondisclosure will tend to conceal fraud or otherwise work injustice. (b) The privilege may be claimed by the person who owns the trade secret or the person's agent or employee. (c) If a court orders a person to disclose a trade secret, it must take any protective measures required by the interests of the privilege holder and the parties and to further justice.[77]

Accordingly, Rule 507—like the UTSA and policy reasonings surrounding intellectual property rights and rights of criminal defendants—is a "claim of privilege" that "warrant[s] such protection under the TUTSA[,]" the Texas Uniform Trade Secrets Act."[78]

For example, the Texas criminal court in *Kelly v. State* considered the admissibility of scientific data by looking at its reliability.[79] Specifically, the court found scientific data reliable, so long as "(a) the underlying scientific theory [is] . . . valid; (b) the technique applying the theory [is] . . . valid; and (c) the technique [is] . . . properly applied on the occasion in question."[80] The relevant reliability factors included:

> (1) the extent to which the underlying scientific theory and technique are accepted as valid by the relevant scientific community, if such a community can be ascertained; (2) the qualifications of the expert(s) testifying; (3) the existence of literature supporting or rejecting the underlying scientific theory and technique; (4) the potential rate of error of the technique; (5) the availability of other experts to test and evaluate the technique; (6) the clarity with which the underlying scientific theory and technique can be explained to the court; and (7) the experience and skill of the person(s) who applied the technique on the occasion in question.[81]

Five years later, the court in *Hartman v. State* emphasized that "under the Rules, the trial judge must ensure that *any and all scientific testimony* or evidence admitted is not only relevant, but *reliable*."[82]

[75] BROUN, *supra* note 61, at 83.

[76] *See* Blaze Taylor, *Claiming Privilege for Proprietary Information: Properly Applying Tex. R. Evid. 507*, TEX. BAR BLOG (Oct. 25, 2018), https://blog.texasbar.com/2018/10/articles/guest-blog/claiming-privilege-for-proprietary-information-properly-applying-tex-r-evid-507/ [https://perma.cc/76TB-K58Y].

[77] TEX. R. EVID. 507.

[78] *See* Taylor, *supra* note 76.

[79] 824 S.W.2d 568, 573 (Tex. Crim. App. 1992).

[80] *Id.*

[81] *Id.*

[82] 946 S.W.2d 60, 62 (Tex. Crim. App. 1997) (emphasis added) (quoting Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 589 (1993)).

In *State v. Pickett*, the New Jersey court "allow[ed] a defendant in a criminal case to obtain the source code for artificial intelligence-powered software used to identify him."[83] The court appeared to recognize the "clash between secrecy and transparency" as evident in situations where an "increasing reliance on technology in legal decision[-]making" exists.[84] As such, by making its decision, the court gave way for "more legal and public scrutiny" on criminal justice technologies; thus, this decision sought to hold third party inventors and the users of these technologies to a higher standard of accountability.[85] Additionally, the *Pickett* decision hopefully overturned convictions that may have been "based on faulty evidence, affected by bias, or manipulated by outside influences."[86]

Christian Chessman, a former Juris Doctor candidate at the University of California, Berkeley, School of Law, recognized the importance of a criminal defendant's access to the source code of criminal justice technologies to grant full fairness in trial.[87] In his article, Chessman analyzed the *Chubbs* case and found that it was only through "judicial examination . . . [that] the justice system [may] search for accidental coding mistakes, willful biases . . . or simply an angry employee gone rogue."[88] Chessman also looked at *In re Source Code Evidentiary Hearings in Implied Consent Matters*[89] and found that the criminal defendants in the case "were able to identify errors in the Intoxilyzer's functioning only after" a thorough review and examination of "the device's source code."[90] Therefore, while trade secret privileges present a controversy within criminal cases, courts and legal scholars are not blind to the present issues and, in fact, recognize the balancing of the intellectual property rights and privileges of trade secret holders and the relevance and reliability of source code information in criminal court proceedings.

B. TRADE SECRET HOLDERS: "OUR PRIVILEGE SHOULD STAY"

From its origins in England through the *Newbery* case,[91] courts and legislators have recognized an existing exclusive right in trade secret information, warranting protection from individuals seeking to misappropriate the information for their own economic benefit.[92] Not only have state governments sought to protect trade secrets, but the federal government itself has issued the UTSA to create uniform legislation to grant rights and protections to holders of

[83] 246 A.3d 279, 301 (N.J. Super. Ct. App. Div. 2021); *see also* David Uberti, *Court Ruling Reflects Latest Pressure on AI Trade Secrets*, WALL ST. J. (Feb. 4, 2021, 7:39 PM), https://www.wsj.com/articles/court-ruling-reflects-latest-pressure-on-ai-trade-secrets-11612485559 [https://perma.cc/B924-YUG9].

[84] *See Pickett*, 246 A.3d at 284; *see also* Meghan J. Ryan, *Secret Algorithms, IP Rights, and the Public Interest*, 21 NEV. L.J. 61, 65 (2020).

[85] *See* Uberti, *supra* note 83.

[86] *See* Ryan, *supra* note 84, at 61.

[87] *See* Chessman, *supra* note 66, at 183.

[88] *Id.* at 199 (footnote omitted).

[89] 816 N.W.2d 525, 525 (Minn. 2012).

[90] Chessman, *supra* note 66, at 197.

[91] *See* Newbery v. James (1817) 35 Eng. Rep. 1011; 2 Mer. 446.

[92] *See* Steiner, *supra* note 16.

trade secrets.[93] Court decisions and legislative resolves stem from a basis of economic value inherent in trade secret information, where "public disclosure could do 'irreparable harm.'"[94] If trade secrets are easily disposable, especially in court proceedings, then the incentive to create and build disappears.[95] In the criminal justice context, "curtailing trade-secrets privileges could dissuade companies from investing in new technologies" because the protections that trade secret holders hope to gain from courts is all for the purpose of precluding, to some degree, great "business risks in the form of intellectual-property theft."[96] In fact, trade secret holders themselves understand that it is "important to protect intellectual property," where violations may "lead to lost or stolen revenue."[97]

Survey Rule 507 in federal courts states the following:

> A person has a privilege, which may be claimed by the person or the person's agent or employee, to refuse to disclose and to prevent other persons from disclosing a trade secret owned by the person, if the allowance of the privilege will not tend to conceal fraud or otherwise work injustice. If disclosure is directed, the court shall take such protective measures as the interest of the holder of the privilege and of the parties and the interests of justice require.[98]

Accordingly, trade secret holders may find that their rights should be honored in criminal proceedings because disclosure may negatively impact their business, and thus have an injustice brought upon them.[99] In fact, Meghan Ryan recognized that "some advantages of relying on" the criminal justice technologies and innovations brought about by third parties "is that they offer the potential to provide greater fairness to defendants across cases and remove judicial and other conscious and unconscious biases from criminal justice decision[-]making."[100] Therefore, policy surrounding trade secrets does not want to preclude companies and inventors from having their technologies used in the criminal justice system for fear that their work will be exposed, thereby destroying their trade secrets.

Courts and legislators have sought to protect trade secret rights, but if disclosure is nonetheless warranted in a criminal proceeding, then where does that leave trade secret holders? If courts choose to honor the constitutional rights of criminal defendants for a full and fair trial, who then protects the information of trade secret holders produced in a criminal case? In reality, "it would be an abuse of discretion for the court not to protect that information during trial."[101]

[93] *See* UNIF. TRADE SECRETS ACT § 1(4).
[94] Uberti, *supra* note 83.
[95] *See id.*
[96] *See id.*
[97] Tashea, *supra* note 41.
[98] BROUN, *supra* note 61.
[99] *See id.*
[100] Ryan, *supra* note 84, at 87–88.
[101] *See* MILGRIM, *supra* note 46.

As such, the judiciary of Texas has sought "to preserve trade secrecy without barring discovery of such information" and require discovery "to include only matters relevant to the case."[102] These Texas courts, and presumably other state courts, do so by issuing protective orders, confining access of confidential information to certain parties, utilizing in-camera hearings, sealing certain records, and ordering parties to the matter not to "disclose an alleged trade secret without prior court approval."[103] Therefore, state criminal courts should only warrant disclosure for "the determination of the controversy," where "its nondisclosure to the discovering party would cause a great hardship"; otherwise, "disclosure should not be required."[104]

C. CRIMINAL DEFENDANTS: "OUR CONSTITUTIONAL RIGHTS ARE VIOLATED"

While trade secret law's history and related policies behind general intellectual property rights require a protection of proprietary information, there still exists the constitutional and human rights of criminal defendants to receive a full and fair trial. When considering the purpose of a trial—which is to discover the truth and act according to the findings of the factfinder—it is evident that allowing disclosure of information is aligned with the "spirit and purpose of discovery[,] [which] is to uncover the truth and allow a case to justly be decided upon all the facts, and not by hiding the facts."[105] Otherwise, a lack of disclosure may prove to be "potentially fatal to a litigator's case."[106]

In fact, the exclusive rights and protections conferred by trade secret law generally occur in the context of civil cases, particularly in relation to economic issues, and preclude misappropriation of the secret information; therefore, the privileges of trade secrets were not intended to "stymie due process or block judicial truth-seeking."[107] When information was disclosed in civil trade secret misappropriation cases, such disclosure often included protective orders; the purpose being to avoid theft of proprietary information that could negatively impact the trade secret holder's business.[108] On the other hand, criminal justice technologies, specifically their source codes and algorithms, do not provide any "meaningful risk of trade secrets being disclosed to a business competitor" because the intended purpose is to execute justice in criminal cases.[109]

When considering the rights of criminal defendants at trial, the Fourteenth Amendment's Due Process Clause states that no state shall "deprive any person

[102] *See* Taylor, *supra* note 76.

[103] *Id.*

[104] *See* MILGRIM, *supra* note 46.

[105] *See* Taylor, *supra* note 76.

[106] *Id.*

[107] 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/CP76-G338].

[108] *See id.*

[109] *See id.*

of life, liberty, or property, without due process of law."[110] One must ask then: Is depriving a criminal defendant access to trade secrets, particularly the source code of criminal justice technologies used to convict defendants, a deprivation of the criminal defendant's entitlement to due process of law? Some would answer in the affirmative. Because, as observed by David Uberti in the *Pickett* case—where the *Pickett* court compelled the lower court in New Jersey "to hand over the source code under a protective order"—this was proper because "[f]undamental due process and fairness demand access."[111]

Accordingly, the *Pickett* case illustrated the court granting the defendant a procedural and substantive right to access proprietary information to ensure a complete and fair trial that ultimately determined the fate of the defendant (i.e., whether the defendant received time for imprisonment, paid a fine, ended up on death row, or received acquittal for the charges made against them).[112] By granting disclosure, criminal defendants are given the "right to present a complete defense[,]" which necessarily "encompasses the defendant's ability to meaningfully test the prosecution's evidence and to present favorable evidence in turn."[113] With that, courts honor a defendant's fundamental right to present a defense because the right becomes properly "subject to strict scrutiny."[114] The standard of strict scrutiny better protects the rights of criminal defendants against the typical reasons courts preclude disclosure: "(1) the source code is irrelevant; (2) the source code is a trade secret; and (3) the state does not possess the source code."[115] These reasons do not "withstand scrutiny, nor do they present the substantial 'legitimate interests' to which [the] fundamental right should 'bow to accommodate.'"[116]Additionally, trade secret information involving "purely private pecuniary interests," is not a "legitimate state interest" for purposes of determining disclosure in criminal proceedings.[117]

In *Holmes v. South Carolina*, the United States Supreme Court found that the fundamental right to present a defense was violated when admissibility of evidence was based upon "a factual assumption that favorably credits the prosecution's evidence."[118] However, the strength of a piece of evidence is dependent upon its *credibility*; therefore, "admission of evidence by a defendant should not rest upon reasoning that *presumes* the *accuracy* or *correctness* of the prosecution's evidence."[119] Moreover, the Sixth Amendment states the following:

[110] U.S. CONST. amend. XIV, § 1.

[111] Uberti, *supra* note 83 (citing State v. Pickett, 246 A.3d 279, 279, 323–24 (N.J. Super. Ct. App. Div. 2021).

[112] *See id.*

[113] *See* Chessman, *supra* note 66, at 200 (footnote omitted).

[114] *Id.* (footnote omitted).

[115] *Id.* at 205 (footnotes omitted).

[116] *Id.*

[117] *Id.* at 209.

[118] *Id.* at 203 (citing Holmes v. South Carolina, 547 U.S. 319, 330 (2006)).

[119] *Id.* (emphasis added) (footnote omitted).

> In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the assistance of counsel for his defense.[120]

Accordingly, because the advancement and development of technology contributes to making conviction determinations in criminal proceedings—in other words, "[a]s technology becomes more central to evidence gathering and defendant profiling"—it therefore warrants a more "open and transparent" procedure during trials.[121] Without access to trade secret information, defendants end up with convictions based on proceedings that failed to grant complete access to evidence; as a result, these types of situations create an unfair and closed justice system.[122]

Moreover, the Sixth Amendment also contains the Confrontation Clause, which grants criminal defendants the right to "be confronted with the witnesses against him . . . ."[123] Therefore, evidence that is testimonial in nature, or statements made for purposes of litigation, must be examined subject to the Confrontation Clause.[124] In *Crawford v. Washington*, the Supreme Court "impose[d] an absolute bar to statements that are testimonial, absent a prior opportunity to cross-examine."[125] On the other hand, non-testimonial statements, or statements usually made during an ongoing emergency, fall within a hearsay exception that ultimately grants admission of the evidence into trial.[126] In the context of criminal justice technologies that "provid[e] incriminating evidence against" defendants, without access to algorithms or source code information, "these defendants lack the opportunity to challenge this incriminating evidence that poses real questions of accuracy . . . [and] bias."[127] In *Melendez-Diaz v. Massachusetts*,[128] the Supreme Court found that the outcomes yielded by "the exercise of judgment or the use of skills that the analysts may not have possessed" required cross-examination of those analysts to ensure that the defendant was afforded their constitutional rights in court.[129] Further, while intellectual property rights of trade secret holders are indeed of great importance, "shrouding the source code and related documents in a curtain of secrecy *substantially hinders* [a] defendant's opportunity to meaningfully challenge reliability."[130]

[120] U.S. CONST. amend. VI.

[121] *See* Tashea, *supra* note 41.

[122] *See id.*

[123] U.S. CONST. amend. VI.

[124] *See* Davis v. Washington, 547 U.S. 813, 821–22 (2006).

[125] 541 U.S. 36, 61 (2004).

[126] *See Davis*, 547 U.S. at 821–22.

[127] Ryan, *supra* note 84, at 65.

[128] 557 U.S. 305, 307 (2009).

[129] *Id.* at 320; *see* Chessman, *supra* note 66, at 219–20.

[130] Wexler, *supra* note 107 (emphasis added).

In addition to precluding defendants from a full and fair trial, lack of disclosure of the criminal justice technologies' proprietary information also deters further innovation of the technologies.[131] Where the policy behind intellectual property rights is "[t]o promote the progress of science and useful arts," is preventing disclosure of trade secrets in criminal trials inhibiting the advancement of the tools and innovations used in the criminal justice system?[132] By limiting disclosure, "other inventors" are unable to "build on the already-existing technologies" which "slows innovation."[133]

In fact, allowing "broad secrecy" does not absolutely "spur or quell competition"; instead, the "broad secrecy" yields various issues, such as inaccuracy.[134] Inaccuracies could lead to "defendants being convicted and deprived of their liberty" because of improper inputs and outputs.[135] Without the ability to test or examine the proprietary information, there is no way to determine whether the technology yields accurate results that will ultimately affect the outcome of a criminal defendant's case.[136] In fact, "there is no absolute privilege for trade secrets and similar confidential information" that would allow trade secret holders to exercise unconditional protection.[137]

In 2012, a chemist falsified evidence used in criminal cases, where the chemist's "misconduct may have jeopardized evidence in about 34,000 drug cases."[138] The chemist "improperly removed evidence, forged [colleagues'] signatures, and didn't properly test drugs."[139] Cases potentially impacted by the chemist's wrongful acts may have avoided injustices if criminal defendants were able to cross-examine and confront the information used against them.[140] While it is clear that intellectual property rights protect the economic value of an individual's trade secrets, it is unfair to criminal defendants in court proceedings given "the proprietary—and thus secret—nature of these computerized algorithms."[141] Notably, when "the government uses incorrect evidence to try, convict, and incarcerate a criminal defendant," the defendant loses a part of their liberty that they can never get back.[142] This is because "evidence produced by computers 'is not uniquely immune from the risk of manipulation;'" rather, "it may involve 'the use of skills' that the programmers lacked[,]" and may involve the "risks from both 'fraudulent' and 'incompetent' programmers"; therefore, to avoid improper results affecting the liberty of defendants, trade secret

[131] *See* Ryan, *supra* note 84, at 63–64.

[132] *See* U.S. CONST. art. I, § 8, cl. 8.

[133] Ryan, *supra* note 84, at 64.

[134] *Id.* at 87.

[135] *See id.*

[136] *See id.*

[137] BROUN, *supra* note 61, at 83.

[138] Brian Ballou & Andrea Estes, *Chemist in Lab Scandal Told Investigators: 'I Messed Up Bad'*, BOSTON.COM (Sept. 26, 2012), https://www.boston.com/uncategorized/noprimarytagmatch/2012/09/26/chemist-in-lab-scandal-told-investigators-i-messed-up-bad/ [https://perma.cc/P6MA-379E].

[139] *Id.*

[140] *See id.*

[141] Ryan, *supra* note 84, at 64.

[142] Wexler, *supra* note 107.

information surrounding criminal justice technologies must be made accessible to the defense.[143]

IV. H.R. 2438 TO THE RESCUE?

In early 2021, California Representative Mark Takano introduced H.R. 2438 into Congress.[144] The purpose of the bill is to regulate criminal justice technologies used against criminal defendants.[145] More specifically, the bill focuses on the following elements:

> [R]equirements for the establishment of testing standards and a testing program for computational forensic software, requirements for the use of computational forensic software by federal law enforcement agencies and related entities *(e.g., crime labs), a ban on the use of trade secret evidentiary privilege to prevent federal criminal defendants from accessing evidence collected using computational forensic software or information about the software (e.g., source code)*, and limits on the admissibility of evidence using computational forensic software.[146]

Accordingly, this Comment argues in favor of passing H.R. 2438 for the reasons stated in the following subsections.

A. THE LACK OF ACCOUNTABILITY IN CRIMINAL JUSTICE TECHNOLOGIES

In a world full of vast technological advancements, technology plays a role in almost every area of life, from travel to education to healthcare and more. In the criminal justice context, "[e]vidence created by computer programs dominates modern criminal trials," but the source code of the criminal justice technologies is insulated from disclosure and access by defense counsel.[147] In effect, defendants "subjected to these . . . technologies" require access to the source code not only for purposes of meeting the defendants' constitutional rights, but also because transparency yields accountability.[148] Because use of technology is not going to be absolved from the criminal justice system, criminal defendants rely on the government to ensure that the use of these technologies "allow[s] for public accountability and transparency."[149]

[143] Chessman, *supra* note 66, at 220 (footnote omitted); *see* Wexler, *supra* note 107.

[144] *See* Justice in Forensic Algorithms Act of 2021, H.R. 2438, 117th Cong. (2021), CONGRESS.GOV, https://www.congress.gov/bill/117th-congress/house-bill/2438?s=1&r=1 [https://perma.cc/8ZUP-Q6KM].

[145] *See id.*

[146] *Id.* (emphasis added).

[147] Chessman, *supra* note 66, at 179.

[148] Karen Michele Nikos-Rose, *Facial Recognition, Cameras, Other Tools Police Use Raise Questions About Accountability: Public Scrutiny Necessary for the Police and the Companies That Make the Equipment*, UC DAVIS (Oct. 14, 2021), https://www.ucdavis.edu/curiosity/news/facial-recognition-cameras-other-tools-used-police-raise-questions-about-accountability [https://perma.cc/QG6P-EDZX].

[149] *Id.*

The more prevalent and commonplace technology has become in a person's everyday life, the more evident it is that technology is imperfect.[150] Some of the issues faced in the use of criminal justice technologies include "poor quality input data, human user error, and bias across demographic groups, including by race and gender."[151] Even the inventors of these technologies understand that "bugs and misconfigurations are inherent in software" and that "accidental errors can manifest in both technical and substantive ways."[152] As for technology that may have been "perfectly written," it may still be subject to errors as a result of "'software rot,' where the quality, functionality, and usefulness of a program actually degrade over time."[153] Improper results are unfavorable as evidenced by cases where laboratory technicians have falsified evidentiary results; in fact, there was a situation where "the federal government imposed ineffective DNA mixture software on forensic science . . . that forced forensic failure" in an abundant amount of cases and resulted in "widespread injustice."[154] Therefore, the only way to avoid, or at least minimize, erroneous results that are used against criminal defendants is to allow access to source code in order to ensure that defendants are not improperly convicted.[155] As the Electronic Frontier Foundation stated: "If you want to make sure the right person is imprisoned—and not running free while someone innocent is convicted—we can't have software programs' source code hidden away from stringent examination."[156]

A study published by the Harvard Data Science Review focused on achieving transparency over fairness.[157] In the study, researchers used a recidivism risk-scoring model (i.e., the COMPAS model) to illustrate that the tendency of reoffence was not dependent upon "the defendant's age"; rather, the study found that there were "defendants with low risk scores but long criminal histories, suggesting that data inconsistencies occur frequently in criminal justice databases."[158] The researchers recognized that the "lack of transparency in COMPAS . . . could lead to dangerous situations for the public."[159] The hope was that courts desire to minimize "inconsistent error-prone decisions" as a result of the lack of transparency in criminal justice technologies affecting the

[150] *Id.*

[151] Wexler, *supra* note 107.

[152] Chessman, *supra* note 66, at 186 (footnote omitted); *see* Kit Walsh, *EFF Asks Court: Can Prosecutors Hide Behind Trade Secret Privilege to Convict You?*, ELEC. FRONTIER FOUND. (Sept. 14, 2017), https://www.eff.org/press/releases/eff-asks-court-can-prosecutors-hide-behind-trade-secret-privilege-convict-you [https://perma.cc/N76N-ZQEP].

[153] Chessman, *supra* note 66, at 190.

[154] *The Government Wants to Take Away Your Right to Use Independent Forensic Software*, CYBERGENETICS (June 23, 2020), https://www.cybgen.com/information/newsroom/2020/jun/Government-wants-to-take-away-your-right-to-use-independent-forensic-software.shtml [https://perma.cc/E4SX-M7L8]; *see* Walsh, *supra* note 152.

[155] *See* Walsh, *supra* note 152.

[156] *Id.*

[157] *See* Cynthia Rudin, Caroline Wang & Beau Coker, *The Age of Secrecy and Unfairness in Recidivism Prediction*, HARV. DATA SCI. REV., Mar. 2020, at 3.

[158] *Id.* at 2.

[159] *Id.* at 31.

lives of defendants subject to these technologies.[160] To conclude its discussion, the study observed the following: (1) "[l]ack of transparency" which thereby "makes it difficult to assess any of the myriad forms of fairness"; (2) injustice imposed upon defendants in the form of procedural harms; (3) potential for unfair economic burden upon the judicial system and taxpayers; and (4) potential that specific individuals may be further wronged by divulging private information.[161] Thus, this Harvard study illustrated the fallacies of criminal justice technologies that warrant its transparency for purposes of protecting the rights and liberties of criminal defendants bound by the results of the technologies.

B. ACCESS TO PROPRIETARY INFORMATION OUTWEIGHS THE NEED TO KEEP PRIVILEGE

The purpose of H.R. 2438 is to "prohibit the use of trade secrets privileges to prevent defense access to evidence in criminal proceedings, provide for the establishment of Computational Forensic Algorithm Testing Standards and a Computational Forensic Algorithm Testing Program, and for other purposes."[162] The bill considers the importance of transparency and accountability "in ensuring the fair administration of justice."[163] Doing so not only creates possibilities of improvement in criminal justice technologies, but also ensures that "defendants [are not left] in the dark."[164]

Prior to H.R. 2438, however, Representative Takano introduced H.R. 4368 (i.e., the Justice in Forensic Algorithms Act of 2019).[165] The 2019 Act was introduced into Congress to grant criminal defendants "access to source code and other information necessary to exercise their confrontational and due process rights."[166] The five main provisions of the 2019 Act included the following:

> 1. The bill would annul trade secrets, eliminating innovation in forensic software.
>
> 2. It would shift responsibility for forensic evidence admissibility away from impartial judges, transferring historic judicial powers to a federal executive agency.

[160] See *id.*

[161] *See id.*

[162] Justice in Forensic Algorithms Act of 2021, H.R. 2438, 117th Cong. (2021).

[163] *See* Walsh, *supra* note 152.

[164] Tashea, *supra* note 41.

[165] *See* Justice in Forensic Algorithms Act of 2019, H.R. 4368, 116th Cong. (2019).

[166] Dayanara Ramirez, *Rep. Takano Introduces the Justice in Forensic Algorithms Act to Protect Defendants' Due Process Rights in the Criminal Justice System*, TAKANO (Sept. 17, 2019), https://takano.house.gov/newsroom/press-releases/rep-takano-introduces-the-justice-in-forensic-algorithms-act-to-protect-defendants-due-process-rights-in-the-criminal-justice-system [https://perma.cc/EHE3-WBE3].

3. The diverse scientific community that tests forensic software would be replaced by a monolithic government unit.

4. Federal testing standards for forensic software that were instituted five years ago would be rebranded as if they were something new.

5. Legal defense teams could disclose company-crippling trade secrets, without incurring any consequences.[167]

Similar to Representative Takano's reasoning for introducing H.R. 2438, the 2019 Act sought to honor a criminal defendant's constitutional rights in court proceedings, specifically a defendant's due process and confrontation rights.[168] Representative Takano stated that his "legislation will open the black box of forensic algorithms and establish standards that will safeguard our [c]onstitutional right to a fair trial."[169] Further, Representative Takano believed that the intellectual property rights underlying trade secrets "should not . . . trump" an individual's due process rights.[170] Without access to source code information, judges and juries will blindly accept the results produced by the criminal justice technologies; however, to avoid constitutional rights issues, it is pertinent that "juries and judges . . . understand the limits of technology and how it works."[171]

Although third-party companies and inventors likely know and understand the workings of their criminal justice technologies, precluding defense counsel from examining the source code or other trade secret information belies fairness and accountability in ensuring its accuracy.[172] As such, there is the potential that defendants "are being convicted based on the results of these potentially flawed forensic algorithms without the ability to challenge this evidence due to the intellectual property interests of the software's developers."[173] When inventors are the only ones who "know how these algorithms work" it "presents a threat to due process rights and violates the confrontation rights guaranteed" to defendants.[174] Therefore, the role of the National Institute of Standards and Technology (NIST), which the 2019 Act sought to create, would be to set the minimum standards of computational forensic software by analyzing the criminal justice technologies and determining "what the limitations are, what the possibilities are, and . . . what the science out there says about [the] data and how these algorithms work."[175] These standards, when enforced, would presumably

[167] *See* CYBERGENETICS, *supra* note 154.

[168] *See* Ramirez, *supra* note 166.

[169] *See id.*

[170] Catherine Matacic, *This U.S. Lawmaker Wants Greater Scrutiny of Algorithms Used in Criminal Trials*, SCIENCE (Sept. 23, 2019), https://www.science.org/content/article/us-lawmaker-wants-greater-scrutiny-algorithms-used-criminal-trials [https://perma.cc/7J6P-NQ9H].

[171] *Id.*

[172] *See* Ramirez, *supra* note 166.

[173] *Id.*

[174] *Id.*; *see also* Matacic, *supra* note 170.

[175] *See* Matacic, *supra* note 170; *see also* Justice in Forensic Algorithms Act of 2019, H.R. 4368, 116th Cong. (2019).

hold third-party inventors accountable and likely minimize erroneous convictions.

Unfortunately, the 2019 Act died, which may have been due to members of Congress failing "to pick it up and understand the underlying issue."[176] Additionally, the 2019 Act was introduced at a time when the "judiciary committee ha[d] a lot on its plate" (i.e., the impeachment investigations against former President Donald Trump).[177] These "bigger attention-getting topics" may have stolen the focus and attention of members from the real issues that the 2019 Act sought to resolve.[178] Thankfully, Representative Takano reintroduced the bill, H.R. 2438, in early 2021.[179] This gives politicians a second opportunity to care about this bill and vote to pass it. By supporting Representative Takano's initiative in passing H.R. 2438, politicians are making the effort to positively impact and bring more fairness to the criminal justice system. More specifically, the bill's passage would not only help innocent criminal defendants but also hold trade secret holders of criminal justice technologies accountable.

C. H.R. 2438 SEEKS TO PROTECT THE CRIMINAL DEFENDANTS

Through the reintroduction of the Justice in Forensic Algorithms Act, Representative Takano hopes to grant "defendants . . . access to source code and other information necessary to exercise their confrontational and due process rights when" criminal justice technologies are used against them.[180] Similar to the 2019 Act, H.R. 2438 seeks to create transparency and understanding behind the criminal justice technologies through the help of the NIST to create "Computational Forensic Algorithms Standards and a Computational Forensic Algorithms Testing program that federal law enforcement must comply with"; this would grant criminal defendants access to proprietary information for purposes of examining and "evaluating the evidence used against them during . . . criminal proceeding[s]."[181] As a result, third parties would be unable to use the trade secret evidentiary privilege to absolutely "withhold relevant evidence from defense attorneys in criminal cases."[182]

Third-party inventors, however, need not worry because "courts have [already] developed numerous mechanisms to protect the interests of trade secret holder[s]"; these measures "include in-camera review, carefully crafted protective orders, trade secret analysis . . . and more."[183] Therefore, rather than precluding the source code information, thus "deny[ing] defendants access,"

[176] Matacic, *supra* note 170.

[177] *Id.*

[178] *See id.*

[179] *See* Justice in Forensic Algorithms Act of 2021, H.R. 2438, 117th Cong. (2021).

[180] Dayanara Ramirez, *Reps. Takano and Evans Reintroduce the Justice in Forensic Algorithms Act to Protect Defendants' Due Process Rights in the Criminal Justice System*, TAKANO (Apr. 8, 2021) [hereinafter TAKANO], https://takano.house.gov/newsroom/press-releases/reps-takano-and-evans-reintroduce-the-justice-in-forensic-algorithms-act-to-protect-defendants-due-process-rights-in-the-criminal-justice-system [https://perma.cc/R4GW-PHU5].

[181] *Id.*

[182] Wexler, *supra* note 107.

[183] Chessman, *supra* note 66, at 213.

courts "should permit access to source code under the protective auspices of judicial oversight."[184] For example, the Supreme Court in *Daubert v. Merrell Dow Pharmacy*[185] found "four flexible criteria" to establish the reliability of expert testimony: "falsifiability, error rate, peer review, and general acceptance within the pertinent field of expertise."[186] Chessman believes that these four criteria are applicable to source code in determining the reliability of criminal justice technologies.[187] Additionally, the United States Court of Appeals for the District of Columbia Circuit in *Frye v. United States*[188] focused on a "general acceptance" of the scientific method "within the pertinent scientific community" and considered "(1) whether the conceptual process embodied in the program is accepted in its pertinent field, and (2) whether the underlying programmed implementation is accepted by experts in the field of computer science."[189] Accordingly, as exampled above, courts have already developed some protective measures for scientific and technical evidence used in criminal proceedings and may draw from its precedents to protect proprietary information while still allowing its admission in court.[190] Therefore, through H.R. 2438, "developers would still be able to get appropriate protective orders from the courts to safeguard their intellectual property interests"; however, the trade secret holders could not depend upon intellectual property rights "arguments to entirely suppress relevant evidence from cross-examination by the defense."[191]

When "courts deny access . . . outright instead of relying on existing protective mechanisms[,]" such courts are "arbitrarily and indefensibly preventing defendants from" a full and fair trial.[192] This is because precluding defendants from accessing algorithm information "threatens [their] lives and liberty in the criminal justice" system, especially if the criminal justice technologies are error-prone.[193] In fact, if H.R. 2438 were passed, the bill would preclude the finding of "trade secret evidentiary privilege to withhold relevant evidence in criminal proceedings."[194] The Federal Rules of Criminal Procedure, the Federal Rules of Evidence, and other applicable rules would still apply to cases dealing with trade secret evidence.[195] Further, H.R. 2438 states:

> In any criminal case, evidence that is the result of analysis by computational forensic software is admissible only if—

[184] *Id.*

[185] 509 U.S. 579, 589 (1993).

[186] *See id.* at 593–94; Chessman, *supra* note 66, at 216.

[187] Chessman, *supra* note 66, at 216.

[188] 293 F. 1013, 1014 (D.C. Cir. 1923).

[189] Chessman, *supra* note 66, at 218; *see Frye*, 293 F. at 1014.

[190] *See* Taylor, *supra* note 76.

[191] *See* Wexler, *supra* note 107.

[192] Chessman, *supra* note 66, at 213.

[193] Ryan, *supra* note 84, at 106; *see* Rudin, Wang & Coker, *supra* note 157, at 5; *see also* TAKANO, *supra* note 180.

[194] Justice in Forensic Algorithms Act of 2021, H.R. 2438, 117th Cong. § 2(b)(1) (2021).

[195] *Id.* § 2(b)(2).

> (1) the computational forensic software has been submitted to the Computational Forensic Algorithm Testing Program of the Director of the National Institute of Standards and Technology and there have been no material changes to that software since it was last tested; and
>
> (2) the developers and users of the computational forensic software agree to waive any and all legal claims against the defense or any member of its team for the purposes of the defense analyzing or testing the computational forensic software.[196]

The measures provided by H.R. 2438 ensure that defendants have access to evidentiary material that affects the outcome of their criminal cases; additionally, it keeps third-party trade secret holders accountable for the technologies used in the criminal justice system.[197] In effect, rather than trade secret protections being treated like the false dichotomy with the only options being "complete secrecy" or "complete transparency," H.R. 2438 provides for a more equitable solution governing trade secret holders' rights and criminal defendants' constitutional rights.[198] In fact, Taylor Moore, a former Center for Democracy and Technology (CDT) Expression Fellow, argued that "[i]ntellectual property law and policy governing trade secrets should be reformed so that" fairness and equity are weighed between an individual's "liberty interests (i.e., due process, free expression, and equal protection) and a company's interest in maintaining its trade secret."[199]

In the reintroduction of the Justice in Forensic Algorithms Act, Representative Dwight Evans, who brought the bill back to Congress alongside Representative Takano, observed that criminal defendants "are being convicted based on the results of . . . potentially flawed forensic algorithms without the ability to challenge . . . [the] evidence due to . . . intellectual property interests."[200] From an intellectual property law standpoint, trade secret cases typically focus on the economic value of the proprietary information to the trade secret holder's business.[201] In the criminal justice context, however, the stakes are different; while there is no doubt that an economic incentive exists among criminal justice technologies, these technologies impact the lives of individuals at a much deeper level than economics, for example, Coca-Cola with its secret ingredients.[202] Further, criminal defendants are affected by secret algorithms that pose the risks of inaccuracy.[203] Therefore, if criminal justice technology can

[196] *Id.* § 2(g).

[197] *See* TAKANO, *supra* note 180.

[198] *See* Taylor R. Moore, *Trade Secrets & Algorithms as Barriers to Social Justice*, CTR. FOR DEMOCRACY & TECH. (Aug. 2017), https://cdt.org/wp-content/uploads/2017/08/2017-07-31-Trade-Secret-Algorithms-as-Barriers-to-Social-Justice.pdf [https://perma.cc/G3K9-M93G].

[199] *Id.*

[200] TAKANO, *supra* note 180.

[201] *See* Ryan, *supra* note 84, at 64.

[202] *See id.* at 87–88.

[203] *See id.* at 87.

convict an individual for a crime, "how do you know that the match is correct and not the result of a software bug?"[204]

On the other hand, prosecutors and trade secret holders against allowing disclosure of proprietary information may argue that H.R. 2438 "would harm scientific innovation, replace DNA truth with State-approved software, and transfer judicial powers from the experienced impartial courts to an unaccountable federal agency."[205] From their point of view, H.R. 2438 would actually conceal the truth from discovery and affect justice because the bill allows the federal government to regulate and control the evidentiary information introduced in criminal proceedings. Unbeknownst to the court and proponents for H.R. 2438, prosecutors and trade secret holders find that criminal justice technologies currently have "the power to bring the light of scientific truth into the courtroom, promoting justice for both the guilty and innocent."[206]

Additionally, opponents of H.R. 2438 may find that there is a lack of protection of trade secret holders' proprietary information because section 2(b) of the bill appears to require disclosure of trade secret information so long as the evidence is relevant.[207] Believing that access to source code will yield reliable and accurate results is flawed because "the text isn't used in testing[,]" though understandably, "its release can wreck an innovative company."[208] In fact, Dr. Mark Perlin, the Chief Scientist and Executive of Cybergenetics, noted that "source code isn't needed (in fact, it can't even be used) to test the accuracy of forensic algorithms: 'You don't learn how a car works by reading its blueprints; you take it for a test run.'"[209] In addition, opponents would emphasize that Congress actually "has no independent constitutional basis to regulate trade secrets."[210] However, if H.R. 2438 passed, Congress would appear to exercise control over proprietary information in the criminal justice context.[211] In the meantime, the "Supreme Court has recognized trade secrets" as a right that warrants "constitutional protection."[212] Therefore, trade secret holders would request Congress to avoid regulating their constitutionally protected information. By privileging proprietary information, Congress, in effect, would "incentivize companies to perform research and development."[213]

The arguments of prosecutors and trade secret holders, however, do not hold weight. Disclosure of proprietary information only increases financial risks for a trade secret holder; while criminal defendants, without disclosure, would risk

[204] *See* Walsh, *supra* note 152.

[205] *See* CYBERGENETICS, *supra* note 154.

[206] *Id.*

[207] *See* Justice in Forensic Algorithms Act of 2021, H.R. 2438, 117th Cong. § 2(b)(1) (2021).

[208] *See* CYBERGENETICS, *supra* note 154.

[209] *Id.*

[210] *See* Conor Tucker, *The DTSA's Federalism Problem: Federal Court Jurisdiction over Trade Secrets*, 28 FORDHAM INTEL. PROP., MEDIA & ENT. L.J. 1, 1 (2017).

[211] *See id.*

[212] Peter F. Daniel, *Protecting Trade Secrets During Discovery*, 30 TORT & INS. L.J. 1033, 1033 (1995) (footnote omitted).

[213] Rudin, Wang & Coker, *supra* note 157, at 5.

losing their freedom.[214] In California, the Electronic Frontier Foundation has urged an "appeals court to allow criminal defendants to review and evaluate the source code of forensic software programs . . . in order to ensure that none of the wrong people end up behind bars, or worse, on death row."[215] Moreover, precluding trade secret disclosure that affects a criminal defendant's liberty would "undermine the social good" that intellectual property could provide.[216] Instead, the criminal justice technologies may yield erroneous results and even indirectly impose "discriminatory social structures when these systems go unchecked and unregulated."[217] To avoid the risks of "harm from a mistake or an inaccuracy," H.R. 2438 should be passed to protect the constitutional rights, including life and liberty, of people negatively affected by criminal justice technology.[218]

V. CONCLUSION

Criminal justice technologies pose a threat to innocent lives affected by their inaccurate, unreliable, and incorrect results. Without disclosure of, or access to, source code or proprietary information surrounding these technologies, there is no way for criminal defendants to receive a full and fair trial when they are unable to confront the very evidence used to incriminate them. Therefore, H.R. 2438 should be passed to grant defendants a right to assess and analyze the technology used against them to protect their rights and liberties.

Trade secret law seeks to protect the confidential information of innovative and creative individuals as well as the economic value of the proprietary information. Trade secret privilege issues frequently arose in civil cases, where defendants attempted to misappropriate the protected information from the trade secret holder. Through trade secret law, courts were able to protect the intellectual property rights of trade secret holders and preclude defendants or other individuals from taking and profiting from the protected information. In civil courts, the trade secret privilege existed to preclude disclosure of confidential information during the discovery process because trade secret holders, when filing suit, should not have to worry about their secret information being revealed to the public, who may in turn take that information and take advantage of its economic value.

In the criminal context, federal and state rules have also sought to protect proprietary information from disclosure in court proceedings. To avoid constitutional issues, such as a violation of due process rights, criminal proceedings sought to use protective orders for confidential information, allowing only the attorneys to access the information for purposes of the case.

However, trade secret privilege is abused when it precludes criminal defendants from ensuring the results yielded by criminal justice technologies are

[214] *See* Ryan, *supra* note 84, at 106.
[215] *See* Walsh, *supra* note 152.
[216] *See* Moore, *supra* note 198.
[217] *See id.*
[218] *See id.*

accurate and reliable. Judges and juries have appeared to place criminal justice technologies on a pedestal for ensuring justice; thus, the criminal justice system believes that it should protect the intellectual property rights of trade secret holders. From the intellectual property perspective, protection of trade secrets encourages trade secret holders to advance their technologies because their intellectual property rights protect their business and the economic value behind their proprietary information. Unfortunately, from the perspective of criminal defendants, privileging trade secret information poses a risk of violating their constitutional rights and liberty. The lives of criminal defendants, in cases where criminal justice technologies are used, are ultimately affected by whatever results the technology yields, whether it is accurate or not. Judges and juries have assumed—sometimes without thinking—that criminal justice technologies always yield true and reliable results; however, that is not always the case. Innocent individuals have been charged and convicted because criminal justice technologies pose the risk of bias, error, and other inaccuracies.

In response to these issues, Representative Takano introduced H.R. 2438, the Justice in Forensic Algorithms Act of 2021, to prioritize criminal defendants above proprietary information. Representative Takano observed innocent people imprisoned from technology that may have yielded unreliable results; therefore, to protect the rights and liberties of these individuals, H.R. 2438 warrants the disclosure of source code information of criminal justice technologies. By requiring disclosure of the information, criminal justice technology companies are held accountable for the reliability of their technologies' use in the criminal justice context. Additionally, through H.R. 2438, these companies are held to a higher standard for the technology used to ensure increased accuracy when such results are levied against criminal defendants. Ultimately, H.R. 2438 will help protect criminal defendants' due process rights, Sixth Amendment rights, and human liberty rights, because the transparency of source code information leads to greater accountability of criminal justice technologies.