TRADE SECRETS & ALGORITHMS AS BARRIERS TO SOCIAL JUSTICE

By Taylor R. Moore

CDT Free Expression Fellow

August 2017

CENTER FOR
DEMOCRACY
& TECHNOLOGY

CENTER FOR
DEMOCRACY
& TECHNOLOGY

Trade Secrets and Algorithms as Barriers to Social Justice

By Taylor R. Moore, CDT Free Expression Fellow

August 2017

Abstract

Various mechanisms in the current intellectual property (IP) system balance competing interests of the rightsholders with the societal needs of the public. Unauthorized copyright use is not considered infringement if the use made is "fair," and patents require that innovations be described in detail to receive protection in order to promote the useful arts and sciences. Moreover, these types of limitations and social balancing mechanisms can be used to facilitate the use of intellectual property in a way that promotes social justice.

Although trade secret law bears the moniker of intellectual property, it lacks sufficient limits and balancing mechanisms to address the needs of the public. In contrast to copyright and patent law, trade secret law has expansive subject matter breadth, minimal requirements, no formal application process before acquisition, and encourages creators not to disclose information. While intellectual property law is intended to optimize social welfare by guarding against both the under- and over-protection of information, this failing in trade secret law can ironically allow IP protection to undermine the social good in certain circumstances.

This is particularly evident with faulty criminal sentencing algorithms that predict a defendant's likelihood of recidivism. Not only do these algorithms exacerbate the disparate impact on people of color in the criminal justice system, but they also grant a broad veil of protection from scrutiny by trade secret law. The lack of social balancing mechanisms, specifically as it applies to harmful criminal sentencing algorithms, puts trade secret law in tension with civil rights and other broader societal considerations.

In light of the disparate impact of criminal risk-assessment tools on minority defendants, the business preference for trade secret protection presents a conflict with basic obligations to protect civil rights. Altering the discussion of trade secrets to include a social balancing mechanism, as is the case in other forms of IP protection, would help to eliminate the tension by directly considering social justice in IP.

Introduction

In 2016, defendant Eric Loomis was sentenced to six years in prison, in part because of his rating on a predictive computer system, COMPAS, that measured his likelihood of recidivism. The court barred Loomis from accessing information related to how COMPAS weighed particular input variables and how these inputs were calculated for his final risk score, because the developer considered such information a trade secret. Because Loomis suspected that the software used sex as a factor in the scoring process, he challenged the court's denial by arguing that it was a violation of his equal protection and due process rights.[1] After the Wisconsin Supreme Court upheld his prison sentence and the use of the risk assessment software, Loomis petitioned the Supreme Court to grant certiorari – which was denied.[2]

Determining a defendant's likelihood of recidivism through risk assessment technology is becoming more commonplace in the United States' criminal justice system. However, in an effort to evaluate the technology's forecast of which individuals would re-offend, researchers found that the algorithm used to make this determination was unfairly biased against blacks.[3] And attempts to understand the components of the technology making these, in some cases, discriminatory decisions are protected by trade secret law. What the *Loomis* case demonstrates is the unique way that a flawed technological tool, protected by a faulty form of intellectual property protection, can merge and ultimately exacerbate racial disparities and impede on civil and human rights.

This paper argues that a social justice framework should be incorporated into trade secret protection when applied to risk-assessment algorithms. The framework is intended to fill the gap in trade secret law that allows unfettered protection for harmful risk-assessment algorithms used in the criminal justice system. Part one of this paper will discuss the lack of a mechanism that balances social justice objectives in trade secret law compared to the other forms of intellectual property. Part two will analyze the need for social justice considerations when deploying algorithms protected by trade secret. It will also examine how trade secret protection affects access to knowledge, the shared goal of both IP protection and human rights law. Finally, part three will posit the building blocks of a framework that will allow courts to consider whether the use of a risk-assessment algorithm in criminal sentencing is permissible.

I. Part I: The Use of Risk Assessment Instruments in Criminal Sentencing

Risk assessment tools, like the one used against Eric Loomis, have been adopted in nine states as of 2016.[4] Although these tools are among the most controversial trade secret technologies entering the criminal justice system, they are already being used in courtrooms across the country in parole, pre-trial, and sentencing determinations.[5] The algorithm used in a risk assessment instrument scores on a scale of "high," "low," based on factors such as one's socioeconomic status, family background, education level, employment status, and neighborhood crime.[6] Although this technology is widely used, there is some variation in the specific risk assessment tools used in each state. For instance, jurisdictions have used: The Correctional Offender Management Profiling for Alternative Sanctions

[1] Wisconsin v. Loomis, 371 Wis.2d 235, 243 (Wisc. 2016).
[2] Wisconsin v. Loomis, 371 Wis.2d 235 (Wisc. 2016), *cert. denied*, 85 U.S.L.W 3601 (U.S. Jun. 26, 2017) (No.16-6387).
[3] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, Machine Bias, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
[4] *Id.*
[5] *Id.*
[6] *See* Angwin; Algorithms in the Criminal Justice System, EPIC, https://epic.org/algorithmic-transparency/crim-justice/ (last visited Jul. 17, 2017).

(COMPAS), Level of Service Inventory Revised (LSI-R), the Public Safety Assessment (PSA), or adapted their own version of the three.[7] Moreover, there is also variation in the types of companies and organizations that make these instruments; some are for-profit companies, like Northpointe, the developer of COMPAS, and other tools, like PSA, are made by non-profit organizations.[8]

Proponents of these tools point to the efficiency that these instruments offer to the clogged U.S. criminal justice system.[9] To be sure, the ability to accurately predict which defendants would commit a crime in the future could alleviate some of the past discriminatory practices in the criminal justice system. In comparison to other countries, the United States incarcerates people at a significantly higher rate; and African Americans are incarcerated at state prisons across the U.S. at more than five times the rate of whites.[10] Much of this disparate impact stems from not only discriminatory laws and policies, but also the personal biases of those making key decisions in the legal process.[11] If technology could accurately predict recidivism, the argument goes, it holds the potential to streamline the criminal justice process and eradicate such discrimination.

However, many of the concerns about the use of risk-assessment instruments pertain to them as a source of bias, as demonstrated by ProPublica's 2016 investigation into COMPAS.[12] ProPublica, a non-profit news organization, launched an in-depth analysis into the racial bias that results from the risk-assessment algorithms used to "inform decisions about who should be set free at every stage of the criminal justice system" by analyzing Northpoitne's tool, COMPAS. After comparing the predicted recidivism of criminal defendants in Florida with their actual rate of recidivism, ProPublica found that COMPAS correctly predicted recidivism 61 percent of the time, but only correctly predicted violent recidivism 20 percent of the time. Although the algorithm correctly predicted who would re-offend amongst black and white defendants at the same rate, it made mistakes that disfavored black defendants. Black defendants were far more likely than white defendants to be incorrectly judged to be at a higher risk of recidivism and violent recidivism,[13] while white defendants were more likely than

[7] *See* EPIC.

[8] Public Safety Assessment, The Arnold Foundation, http://www.arnoldfoundation.org/initiative/criminal-justice/crime-prevention/public-safety-assessment/ (last visited July 17, 2017).

[9] Angwin, *supra* note 3; Melissa Hamilton, We Use Big Data to Sentence Criminals. But Can the Algorithms Really Tell Us What We Want to Know, The Conversation (Jun. 5, 2017), http://theconversation.com/we-use-big-data-to-sentence-criminals-but-can-the-algorithms-really-tell-us-what-we-need-to-know-77931. ("Automated risk assessment is seen as a way to standardize the process. Proponents of these tools, such as the nonprofit National Center for State Courts, believe that they offer a uniform and logical way to determine risk.")

[10] Ashley Nellis, Ph.D., The Color of Justice: Racial and Ethnic Disparity in State Prisons, The Sentencing Project (June 14, 2016), http://www.sentencingproject.org/publications/color-of-justice-racial-and-ethnic-disparity-in-state-prisons/.

[11] Id.("Cassia Spohn's research on sentencing reasons that for less serious crimes, judges might depart from the constraints of the law, allowing other factors to enter into their judgment. These factors might include forms of racial bias related to perceived racial threat."); Angwin, *supra* note 3.

[12] Angwin, *supra* note 3.

[13] *Id.* ("[The] analysis found that black defendants who did not recidivate over a two-year period were nearly twice as likely to be misclassified as higher risk compared to their white counterparts…").

black defendants to be incorrectly flagged as low risk.[14] Even when controlling for violent prior crimes, age, gender, and future recidivism, black defendants were still more likely than white defendants to be assigned higher risk scores.[15]

An additional source of concern is the intellectual property law used to protect this software, as well as the lack of transparency around its components, which include: data used as input to an algorithm, the algorithm itself, and final models. As more of these technologies enter into criminal justice proceedings, developers continue to ward off attempts to unearth details about how their tools function by asserting that the information is protected by trade secret law. Flawed algorithms shrouded in a faulty form of intellectual property, deployed in criminal sentencing, and lacking clear transparency requirements are likely to reinforce discriminatory hierarchies. The White House's first Big Data Report warned of "the potential of encoding discrimination in automated decisions" – that is, discrimination may "be the inadvertent outcome of the way big data technologies are structured and used."[16] In the 2016 report, the White House noted the risk of data and algorithmic systems being used in ways that exacerbate unwarranted disparities, especially in the criminal justice system.[17]

Permitting the perpetuation of discrimination through weakness in trade secret protection undermines the underlying principles of intellectual property protection and, instead, stifles innovation, progress, and societal development. In *Loomis v. Wisconsin*,[18] the defendant argued that his inability to access and challenge the assessments or calculations that transformed the underlying data was an impermissible violation of his due process rights. The state, however, ruled against Loomis, and the Supreme Court has denied Loomis's cert petition. However, given the increasing use of these technologies in a variety of contexts across the judicial system, this issue is likely to come before a court in another case in the near future.

II. Part II: Trade Secret And Risk-Assessment Tools – The Social Effects And The Discriminatory Impact

A. Trade Secret Protection in the United States

Unlike U.S. copyright and patent law, the legal justification for trade secret law does not come from the Constitution,[19] but is instead based in common law and codified separately in most states.[20] U.S. trade

[14] *Id.* ("...white defendants who re-offended within the next two years were mistakenly labeled low risk almost twice as often as black re-offenders.").

[15] *Id.* ("The analysis also showed that even when controlling for prior crimes, future recidivism, age, and gender, black defendants were 45 percent more likely to be assigned higher risk scores than white defendants.") ("The violent recidivism analysis also showed that even when controlling for prior crimes, future recidivism, age, and gender, black defendants were 77 percent more likely to be assigned higher risk scores than white defendants.").

[16] *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President, May 2014, https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

[17] *Id.*

[18] Loomis, at 243.

[19] U.S. Const. art. I, § 8, cl. 8.

secret law is meant to protect valuable business information from theft and espionage.[21] The threshold requirement for a trade secret is that the information being protected is commercially valuable (such as a customer list, a method of production, or a secret formula for a soft drink).[22] Not only is there no formal application process for trade secret protection, but a trade secret can be maintained indefinitely as long as the rightsholder takes reasonable precautions to keep the information secret.[23]

The flexibility afforded by trade secret's minimal substantive requirements and lack of a formal application process makes it a favored form of protection for innovators, start-ups, and companies seeking to protect proprietary software.[24] Trade secret is often chosen over patent protection because trade secret law is the only form of IP protection that gives innovators any meaningful protection over algorithms. Algorithms, as mathematical formulas, are abstract ideas which precludes them from patent protection.[25]

In the case of algorithmically driven products, disclosure of how the product works not only undermines its protection, it can destroy the creator's ability to exploit their intellectual property and can even render the product ineffective.[26] But while this form of IP protection allows companies to securely deploy cutting-edge software in various fields, it can simultaneously perpetuate and exacerbate existing discriminatory social structures when these systems go unchecked and unregulated.[27] Moreover, if the instrumental mandate of intellectual property is truly to increase access to knowledge and support societal benefits,[28] it is counterproductive to encourage innovation that has the potential to foster discrimination without some kind of balancing/limiting mechanism.

[20] Brian T. Yeh, Protection of Trade Secrets: Overview of Current Law and Legislation, Congressional Research Service (Apr. 22, 2016), https://fas.org/sgp/crs/secrecy/R43714.pdf.
[21] *Id* at 3.
[22] *Id*.; ConFold Pac v. Polaris Indus., 433 F.3d 952, 959 (7th Cir. 2006).
[23] *Id*.
[24] Deepa Varadarajan, Trade Secret Fair Use, 83 Fordham L. Rev. 1401 (2014).
[25] In Diamond v. Diehr, the Court held that mathematical formulas in the abstract are not eligible for patent protection. Therefore, software algorithms could not be patented. *See* Diamond v. Diehr, 450 U.S. 175 (1981).
[26] Tania Cerquitelli, Daniele Quercia, and Frank Pasquale, Transparent Data Mining for Big and Small Data, 30 Springer (2017) ("Barriers and challenges to effective algorithm transparency efforts were…concerns of proprietary information that would damage competitive advantages, or leave a system open to manipulation…privacy considerations from disclosure of improperly anonymized data…")
[27] A.R. Lange, *Digital Decisions: Policy Tools in Automated Decision-Making*, Center for Democracy and Technology (Apr. 10, 2017), https://cdt.org/files/2016/01/2016-01-14-Digital-Decisions_Policy-Tools-in-Auto2.pdf. ("Algorithms learn based on the training data and human-defined inputs and selection criteria, which means that discrimination can be 'baked in' to the process from the beginning...An algorithm is useful for identifying trends based on statistical correlation and, in the right hands, can sometimes be used to accurately predict a specific outcome. However, it can only predict the future based on the past—or more specifically on whatever data about past events is on hand. Because of this, the results can unintentionally be discriminatory or exacerbate inequality — 'garbage in, garbage out' [short hand for "put biased data in, get biased results out'] is one of the potential problems of using this technology to make decisions.").
[28] *See generally*, Intellectual Property Protection and Enforcement, The World Trade Organization, https://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm (last visited Jan. 8, 2017)

In fields such as criminal sentencing, where traditionally marginalized groups are historically disadvantaged, algorithmic discrimination that is protected by trade secret law is particularly damaging because it threatens access to information. Under traditional methods, black and Latino offenders sentenced in state and federal courts face significantly greater odds of incarceration than similarly situated white offenders, and receive longer sentences than their white counterparts in some jurisdictions.[29] As the use of opaque risk-assessment tools increases, there are concerns about the reinforcement of existing prejudices and inequalities through a “techno-social divide.”[30] Researchers found that such risk-assessment formulas have been written in a way that guarantees black defendants will be inaccurately identified as future criminals more often than their white counterparts.[31]

B. Social Justice Considerations in Intellectual Property Protections

Trade secret law, like other forms of intellectual property protection, is intended to promote information creation and dissemination. This makes it inextricably intertwined with fundamental rights to freedom of expression and access to information.[32]

Legal scholars, such as Peter Menell,[33] Lateef Mtima,[34] and Margaret Chon,[35] argue that an important social utility exists at the intersection between intellectual property law and broader social justice concerns. They argue that if the primary goal of IP law is to increase knowledge for positive uses in society, then there must be a fuller consideration of how intellectual property law affects access to information and public goods such as education and healthcare. As important as it is to recognize the

[29] The American Civil Liberties Union, Written Submission of the American Civil Liberties Union on Racial Disparities in Sentencing, https://www.aclu.org/sites/default/files/assets/141027_iachr_racial_disparities_aclu_submission_0.pdf.

[30] Jules Polonetsky & Omer Tene, *Who is Reading Whom Now: Privacy in Education from Books to MOOCs*, 17 Vand. J. Ent. & Tech. L. 927 (2014); Alex Bradshaw, *States Take Steps to Limit School Surveillance of Student Social Media Pages*, Center for Democracy and Technology (Jan. 27, 2016), https://cdt.org/blog/states-take-steps-to-limit-school-surveillance-of-student-social-media-pages/ (discussing the ways in which student surveillance can lead to racial, ethnic, and religious profiling by schools); Angwin, *supra* note 3.

[31] Julia Angwin and Jeff Larson, Bias in Criminal Risk Scores Is Mathematically Inevitable, Researchers Say, ProPublica (Dec. 30, 2016), https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say.

[32] Because IP is a social ordering mechanism that plays a role in determining the information that the public has access to, the dissemination of information component of IP that is meant to incentivize creation also impacts human rights. Steven D. Jamar, A Social Justice Perspective on the Role of Copyright in Realizing International Human Rights, 25 Pac. McGeorge Global Bus. & Dev. L.J. 289, 291 (2012) (“The interaction of copyright with human rights extends far beyond incentivizing the creation and dissemination of information. At the polar opposite of facilitating and encouraging dissemination, a too-encompassing copyright law could stymie creation and dissemination of information by limiting access to and use of that information. Consequently, in order to ensure that the public interest and the individual rights of expression are served (as noted by the U.S. Supreme Court in Eldred), copyright law itself must be subject to safeguards in the form of limitations on the extent of the rights. In particular, the exclusion of ideas from protection and the grant of fair use serve to balance the grant of a property right with the imperatives of human rights.”).

[33] *See* Peter S. Menell, Property, Intellectual Property, and Social Justice: Mapping the Next Frontier, 5 Prop. Rts. Conf. J. 147 (2015).

[34] Lateef Mtima, Copyright and Social Justice in the Digital Information Society: “Three Steps” Toward Intellectual Property Social Justice, 53 Hous. L. Rev. 459 (2015).

[35] Margaret Chon, Intellectual Property and the Development Divide, 27 Cardozo L. Rev. 2821 (2006)

economic and utilitarian benefits of intellectual property protection, it is equally important to recognize how the law affects access to information. This type of consideration is particularly necessary when examining companies protecting their algorithms by trade secret law and deploying them in situations that impinge access to knowledge.

The right to freedom expression, which includes access to information, is a fundamental right enshrined in the framework of the International Covenant on Civil and Political Rights (ICCPR).[36] Free expression is recognized as an enabling right that allows individuals to fully engage in their enjoyment of other rights, including their economic, social, and cultural rights. The pursuit of social justice is the effort to eliminate barriers to full and equal participation in social, economic, and cultural life – trade secret protected algorithms can act as a barrier to information, which fundamentally impacts human rights and social justice.

III. Part III: Addressing the Problem: Identifying And Delineating A Social Balancing Mechanism For Trade Secret In The Context Of Risk-Assessment Algorithms

A. The Social Justice Flaw in Trade Secrecy

The current intellectual property regime makes social justice accommodations to promote socially balanced IP law that will ultimately benefit the public.[37] Disclosure requirements for copyright and patents reflect the value that scientific and technical openness benefits society more than confidentiality and secrecy.[38]

Patent protection balances the interests of the rightsholder with those of the public by requiring a written description of the protected invention "to enable" a person of ordinary skill in the field to make

[36] International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), U.N. GAOR, 21st Sess., Supp. No. 16, U.N. Doc. A/6316, at 16 (Dec. 16, 1966) [hereinafter ICCPR] (entered into force Mar. 23 1976).

[37] Jamar, supra note 28, at 296 ("With respect to real property, the power of eminent domain, zoning, nuisance, and other limitations for the public good are commonplace. Intellectual property - even if founded on natural law - is properly subject to similar limitations for the public good. As with core human rights like freedom of expression, intellectual property rights cannot be so absolute that they unduly impinge on other rights (such as free speech) or undermine the public good. Finally, the granting of intellectual property rights themselves - regardless of the underlying theory - can serve the interests of social justice and the public good. Thus, a natural rights perspective is not necessarily antithetical to crafting intellectual property law, policy, and administration to encourage innovation and entrepreneurship; balancing interests is the key.")

[38] Mtima, *supra* note 30 at 462 ("Intellectual property social justice contemplates the precepts of socially equitable access, inclusion, and empowerment as both intrinsic and essential to the fulfillment of the goals of intellectual property social utility."); Deepa Varadarajan, Trade Secret Fair Use, 83 Fordham L. Rev. 1401, 1404, 1407 ("To be liable for trade secret misappropriation, however, one must "misappropriate" the protected information. That is, the acquisition, use, or disclosure of the information must involve "improper means" or breach of a confidentiality duty.6 This requirement makes trade secret law unique and reflects how its origins differ from those of patent and copyright laws. Despite such differences, however, courts and scholars increasingly view trade secret law as a subset of intellectual property, because like patent and copyright laws, trade secret law can also serve as a mechanism to encourage invention and creation.") (Patent law protects certain categories of inventions that are useful, new, and nonobvious in light of the previous knowledge (or "prior art") and satisfy various disclosure requirements.").

use of the invention.[39] In copyright, the primary social balancing mechanism is the Fair Use Doctrine.[40] Recognizing the public privilege to make “fair use”[41] of a copyrighted work promotes a socially balanced perspective in copyright and equitably weighs an author’s exclusive right with the social utility objectives of copyright.[42]

While trade secret law protects certain kinds of information as intellectual property protection, it lacks any expressly delineated social justice balancing mechanism between the rightsholder and the public, unlike patents and copyright. It effectively prioritizes secrecy over the dissemination of information for a never-ending amount of time, requiring only that the object of the trade secret remain undisclosed. Here, the general model of IP protection – protection for a work or invention in exchange for the public benefiting from an expanded corpus of knowledge – is not followed. In some cases, the public certainly receives some direct benefit from the trade secret protected product. However, the calculus is fundamentally different in cases where the harm from a mistake or an inaccuracy is so high and incentives to cure such flaws are not properly aligned.

This is especially true when undisclosed information will be deployed in a way that affects an important system of civic life (e.g., the criminal justice system). Without any social balancing mechanism, analogous to fair use, trade secret law could be a vehicle for societal harms that are not easily discoverable. As scholars have noted, the steady advancement of information technologies related to the “creation, dissemination, and use of information in all its forms” poses new and unique challenges to the “legal regime in mediating competing interests –especially intellectual property law.”[43]

Disclosure to other regulatory agencies can mitigate some of the risks of certain trade secrets. For instance, the recipe for Coca-Cola can be protected by trade secret law, but the beverage is also covered under Food and Drug Agency (FDA) regulation of food safety. This “safety valve” may well be effective in industries where the end product of a trade-secret protected algorithm is already

[39] 35 U.S.C. 112(1)

[40] Mtima, *supra* note 30.

[41] As part of the fair use determination, courts will consider: (1) the purpose and character of your use; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion taken; and (4) the effect of the use on the potential market; See 17 U.S.C. § 107 (2012).

[42] Lateef Mtima, Copyright and Social Justice in the Digital Information Society: “Three Steps” Toward Intellectual Property Social Justice, 53 Houston L. Rev. 459, 470. (For example, a 2012 copyright case, adjudicated by U.S. Court of Appeals for the Second Circuit, explicitly considered the social objectives of a copyright use in its final decision. In the case, the court held that Google Books, which “undertook digital scans of books in several university libraries in order to enhance public access to, scholarly research in, and archival preservation of these books, also constitute[ed] a transformative fair use.” In the case, the court explicitly considered the “objectives of the federal Americans with Disabilities Act in its assessment of the pertinent copyright interests, and ultimately concluded that unauthorized reproduction of copyrighted works for the purpose of making them accessible to the blind must be as a Fair Use.”)

[43] Jamar, *supra* note 28 at 298 (“With the ongoing explosion of information technologies relating to creation, dissemination, and use of information in all its forms, the challenges and opportunities are greater than ever before. This exaggerated impact of information concomitantly makes the impact of the legal regime in mediating competing interests - especially intellectual property law and most particularly copyright law - more important than it may have been historically.”).

regulated; for example, if Coca-Cola were to develop a recipe for 'New Coke' through a proprietor algorithm, the beverage would still be subject to FDA regulations. But in many cases, there may be no pre-existing regulations that apply to the outputs of an algorithm.[44] Moreover, waiting for a risk-assessment algorithm to fall under the purview of another form of established regulation is not an appropriate or efficient form of recourse to address the *immediate* and acute concerns faced by defendants currently being sentenced by these algorithms. Additionally, a solution must address specifically intellectual property because the problem in this situation stems from a flaw in a form of IP. Having a balancing mechanism that is "baked into" trade secret law provides a more reliable touchstone not only for individuals subjected to the algorithms, but also as a quality standard for companies as they release new risk-assessment technology.

B. Creating Equitable Trade Secrets Solutions

The outcome in *Loomis* demonstrates the need to address how trade secret protection and civil rights interact with one another. Although there have been rich discussions and advances by researchers around algorithmic accountability as a general issue,[45] it is important to address and examine this situation from an intellectual property perspective because IP is one of the main barriers to this information. If trade secret protection operated less like a binary, where the only options for a company are complete secrecy and complete transparency, there could be fair and balanced trade secret protection.

Intellectual property law and policy governing trade secrets should be reformed so that there is an equitable balance between people's liberty interests (i.e., due process, free expression, and equal protection) and a company's interest in maintaining its trade secret. Now that more technology acts as a gatekeeper to resources and democratic systems, it is necessary to ensure that there are social balancing mechanisms in place that specifically apply to the intellectual property that protects risk-assessment tools.

Because trade secret law protects everything from recipes, client lists, and algorithms, it is important that any type of proposed framework apply specifically to the use of algorithms in the criminal justice system. This framework is not attempting to apply the standards of criminal procedure onto trade secret protected algorithms simply because they are used in the criminal justice system. Instead, this framework is intended to make certain that this form of IP, which is good for algorithms, does what it's supposed to do when this technology is applied in criminal sentencing. A safety valve, specifically applied to risk-assessment algorithms, are needed to bridge the incompatibility between trade secrecy and the openness required in criminal procedure.

[44] *Contra*, European Union's new General Data Protection Regulation effectively create a "right to explanation," whereby a user can ask for an explanation of an algorithmic decision that was made about them.

[45] Nicholas Diakopoulos and Sorelle Friedler, How To Hold Algorithms Accountable, MIT Technology Review (Nov. 17, 2016), https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/; Alex Rosenblat, Tamara Kneese, and Danah Boyd, Algorithmic Accountability, Data & Society (Mar. 17, 2014); https://datasociety.net/pubs/2014-0317/AlgorithmicAccountabilityPrimer.pdf.

To better achieve this balance, I propose a loose framework for transparency when a defendant challenges risk-assessment algorithms.

There Must Be Structured Frameworks for Limited Disclosure of Trade Secret Protected Algorithms That Are Used in the Criminal Justice System When They Are Challenged by a Defendant

Loomis v. Wisconsin demonstrated the need for clearly articulable circumstances in which a challenged trade secret protected algorithm should be disclosed. Trade secret protection should not hide poorly functioning algorithms; thus, a workable framework is required. Similar to fair use, this proposed framework is meant to be a safety valve in trade secret law that specifically applies to algorithms used in the criminal justice system and is meant to address the ways in which IP law directly conflicts with social welfare.

Previously, proposed safety valves for trade secret law have included a proposal for trade secret fair use.[46] This former framework was based on the fair use standard used in copyright, but was intended to address permissible circumstances wherein a transgressor violates trade secret law for a socially beneficial reason, like follow-up improvements to something protected by trade secret or for First Amendment interests. The framework proposed in this paper also resembles copyright fair use in certain respects, but diverges in its attempts to specifically address a narrower question. Unlike copyright fair use and the previously proposed model for trade secret fair use, this framework does not evaluate whether an individual made use of another's intellectual property for permissible reasons. Instead, it focuses on providing a standard for courts to assess whether a risk-assessment tool, protected by trade secret law, is being unfairly applied in criminal sentencing.

In copyright, fair use is an important social valve because it allows courts to consider the social impacts of unauthorized uses of copyrighted material. Additionally, the fair use framework is purposefully flexible in that it uses a non-exhaustive list of factors to be considered when determining whether an unauthorized use is permissible. Instead of a preconceived list, fair use allows courts to weigh four statutory factors when evaluating the unauthorized use of copyrighted work: (1) the purpose and character of the use (e.g., whether such use is of a commercial nature or is for nonprofit educational purposes); (2) the nature of the copyrighted work (e.g., whether it is of a technical nature, like a manufacturing process, or a business nature, like pricing data); (3) the amount and substantiality of the work (e.g., the extent to which the defendant has "improved" upon the trade secret information); (4) the effect that allowing the use would have on the market for the copyrighted work.

As a matter of right, a similar framework needs to be established within the context of trade secret when it applies to algorithms. Like fair use, this framework should be a flexible series of factors that the court should use to consider when analyzing whether the use of a risk-assessment tool is permissible in sentencing. The factors that a court should consider when the permissibility of the use of a risk-assessment algorithm in a sentencing determination are:

[46] *Supra*, Deepa note 34.

(1) Whether the Use of the Tool Poses a Risk to a Defendant’s Liberty Interest (e.g., the 14th Amendment)

When a criminal plaintiff challenges a criminal risk-algorithm used against them based on its validity or violation of constitutional rights, a plaintiff needs to show the court that there must be a limited lift on the veil on the trade secret protected algorithm. Similar to Loomis, the defendant must establish that there is an important liberty interest at stake, such as one’s due process right and the right to equal protection under the law. This is an important preliminary standard because it ensures that the test is only applied to a very narrow class of people that have the greatest potential of harm by a risk-assessment tool.

(2) A Demonstration of a Pattern of Bias When the Tool Is Used in Sentencing Determinations

Second, the court should consider evidence showing that that there has been a pattern of bias in the tool’s assessments of defendant’s. Similar to ProPublica’s evidence related to COMPAS, there needs to be evidence that a certain type of defendant was consistently ascribed higher risk assessment scores than their white counterparts for the same/similar crimes.

(3) Whether the Producer(s) Of the Algorithm Took Affirmative Steps to Account for Bias

Finally, there needs to be an assessment of the affirmative steps taken to adjust its software and mitigate bias. This could include evidence that a company scrutinizes its algorithm through audits,[47] internal ethical review board/committee,[48] or through some other method. Once that process is satisfied the judge should rule on whether bias is likely and if so the court should demand disclosure of relevant components of the algorithm.

This framework provides a model that fairly benefits all interested parties by providing a limited and narrow incursion into a company’s trade secret material. Not only is this framework flexible enough to adapt to different types of risk algorithms, but it also helps companies understand and anticipate the circumstances that could result in the disclosure of some component of their software. Additionally, the flexibility and lack of an exhaustive list of standards and criteria needed to prove bias ensures that the test remains malleable enough so that challengers of the algorithm can introduce a wider array of

[47] Diakopoulos & Friedler, *supra* note 41. (“The principle of *auditability* states that algorithms should be developed to enable third parties to probe and review the behavior of an algorithm. Enabling algorithms to be monitored, checked, and criticized would lead to more conscious design and course correction in the event of failure.”)

[48] The Information Commissioner’s Office’s (ICO’s) response to the Science and Technology Committee’s call for evidence on algorithms in decision-making, Information Commissioner’s Office (Apr. 10, 2017), https://ico.org.uk/media/about-the-ico/consultation-responses/2017/2013970/ico-response-house-of-commons-science-tech-algorithms-20170410.pdf. (“...internal organisational ethics boards can also be setup to apply ethical principles and assess difficult issues that can arise in the creation and use of algorithms in decision-making. Such boards, or committees, can raise relevant questions about matters of fairness and accuracy in order that any potential issues can be identified and then addressed by the data scientists responsible for the algorithm.”)

evidence concerning a tool's potential bias. On the other hand, it also allows companies to find new ways to mitigate bias with their tools.

Going forward, an additional component of this framework that will need to be developed will be a determination of what *can* feasibly be explained about the design of the algorithm if a company fails to satisfy the elements of the framework, such as the data that went into its creation and its decision-making. Moreover, courts will need to determine how much information a company needs to furnish about their protected software on a case-by-case basis. For instance, it might be inappropriate to demand to see a company's source code in every case that challenges its equitability. Additionally, this framework puts a burden on judges to become better versed on how algorithms work and the various ways that they can create a feedback loop that contributes to bias through the help of experts. However, this learning curve is not dissimilar to the one that judges have to undergo in a complex music copyright case, where experts in musicology may be necessary.

Conclusion

The expansive nature of trade secrets, coupled with the lack of meaningful limits and doctrinal indifference to social justice considerations inherent in this form of IP protection, allows companies to block a wide array of information from scrutiny. This is particularly concerning, given trade secret law's expansive subject matter breadth, ease of acquisition, and increasing attractiveness to companies.

Intellectual property law is intended to optimize social welfare by guarding against both the under- and over-protection of information. Because of the significant role of IP protection in the technologies that inform our lives and social systems, it is increasingly important that IP be balanced amongst the public and rightsholders, and comport with the social needs of the society. The fact that trade secret protection has a low threshold requirement for something to be considered a trade secret, unlike other forms of IP, means that there is more room for the continued protection of potentially harmful technologies under this form of IP law. This strong legal protection for technology with potentially harmful consequences will continue to pose a threat to fundamental rights when such technology is used in situations that depend on transparency as a core component of their legitimacy, such as criminal justice.

Tackling this requires a reform to trade secret law. This will have to be an effort that is taken up by companies and the judicial system together. The case law, as well as the research into the discriminatory effect of risk assessment algorithms, requires answers from companies. It is no longer sufficient for companies to remain legally insulated by trade secret law while asking the public to blindly trust their intentions. Going forward, it will be important to build on the various factors from the framework outlined in this paper as research on this topic continues to take shape. This ensures that the framework remains up to date with current standards on ethical and accountable algorithms.