LIFE, LIBERTY, AND TRADE SECRETS: INTELLECTUAL PROPERTY IN THE CRIMINAL JUSTICE SYSTEM

Rebecca Wexler[*]

ABSTRACT

From policing to evidence to parole, data-driven algorithmic systems and other automated software programs are being adopted throughout the criminal justice system. The developers of these technologies often claim that the details about how the programs work are trade secrets and, as a result, cannot be disclosed in criminal cases. This Article turns to evidence law to examine the conflict between transparency and trade secrecy in the criminal justice system. It is the first comprehensive account of trade secret evidence in criminal cases. I argue that recognizing a trade secrets evidentiary privilege in criminal proceedings is harmful, ahistorical, and unnecessary. Withholding information from the accused because it is a trade secret mischaracterizes due process as a business competition.

---

[*] Rebecca Wexler is a Yale Public Interest Fellow at The Legal Aid Society and a Resident at The Data and Society Institute. I am grateful to Tracey Meares for her feedback and generous guidance since the inception of this project. Andrea Roth's and Edward Imwinkelried's incisive, in-depth comments and detailed correspondence have been invaluable. Thank you to Kiel Brennan-Marquez, Bryan H. Choi, Jessica Eaglin, Janet Haven, Edward Imwinkelried, Caroline Jack, Amy Kapczynski, Logan Koepke, Charlton McIlwain, Josh Scannell, Kevin Werbach, and Elana Zeide for thoughtful responses to earlier drafts. Thank you to Akhil Reed Amar, Ian Ayres, Jack Balkin, danah boyd, Owen Fiss, Peter Galison, Keith Hiatt, Dan Kahan, Alexa Koenig, Julie Krishnaswami, and participants in the Information Society Project Ideas Lunch series for energizing discussions. David Murdter provided sharp, dedicated research assistance.

CONTENTS

INTRODUCTION

This summer, the Wisconsin Supreme Court rejected a defendant's request to scrutinize alleged trade secrets in an algorithmic risk assessment instrument used to sentence him. The court reasoned that no due process violation occurred in part because the judge's own access to the secrets was equally limited. In 2015, a death row defendant in California was denied access to the source code for a forensic software program that generated the key evidence against him; the program's commercial vendor considers the code to be a trade secret. The Department of Justice has claimed a trade secrets privilege to refuse to disclose information about the operation of a cybercrime investigative software program, impeding judicial review of whether the warrantless use of the tool violates the Fourth Amendment.

These cases and others like them herald a growing trend. Criminal justice decision-making is becoming automated and privatized. From police to crime laboratories to courts, algorithmic and data-driven technologies increasingly guide criminal justice outcomes. Predictive policing systems deploy officers to "hot spot" neighborhoods. Forensic scientists use proprietary software programs to analyze DNA, fingerprint, ballistic, face and image recognition, social media, and other forms of digital evidence. And judges and parole boards rely on risk assessment instruments, which purport to predict whether an individual will commit a future crime, to decide who will make bail or parole.

As these technologies enter criminal proceedings, they are bringing new types of property claims with them; developers often assert that details about how the tools function are trade secrets. These developers purport to own intellectual property rights in the very means by which the state decides what neighborhoods to police, whom to incarcerate, and for how long. The introduction of intellectual property into the criminal justice system raises under-theorized tensions between life, liberty, and property interests. Criminal defendants enjoy a unique array of procedural rights: to confrontation and compulsory process, to present a defense, to due process and a public trial. These guarantees increasingly clash with trade secrets in criminal justice technologies.

This Article turns to Evidence Law to examine the conflict between transparency and trade secrecy with respect to these emerging criminal justice technologies. It is the first comprehensive account of trade secret evidence in criminal cases. In sharp contrast to an apparent growing consensus among courts, legislators, and scholars alike, I argue that trade secrets should not be privileged in criminal proceedings. As with other kinds of sensitive information, such as witnesses' medical records, courts may issue protective orders to limit the use and distribution of relevant evidence beyond the needs of the proceeding.[1] But trade secrets holders should wield no special power to block defendants' access to evidence altogether.

What I will refer to as the "intellectual propertization" of core aspects

[1] In later parts, this Article briefly raises the potential conflict between protective orders and Sixth Amendment public trial rights. However, I do not analyze the issue in depth and it is ripe for future scholarly contribution. For a helpful overview of recent public trial jurisprudence, *see* Note, Kristin Saetveit, *Close Calls: Defining Courtroom Closures Under the Sixth Amendment*, 68 STAN. L. REV. 897 (2016).

of the criminal justice system is hardly an isolated phenomenon. Legal scholars have debated the clash between secret "black box" methods in algorithmic tools and values of transparency and accountability in a wide array of public and private domains. This debate over secrecy and disclosure has touched everything from intelligence surveillance and public infrastructure,[2] to commercial activities,[3] health care;[4] administrative decision-making,[5] and to some extent civil and criminal procedure.[6] Yet to date, iterations of these tensions in Evidence Law remain almost entirely unexamined.[7] This lack of scrutiny is all the more

---

[2] *See, e.g.*, Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843 (2014) (documenting the governments' failure to notify criminal defendants of secret electronic surveillance programs), *and* David S. Levine, *Secrecy and Unaccountability: Trade Secrets in our Public Infrastructure*, 59 FLA. L. REV. 135 (2007) (examining trade secrets in voting machines and municipal wireless Internet providers).

[3] *See, e.g.*, Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014) (considering trade secrets in automated scoring systems such as credit ratings).

[4] *See, e.g.*, Roger Allen Ford & W. Nicholson Price, *Privacy and Accountability in Black-Box Medicine*, 23 Mich. Telecomm. & Tech. L. Rev. 1 (2016).

[5] *See, e.g.*, Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735 (2015) (arguing that data-driven administrative decision-making creates a *de facto* "guilty until proven innocent" burden); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 117 (2014) (suggesting that procedural due process should guarantee a "right to audit the data used to make the determination"); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008).

[6] *See, e.g.*, Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981 (2014) (identifying non-intellectual property barriers, such as states secrets, that impede defense access to evidence); Brandon L. Garrett, *Big Data and Due Process*, 99 CORNELL L. REV. ONLINE 207 (2014) (considering how big data evidence interacts with constitutional criminal procedure); Erin Murphy, *The new Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CAL. L. REV. 721, 729-30 (2007) (raising proprietary interests as one of a number of problems with the oversight of new forensic techniques).

[7] Welcome exceptions to the general lack of scrutiny include Andrea L. Roth, *Machine Testimony*, __ YALE L.J. __ (forthcoming 2017); Edward J. Imwinkelried, *Computer Source Code: A Source of the Growing Controversy Over the Reliability of Automated Forensic Techniques*, __ DEPAUL L. REV. __ (forthcoming 2017); *and* Note, Christian F. Chessman, *A 'Source' of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CAL. L. REV. __ (forthcoming 2017); Jennifer Mnookin, *Of Black Boxes, Instruments, and Experts: Testing the Validity of Forensic Science*, 5 EPISTEME 343 (2008) (discussing source code transparency issues in admissibility hearings); Note, Jennifer N. Mellon, *Manufacturing Convictions: Why Defendants are Entitled to the Data Underlying Forensic DNA kits*, 51 DUKE L.J. 1097 (2001) (arguing that DNA evidence should be inadmissible unless the underlying testing protocols are disclosed). *See also* Jessica Eaglin, *When Technology Replaces Judicial Discretion*, (working paper,

troubling given that privilege law, which applies to pretrial and post-conviction proceedings, has maintained relevance even as the number of trials has plummeted.[8]

I begin in Part I by describing examples of recent trade secret claims that have followed in the wake of a widespread adoption of algorithmic, data driven and other types of software programs in criminal justice decision-making. Part II explains the current standards that govern the trade secrets evidentiary privilege and makes the novel argument that privileging trade secrets is particularly harmful in criminal cases. As applied to criminal proceedings, the existing standards for the privilege do not adequately safeguard against over-claiming and abuse, and will almost certainly lead to the wrongful exclusion of highly probative evidence. Further, recognizing the privilege in this context offends procedural justice by signaling that the government values trade secrets holders as a group more than those directly affected by criminal justice outcomes, including other types of material witnesses compelled to testify in criminal cases.

In Part III, I argue that a broad trade secrets privilege in criminal trials is also ahistorical, by explaining that the standards governing the privilege developed in, and for, civil disputes. By mining previously under-scrutinized archival records, I recover key dissents to recognizing a trade secrets privilege—even in civil cases—that have been discarded from the historical record. I then use those unearthed dissents to develop a more thorough intellectual history of the privilege, which in turn exposes legislative efforts to manufacture a general consensus in its favor. Next, I show that, despite widespread acceptance of the privilege during the mid-Twentieth Century, its application to criminal proceedings was virtually unprecedented until the 1990s.

Part IV then argues that the trade secrets privilege is unnecessary in criminal actions because narrow criminal discovery statutes and subpoena procedures already tightly restrict defendants' access to immaterial information. And when non-frivolous defense requests for information create a credible risk of harm, alternate remedies are available without barring access altogether. Finally, Part V addresses the likely counterargument that the privilege is necessary to incentivize innovation in

---

on file with author) (arguing to apply the *Daubert* test to proprietary technologies used in sentencing).

[8] *See* Fed. R. Evidence 1101 (applying privileges to all judicial proceedings).

new criminal justice technologies. I consider the underlying theoretical rationales for both trade secrets and evidentiary privileges and conclude that neither justify withholding trade secrets evidence from the accused. The Article then concludes with thoughts about how the trade secrets inquiry sheds new light on how evidence rules do, and should, function differently in civil and criminal cases.

I. TRADE SECRETS IN THE CRIMINAL JUSTICE SYSTEM

Data-driven, algorithmic computer systems and software programs are being adopted across the criminal justice system, from policing and investigations to forensic evidence to pre-trial detention, sentencing, and parole. The developers of these tools often claim that the details about how they work are trade secrets. This Part provides an overview of some of the trade secret technologies currently in use at different stages of criminal proceedings. It also presents examples of defense challenges to, and court responses to, the lack of transparency in these tools.

Quantifying the number of trade secret privilege claims in criminal cases is difficult for two reasons. First, inadequate documentation and indexing of court records precludes a comprehensive search of pre-trial motion papers from either federal or state courts. For instance, the defense attorney in *Ocasio*, discussed below, provided me with personal copies of the motion papers in which a claim to the trade secrets privilege was litigated. Few of those documents appear on Westlaw. While at least one media outlet covered the case, it never referenced the privilege issue.[9] And *Ocasio* was a federal case; the records of state trial courts—where the vast majority of criminal prosecutions occur—are even more difficult to search. Trial papers are slightly more accessible than pre-trial records, but an overwhelming majority of criminal cases end in plea agreements before trial ever begins.[10] Second, the bulk of would-be trade secret privilege claims in criminal proceedings likely go uncounted because, even in the absence of an express privilege claim, many judges treat discovery demands and subpoenas for alleged trade secrets with unwarranted reserve. When privilege claims are explicit, defendants may fail to challenge them. Either trend would make the effect of the privilege at once more powerful and more opaque.

---

[9] Susan Brenner, The subpoenas, the Motion to Quash and the Source Code, CYB3RCRIM3, June 17, 2013, 7:57 AM.

[10] *See* BUREAU OF JUSTICE STATISTICS, SUMMARY FINDINGS (Ninety-five percent of felony convictions result from plea deals.).

In sum, it is impossible to measure the full scope of problems that secrecy creates because what is missing is unknown. In the criminal justice context, doubt about what is missing is arguably harm unto itself; the very possibility of concealing information about criminal justice technologies behind a veil of trade secrecy may offend trust in the system. In any event, despite these methodological limitations, the fact that there are readily apparent anecdotal examples of conflicts over trade secrets in criminal justice technologies suggests that the problem is substantial.

A. Evidence

The first category of criminal justice technologies in which developers have claimed trade secrets is in evidence of guilt presented at trial. For example, death penalty defendant Martell Chubbs was denied access to the source code for a forensic software program used to convict him because the developer claimed it was a trade secret. The California trial court had ordered the code to be disclosed subject to a protective order, reasoning that without the code, Mr. Chubbs would be denied "a right to confront and cross-examine witnesses."[11] The opinion was not the first of its kind. Just three years earlier, the Ninth Circuit had held that criminal defendants have a right to "background material" on forensic software programs to enable them "to pursue a more effective examination," and that they "should not have to rely solely on the government's word [when] a charge against the defendant is predicated largely on computer software functioning in the manner described by the government, and the government is the only party with access to that software."[12] But in Mr. Chubbs's case, the software developer refused to comply with the trial court's order, arguing that the source code was privileged.[13] The appeals court ruled for the developer and overturned the order, finding that the code was not relevant or necessary to the defense. In doing so, the court applied a heightened standard of relevance based on California's statutory trade secrets privilege that had theretofore only ever been applied in civil disputes, extending those standards for the first time to a criminal case.[14]

At least eight states in the past five years have likewise denied defendants access to source code for probabilistic DNA analysis software

---

[11] People v. Chubbs, 2015 WL 139069 (Jan. 9, 2015), at *4.

[12] United States v. Budziak, 697 F.3d 1105, 1112-13 (2012).

[13] *Chubbs*, 2015 WL 139069 at *4.

[14] *Chubbs*, 2015 WL 139069 at *5 (raising the burden from a mere "showing of good cause—that is specific facts justifying discovery," as determined in Barrett, to the more challenging Bridgestone standard of relevance).

programs because the code was alleged to be a trade secret.[15] These software programs work in complex scenarios—such as with minute or degraded samples of DNA and mixtures of DNA from multiple sources—in which human experts cannot reach reliable results. Analysis of "low copy number" DNA and DNA mixtures is an emerging practice that pushes the boundaries of established DNA science.[16] There is currently no universally accepted statistical method to perform this kind of analysis. As a result, software developers must choose not only how to implement a statistical model through code but also which model of the underlying biological phenomena to use.[17] Competing software programs have been found to produce divergent results from identical test samples.[18] In a recent child homicide case, two software programs reached different conclusions regarding whether defendant Nick Hillary's DNA was included in a crime scene sample.[19]

Given the uncertainties surrounding low copy number and mixed DNA analysis, defendants have been particularly concerned about scrutinizing the code that purports to implement these methods. But probabilistic genotyping is merely one of numerous forensic methods that are, or will soon become, automated through trade secret software programs. The algorithms that generate candidates for latent fingerprint analysis are proprietary.[20] The algorithms used to search ballistic information databases for firearm and cartridge matches are secret and inaccessible to

---

[15] *See* Commonwealth v. Michael Robinson (Pa. 2016); Esau Johnson (NY 2016); People v. Chubbs (Cal. App. Ct. 2015), John Wakefield in NY; Ohio v. Shaw (2014); Commonwealth v. Foley, 38 A.3d 882, 888-90 (Pa. Super. Ct. 2012). *See also*, Note, *The Admissibility of TrueAllele*, 72 WASH. & LEE L. REV. 1033, 1061-70 (2015).

[16] *See* FORENSIC SCIENCE IN CRIMINAL COURTS 82 (Sept. 2016) ("PCAST Report") (finding that manually analyzing complex DNA mixtures "is not foundationally valid").

[17] *See, e.g.*, Paolo Garofano, et. al., *An Alternative Application of the Consensus Method to DNA Typing Interpretation for Low Template-DNA Mixtures*, 5 FORENSIC SCI. INT'L 422 (2015) (explaining that the lack of a "universally-accepted" method "leads experts to differently interpret evidence in the Court applying several statistical approaches").

[18] *Id.*, at 423.

[19] PCAST Report, *supra* note __ at n. 212. As of February 23, 2017, the precise details of this case are not yet clear to me. *See also,* AN ADDENDUM TO THE PCAST REPORT ON FORENSIC SCIENCE IN CRIMINAL COURTS, at 8. Dr. Buckleton, one of the developers of STRmix, observed that, "STRmix included, TrueAllele [was] inconclusive," and commented that there was some uncertainty about the sample tested. Email from Buckleton (on file with Author) (Feb. 23, 2017). While the details of the DNA analysis at issue in *Hillary* are merely marginally relevant to this Article, the case illustrates the possibility of disagreement among experts in the field that may motivate defendants to seek to scrutinize the underlying methodologies of these tools.

[20] PCAST Report, *supra* note__ at 250-51.

independent auditors.[21] Some developers of face recognition technology have refused even to disclose the user manuals for their software programs.[22] And in September 2016, the President's Council of Advisors on Science and Technology recommended automation as one means of "accelerating the development of objective methods" in the forensic sciences in general.[23] Given that trade secrecy is arguably the primary intellectual property protection for source code today,[24] this trend toward automation in forensic science disciplines will surely increase the number of trade secret claims concerning the details of those methodologies.

Whether and when criminal defendants should be able to review the source code for forensic software programs is a matter of live debate among courts, scholars, and practitioners alike.[25] Some scientists and technologists contend that failure to disclose source code used in scientific research violates the "detailed publication and disclosure of information necessary to satisfy peer review, experimental reproduction, and the ability to build upon another's work."[26] Attorneys Jessica Goldthwaite, Clinton Hughes, and Richard Torres of The Legal Aid Society argue that the Confrontation Clause requires access to source code in forensic technologies.[27] Some legal scholarship has also detailed some of the scenarios in which access to source code could be relevant to determine a forensic software program's accuracy and reliability, as well as to maintain rights of cross-examination and due process.[28] I have also previously argued that defendants should be granted access to source

---

[21] *Id.*, at 133.

[22] GEORGETOWN LAW CENTER ON PRIVACY & TECHNOLOGY, THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA (Oct. 18, 2016)

[23] PCAST Report, *supra* note__ at 125.

[24] *See, e.g.*, Derek Handova, *The Business of IP: Choosing Between Patents and Trade Secrets*, IP Watchdog (May 25, 2016).

[25] *See, e.g.*, Matt Tusing, *Machine-Generated Evidence: Preserving an Appealable Issue*, 43 No. 1 THE REPORTER 13 (2016) (describing cases where courts have ordered review of the source code in forensic devices).

[26] *See*, Darrel C. Ince, et. al., *The case for open Computer Programs*, 482 NATURE 485 (2012) ("[A]nything less than the release of source programs is intolerable for results that depend on computation."); Erin E. Kenneally, *Gatekeeping out of the box: Open Source Software as a Mechanism to Assess Reliability for Digital Evidence*, 6 VA. J. L. & TECH. 13 (2001); Brian Carrier, *Open Source Digital Forensics Tools: The Legal Argument*, STAKE INC. (2002).

[27] Jessica Goldthwaite, Clinton Hughes, & Richard Torres, *Mixing it Up: Legal Challenges to Probabilistic Genotyping Programs for DNA Mixture Analysis*, THE CHAMPION (forthcoming 2017).

[28] , *Computer Source Code*, *supra* note __; Roth, *Machine Testimony*, *supra* note __; Chessman, *A 'Source' of Error*, *supra* note __.

code.[29]

Other technologists and legal scholars, including Edward Felten, Joel Reidenberg, and David Robinson among others, maintain that source code review is often unnecessary because alternate methods are available to evaluate software programs.[30] Writing about an earlier wave of litigation concerning the disclosure of source code in breath test devices, Jennifer Mnookin argued that courts determining the admissibility of scientific evidence should prioritize validation studies over scrutinizing the inner workings of "black-box" methods.[31]

However, criminal defendants' unique procedural rights should set the terms of the source code disclosure debate well beyond the issue of best practices from a purely scientific or technological perspective. Scientific or industry consensus about necessary and sufficient methods for software quality assurance—if and where such consensus exists—does have a role in determining the admissibility of expert evidence under *Daubert* or *Frye*. But once that evidence is admitted, defendants' rights to scrutinize and cross-examine it have merely begun. This distinction is well founded; the incentives that shape the production of scientific consensus differ from the risks and obligations of criminal cases.[32] If the scientific method marked the limit of criminal procedure, the justice system would not be necessary. When evidence is sought for confrontation, a scientific view of relevance should be a floor not a ceiling.

This Article enters the debate orthogonally, in the sense that it is most concerned not with the substance of the information itself but rather with the legal burden that defendants must meet in order to succeed in a discovery or subpoena motion. Some courts have denied defendants access to source code in forensic technologies because they have deemed that code to be irrelevant. Other courts have denied defendants the same because they have deemed the code to be privileged. The arguments in this Article do not apply to evidence that is *certain* to be irrelevant; privileging evidence we know to be irrelevant can do little harm. But when evidence *might* be relevant, the precise ex ante burden that defendants must meet in

---

[29] Rebecca Wexler, *Convicted by Code*, Slate (Oct. 2015).

[30] Joshua A. Kroll, et. al., *Accountable Algorithms*, 165 U. PENN. L. REV. __, 6 (forthcoming 2017).

[31] Mnookin, *supra* note __.

[32] Thank you to Jack Balkin for bringing to my attention the differences in institutional incentives for the production of scientific knowledge and criminal case outcomes.

order to compel disclosure via discovery or subpoena can matter a great deal. This burden is my central concern. If courts shrink the relevance standard by pegging it blindly to the scientific method, the burden to show relevance will be too high. The trade secrets privilege raises that burden further still. Intellectual property should not receive such special treatment.

B. Pre-trial Detention, Sentencing, and Parole

A second group of criminal justice technologies in which developers have claimed trade secrets is in actuarial risk assessment instruments used to predict an individual's likelihood of recidivism. Decision-makers use these tools to guide decisions about whether or not to set bail pre-trial, what sentence to impose, and whether to grant parole. For example, defendant Eric Loomis was denied access to information about a predictive computer system used to sentence him to six years in prison because the developer considered it a trade secret. The system, called COMPAS, is an actuarial risk assessment instrument that purports to predict the likelihood that someone will commit a future crime. Mr. Loomis suspected that the tool used his sex as a factor in assessing his risk, and sought to bring equal protection and due process challenges.[33] But the developer refused to disclose information about how the system weights input variables and how it calculates a final risk score from those inputs.[34] The Wisconsin Supreme Court acknowledged that the trade secrets barriers prevented both the parties and the court from determining precisely how the system accounts for sex, but found that the equal protection claim was unpreserved.[35] The court also found that the due process challenge failed because, among other reasons, the judge and Mr. Loomis had equally limited access to the trade secret information.[36] The opinion never

---

[33] Wisconsin v. Loomis, 371 Wis.2d 235, 252, 259, 268 (Wisc. 2016) (considering "whether the use of a COMPAS risk assessment at sentencing 'violates a defendant's right to due process . . . because the proprietary nature of COMPAS prevents defendants from challenging the COMPAS assessment's scientific validity.").

[34] *Loomis*, at 258.

[35] *Loomis*, at 267 ("Due to the proprietary nature of COMPAS, the parties dispute the specific method by which COMPAS considers gender."). The government argued that the system merely uses gender for "statistical norming," whereby an individual's score is scaled by comparing it to those of others in a pre-selected group, and thus that no equal protection issue occurred. *Id.*, at 268; *See also,* Klingele, *The Promises and Perils of Evidence—Based Corrections*, 91 NOTRE DAME L. REV. at 576.

[36] *Loomis*, at 244 ("[T]his is not a situation in which portions of a PSI are considered by the circuit court, but not released to the defendant. The circuit court and Loomis had access to the same copy of the risk assessment.").

mentioned the fact that the judge and defendant's incentives to scrutinize the system differ, or even that only one could choose whether to use the system while blind to its methodology.

Risk assessment instruments used in sentencing, parole, and pre-trial bail and detention determinations are among the most widely reported and controversial trade secret technologies entering the criminal justice system.[37] Advocates claim that these systems can reduce mass incarceration without endangering public safety by identifying low risk individuals for release. Automation may also help to correct for human bias in judicial decision-making. Yet critics argue that the tools may reinstate past biases, in part because they rely on biased historical data to make future predictions.[38] Concerns have also arisen from the fact that many developers refuse to disclose the training data, algorithms, and final models that comprise these systems. Legal scholar Jessica Eaglin has detailed how numerous institutional incentives discourage both private and public developers from sharing information about "the design, development, and evaluation of privately-created risk assessment tools used in the criminal justice system."[39] Private commercial vendors, non-profit foundations, and government agencies have all developed risk assessment instruments.[40] Even non-commercial entities have refused fully to disclose information about how the tools are built.[41]

As with source code disclosure, the extent of transparency that should be required in the training data, methodology and construction of risk assessment systems is a matter of live debate.[42] Some policymakers and

---

[37] *See, e.g.*, Sonja B. Starr, *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, 66 STAN. L. REV. 803 (2014). *See also*, ProPublica *Machine Bias*; Washington Post response.

[38] Training a machine learning algorithm on past policing policies that disproportionately targeted certain populations, such as New York City's Stop & Frisk policing program, may cause the tool artificially to predict a higher likelihood of re-arrest for those populations. A ProPublica audit of one commercial tool found that the algorithm erroneously categorized Black defendants as high risk twice as many times as white defendants. *See, e.g.*, Jeff Larson et al., *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA (May 23, 2016).

[39] Eaglin, *Constructing Recidivism*, *supra* note __at 41-43, 50-55.

[40] *See, e.g.*, Northpointe, Inc.; The Arnold Foundation; The New York City Criminal Justice Agency.

[41] *See, e.g.*, New York's CJA tool and forthcoming analysis by HRDAG.

[42] *See, e.g.*, Ric Simmons, *Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in our Criminal Justice System*, 2016 MICH. ST. L. REV. 947, 994-98 (discussing transparency requirements for algorithms and data sets used in risk assessment instruments); Katherine Freeman, *Algorithmic Injustice: How the Wisconsin*

scholars argue that independent audits that rely on "black-box" validation testing should suffice.[43] Others point out that this method of testing has limits.[44] One limit of black-box testing is the volume and scope of test data required to evaluate how the tool will perform in unforeseen circumstances. More specific to risk assessment instruments, systemic racial bias in historical criminal justice data may wrongfully appear to validate present racial bias in these tools.[45] Testing against historical data also necessarily omits counterfactual outcomes, such as how an individual who was ranked high risk and incarcerated would have behaved had they been released. And it is impossible to test these systems during and post deployment because the ranking individuals receive may affect their future outcome. A high-risk ranking, for instance, might extend an experience of incarceration, making a successful re-entry into the community more difficult and increasing the likelihood of future criminal activities. A series of high-risk rankings across a community could focus disparate policing and surveillance practices on that community, thereby increasing the chance that individuals ranked high-risk within the community will be re-arrested.[46] Put simply, risk assessment instruments can create feedback loops that produce the results they predict.[47] Black-box validation studies may be ill suited to identify these types of pathologies.[48]

Once again, this Article enters the debate orthogonally. My interest

---

Supreme Court Failed to Protect Due Process Rights in State v. Loomis, 18 N.C.J.L. & Tech. On. 75 (2016).

[43] *See, e.g.*, Eaglin, *Constructing Recidivism*, *supra* note__at 11 (describing policymakers' reliance on validation studies in adopting risk assessment instruments).

[44] *See, e.g.*, Kate Crawford; Solon Barocas & Andrew D. Selbst, *supra* note__.

[45] Eaglin, *Constructing Recidivism*, *supra* note __ at 41 ("Unfortunately, there is no 'good data' to use that would resolve disparities in the justice system.").

[46] *See* Laurel Eckhouse, *Big Data may be Reinforcing Racial Bias in the Criminal Justice System*, WASH. POST (Feb. 10, 2017) ("We need more transparency and better data to learn whether these risk assessments have disparate impacts on defendants of different races."); Patrick Ball, Julie Ciccolini, Cynthia Conti-Cook, Laurel Eckhouse, Kristian Lum, & Joshua Norkin, *Beyond 'Minority Report': Computer Models, Crime Data, and Dangerous Assumptions*, (working paper on file with author) (forthcoming 2017).

[47] *See, e.g.*, Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Cal. L. Rev. 671 (2016) (explaining how big data mining can entrench past biases); CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION (2016).

[48] *See*, Michael Mattioli, *Disclosing Big Data*, 99 MINN. L. REV. 535 (2014). *See also*, Simson Garfinkel, et. al., *Bringing Science to Digital Forensics with Standardized Forensic Corpora*, 6 DIGITAL INVESTIGATIONS S2 (2009) ("[M]uch of today's digital forensic research results are not reproducible. For example, techniques developed and tested by one set of researchers cannot be validated by others since the different research groups use different data sets to test and evaluate their techniques.").

lies in evaluating whether and how new criminal justice technologies impede modes of argument that were previously available to the defense. To be sure, even with trade secrets and other barriers to transparency, defendants can contest the quality of information that goes into an algorithmic system,[49] and use facts not included in the assessment to argue against the risk scores that come out.[50] But barriers to transparency in these tools obstruct other kinds of arguments that defendants are uniquely positioned and entitled to make. For example, without knowledge of the tool's weights and method of calculating input factors, it is impossible to evaluate the significance of an input error.

The New York State COMPAS-Probation risk and needs assessment tool (a parallel product to that at issue in *Loomis*) is currently used by fifty-seven New York state probation departments in probation, pretrial release, and sanction determinations. A COMPAS supervision tool was also implemented in New York in 2012.[51] To generate a final risk score, COMPAS relies on manual inputs from surveys that the subject of the assessment and another human evaluator both fill out. At least three New York inmates denied parole have shown in grievance challenges that the person who implemented their evaluations inputted a "yes" where they should have used a "no" in response to a question about disciplinary issues. When one inmate received a re-assessment to correct that single error, his final risk score dropped a full category. Happenstance comparison of these cases has given a miniscule amount of insight into how the system weights and calculates one input factor. But more generally, the developer's trade secrets prevent individuals who seek to challenge their COMPAS assessments from knowing whether any other erroneous input has altered their score, and by how much.[52]

---

[49] *Loomis*, at 260 ("Thus, to the extent that Loomis's risk assessment is based upon his answers to questions and publicly available data about his criminal history, Loomis had the opportunity to verify that the questions and answers listed on the COMPAS report were accurate.").

[50] *Id.* ("Loomis had an opportunity to challenge his risk scores by arguing that other factors or information demonstrate their inaccuracy.").

[51] *New York State COMPAS-Probation Risk and Needs Assessment Study* 1 (2012). Jennifer Parish of the Urban Justice Center previous attempt to FOIL information about NYS COMPAS in 2014. Her request for instruction manuals, training guides and information regarding scoring for the COMPAS Reentry Assessment tool was rejected pursuant to the trade secrets exemption under FOIL because "these materials are the sole property of Northepointe." This FOIL request was submitted in connection with an Article 78 ruling finding that the COMPAS tool was not adequately tailored for use on individuals with mental illness. *Hawthorne v. Stanford*, No. 0811-14 (May 27, 2014).

[52] Thank you to Cynthia Conti-Cook for informing me of these cases.

As with source code review in forensic-science methods, tackling issues of accuracy or bias in new technologies from a scientific perspective does not adequately account for criminal defendants' rights to contest the evidence against them. The methods to resolve questions in science and in criminal proceedings differ. One should not replace the other.

C. Investigations

In *United States v. Ocasio*, a software program that scans online networks for child pornography flagged three files on defendant Angel Ocasio's computer. But when police obtained a warrant to search his actual computer, the files were not discovered. Ocasio argued that the program violated the Fourth Amendment by scanning private folders on his hard drive, and that its results were insufficiently reliable to support the probable cause needed for a warrant. To develop those claims, he sought information about how the program works, including its source code and documentation, operation manuals, and training materials.[53] The developer of the software program conceded that, "[w]ithout the source code, it is not possible to authenticate the function of the application or validate its 'calibration.'"[54] Nonetheless, the Department of Justice argued that the information was shielded from disclosure by *both* the law enforcement privilege and also by "copyright and trade secret laws."[55] The court in *Ocasio* found "any claim of trade secret privilege to be inappropriate,"[56] and ordered disclosure of the requested materials subject to a protective order.[57] But the fact that the Department of Justice would

---

[53] Motion to Compel Production of Materials Pertaining to Peer-to-Peer Investigative Software, United States v. Angel Ocasio, No. 3:11-cr-02728-KC, ECF 117 (April 8, 2013), at 7.

[54] Aff. William S. Wiltse, United States v. Angel Ocasio, No. 3:11-cr-02728-KC, ECF 118-1 (April 15, 2013), at 4.

[55] Order, United States v. Angel Ocasio, No. 3:11-cr-02728-KC, ECF 139 (May 28, 2013), at 2. The developer also claimed *both* the law enforcement and a trade secrets privilege. Order, United States v. Angel Ocasio, No. 3:11-cr-02728-KC, ECF 150 (June 6, 2013), at 7.

[56] Order, United States v. Angel Ocasio, No. 3:11-cr-02728-KC, ECF 150 (June 6, 2013), at 9; 2013 WL 2458617 at *5.

[57] Order, United States v. Angel Ocasio, No. 3:11-cr-02728-KC, ECF 163 (June 16, 2013), at 2, 8, 11. Similar issues are currently playing out across the country in hundreds of cases in which the FBI deployed a malware tool to circumvent an IP-masking program on defendants' computers, called Tor. *See, e.g.*, Cyrus Farivar, *Feds may let Playpen Child Porn Suspect go to keep Concealing Their Source code*, ARSTECHNICA, Jan. 9, 2017, 4:30PM. At least one federal judge has found that the FBI's software program

even attempt to use trade secrets as a shield illustrates the risk that government agencies may use intellectual propertization as a means to avoid judicial scrutiny.

Other areas where trade secrets may arise in defense challenges to investigative technologies include face recognition and predictive policing.[58] Some police departments have denied open records requests for the user manuals for face recognition systems by citing trade secrets exemptions to their disclosure obligations.[59] User manuals can reveal information relevant to criminal defendants' challenges to the legality of an investigative method under the Fourth Amendment, such as whether the system generates a set number of face 'matches' or delivers fewer when it has greater confidence in each, and whether the system was calibrated for certain racial groups and not others.[60] Many predictive policing systems are similarly opaque. Like risk assessment instruments, these are data-driven algorithmic systems that rely on historical data to model the likelihood of future crimes.[61] Transparency around the algorithms themselves can facilitate independent review. For instance, when a leading

---

violated the Fourth Amendment because it works by placing code onto a defendant's computer without permission. Order Denying Motion to Suppress, United States v. Torres, 5:16-cr-oo285-DAE, ECF 33 (Sept. 9, 2016), at 9.

[58] *See, e.g.*, Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, __ N.Y.U. L. Rev. Online __ (forthcoming 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2924620.

[59] *See* PERPETUAL LINE-UP, *supra* note__. The Center on Privacy & Technology and Georgetown Law Center requested both user manuals and technical specifications from the developers of the tools, and also the policies, procedures, and training materials related to law enforcement agencies' use of such software. Police departments in Nebraska and Delaware cited trade secrets exemptions as a reason to deny these requests. Letter to Clare Garvie, Center on Privacy & Technology, from Lincoln Police Department (Jan. 22, 2016) (denying open records request and citing Nebraska Revised Statute 84-712.05(3) exemption for trade secrets); Letter to Clare Garvie, Center on Privacy & Technology, from Col. Nathaniel McQueen, Jr., Division of State Police Delaware (Nov. 9, 2016).

The Iowa Department of Public Safety explained in detail that even the user manuals for these software systems are proprietary, contain trade secrets, and include "specific information about the operation of the system, the specific features provided by the technology system, the methods used for auditing, and other information that could disclose key information about the operation of the system." Letter to Clare Garvie, Center on Privacy & Technology, from Rozann M. Ryan, Comm. Dep't of Public Safety, Iowa (Apr. 1, 2016).

[60] Thank you to Alvaro Bedoya for sharing these explanations of why user manuals can reveal critical information about a tool.

[61] PredPol, HunchLab; Chicago heat list; Arnold PSA being retooled for use in policing.

vendor of predictive policing software, PredPol, published its algorithm in a peer-reviewed journal,[62] independent data scientists were able to re-implement the algorithm and to produce the first empirical evidence of how predictive policing systems can exacerbate biases in historical policing data while appearing to justify them.[63] Defendants seeking to challenge the accuracy of these systems,[64] whether police may rely on them to satisfy Fourth Amendment reasonable suspicion for a stop,[65] or whether the tools are systematically biased on the basis of race or other factors,[66] may face trade secrets barriers to developing their claims.[67] In a case currently before the D.C. Circuit, *Stephen Aguiar v. DEA*, a convicted defendant seeks to FOIA a copy of the mapping software that the government used to analyze and visualize GPS location tracking data,[68] the results of which were introduced into evidence at his criminal trial.[69]

---

[62] G.O. Mohler, et. al., *Randomized Controlled Field Trials of Predictive Policing*, 100 J. of American Statistical Ass'n 1399 (2015), http://amstat.tandfonline.com/doi/full/10.1080/01621459.2015.1077710?scroll=top&needAccess=true&.

[63] PredPol has refused to release the training data used to create its algorithm, making it impossible to replicate the research that the company published in a peer-review journal. Without access to the training data, researchers could (and did) speculate that this type of system would produce a feedback loop: because police are likely to find more crimes where they are deployed and fewer where they are not, each day's arrest data will appear to fulfill the models' past predictions and strengthen its future predictions of crime density in targeted areas. Kristian Lum, et. al., *To Predict and Serve*, 13 SIGNIFICANCE 14 (Oct. 2016). Difficulty obtaining data makes this type of study rare.

[64] *See, e.g.*, Nissa Rhee, *Study Casts Doubt on Chicago Police's Secretive 'Heat List'*, CHICAGO MAGAZINE (Aug. 17, 2016).

[65] *Cf.*, Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 Emory L. J. 259 (2012); Andrew Guthrie Ferguson, *Crime Mapping and the Fourth Amendment: Redrawing 'High Crime Areas'*, 63 Hastings L. Rev. (2011).

[66] *See, e.g.*, Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. Pa. L. Rev. 871, 883-86 (2016) (identifying four sources of "mistaken predictions" in machine learning tools).

[67] Some tools currently on the market show that for-profit companies can embrace transparency and remain profitable. One company, Azavea, uses open source algorithms, publishes the variables it uses and the claimed accuracy of each, and has shared its full predictive models with journalists. Maurice Chammah & Mark Hansen, *Policing the Future*, THE MARSHALL PROJECT, Feb. 3, 2016, 7:15AM. Palantir, IBM, Hitachi, Motorola, and Lexis all have less transparent competitor products.

[68] Stephen Aguiar v. Drug Enforcement Administration, 139 F. Supp. 3d 91 (2015) (currently on appeal to D.C. Circuit).

[69] The government introduced maps produced via use of the software into evidence. United States v. Aguiar, 737 F.3d 251, 255 (2013). In motion filings, the software was described as follows: "Proprietary DEA software collects and records the information transmitted by GPS devices, and allows case agents to then monitor and analyze the information." 2012 WL 3150932, at *7. The Second Circuit's opinion described the software as follows: "The DEA developed software that allows agents to save, track and

To date, Mr. Aguiar has not been successful at compelling disclosure of the software program under FOIA.

Secrecy around law enforcement methods for investigating crime is not new.[70] Sometimes, as with algorithms used to flag IRS filings for audits, the effectiveness of an investigative tool depends on concealing information about how it works.[71] Nor is excessive secrecy around investigative methods new. For one recent example among many, the FBI required police departments across the country to sign nondisclosure agreements promising to conceal information about "Stingrays," an invasive cellphone tracking tool, including how the devices work and even the mere fact of their use. Police were to hide this information from both defendants and the courts.[72] Some judges have since found that the warrantless use of Stingrays violates the Fourth Amendment.[73] Secrecy around these devices enabled police—for nearly a decade and as a matter of course—to perform what some courts deem unconstitutional searches while evading judicial review.[74]

Trade secrets claims in investigative technologies add yet another layer of concealment to criminal proceedings. Police may evade proper scrutiny by outsourcing their investigative techniques to private companies. These companies can claim that they are not agents of the state, and thus that they are free from Fourth Amendment and other constitutional

---

analyze the data generated by the GPS device." 737 F.3d, at 255. As of February 2017, the DEA has refused to share the software program with Mr. Aguiar, or even to provide him with a map visualizing the GPS data it collected on his location. *See* oral argument, D.C. Circuit, Feb. 2017.

[70] The need to keep certain methods secret from the general public is reflected in The Freedom of Information Act exemption for law enforcement records that "would disclose techniques and procedures for law enforcement investigations . . . if such disclosure could reasonably be expected to risk circumvention of the law." The Freedom of Information Act, 5 U.S.C. 552(7E).

[71] *See, e.g.*, Kroll, et. al., *supra* note__ ("The process for deciding which tax returns to audit, or whom to pull aside for secondary screening at the airport, may need to be partly opaque to prevent tax cheats or terrorists from gaming the system.").

[72] *See, e.g.*, Jessica Glenza, *Stingray Spying: FBI's Secret deal with Police Hides Phone Dragnet from Courts*, THE GUARDIAN (Apr. 10, 2015); Kim Zetter, *Emails show feds Asking Florida cops to Deceive Judges*, WIRED MAGAZINE (June 19, 2014).

[73] *See* United States v. Lambis, 1:15-cr-00734-WHP (July 12, 2016) ("Absent a search warrant, the government may not turn a citizen's cellphone into a tracking device.").

[74] The NYPD recently disclosed that its standard operating procedure since 2008 has been to seek a court order for a pen register, which is a different type of technology, and then use a Stingray instead. *NYPD Has Used Stingrays More Than 1,000 Times Since 2008*, NYCLU (Feb. 11, 2016).

restrictions, beyond the reach of discovery statutes, and exempt from *Brady* disclosure obligations.[75] If the information at stake might reveal not how to circumvent an investigative method but rather whether that method is sufficiently accurate and reliable to establish probable cause; whether it unreasonably intrudes on privacy; or whether it unfairly targets particular racial groups, police may have incentives to avoid possessing, controlling, or even closely evaluating the relevant information themselves. Arguing that the information is a trade secret and not theirs to disclose presents a convenient solution.

II. A CRIMINAL TRADE SECRETS PRIVILEGE IS HARMFUL

Today, it is widely accepted by legislators, judges, and scholars alike that a trade secrets evidentiary privilege both does and should exist. Two-thirds of the states have codified the privilege in their evidence rules.[76] Courts in most of the remaining jurisdictions recognize some common law variation of it.[77] A few scholars have taken a measured, even critical, approach. Kenneth Graham, Jr. calls the privilege "controversial,"[78] arguing that trade secrets protection used to be afforded merely as an equitable manner by courts, and that this protection only recently achieved privilege status.[79] But the clear majority of existing literature treats the privilege as self-evident. Some commentators have also claimed that the privilege should apply to criminal as well as civil cases. The most overt

---

[75] *But see*, United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016) (A private, non-profit organization that investigates cybercrimes either qualified as a government entity or acted as a government agent.).

[76] *See* Kenneth W. Graham, Jr., *Statutory History*, *in* Wright & Miller, 26 FED. PRAC. & PROC. EVID. § 5641, n.25 (2017) (detailing the status of the trade secrets privilege in various jurisdictions and finding that status uncertain for: Arizona, Colorado, Idaho, Iowa, Louisiana, Michigan, Minnesota, Mississippi, Montana, North Carolina, Ohio, Oregon, Rhode Island, Tennessee, Vermont, Washington, West Virginia, Wyoming, Military Law).

[77] Imwinkelried claims that "[e]very American jurisdiction recognizes an evidentiary privilege protecting trade secrets." Imwinkelried, *Computer Source Code*, *supra* note__at 13. *See also*, Edward Imwinkelried, *The New Wigmore*, Evidentiary Privileges § 9.2.1. Graham gives a competing assessment, noting that at least some federal courts have "stated that there is no federal trade secrets privilege," and contending that, "[w]ith the notable exception of New York, most of the states have no case law recognizing the privilege." Graham, *supra* note__ at §§ 5641-42, n.25.

[78] Graham, *supra* note__ at § 5642, n.258.

[79] Graham, *supra* note__ at § 5642 ("The Restatement, the writers, and the courts all seem to have thought that there was no privilege for trade secrets, but only an equitable procedure to protect against disclosure. . . . What led the Advisory Committee and the state drafters to follow Wigmore and create a "limited trade secrets privilege?").

endorsement to date has come from Edward Imwinkelried, who sanctioned the privilege for both criminal and civil proceedings by maintaining that private companies that develop forensic software programs for use in criminal trials "have a perfect right to assert the evidentiary privilege for their trade secrets."[80]

I challenge the common consensus in favor of the trade secrets privilege by arguing that none should exist in criminal proceedings.[81] As a backdrop to this argument, this Part describes the rules governing the trade secrets privilege and explains why each rule is harmful to apply in criminal proceedings. In brief, courts first consider whether the alleged trade secret is valid and whether ordering its disclosure would cause harm. Next, they assess whether the information is relevant and necessary to the case. Finally, they weigh the risk of harm from disclosure against the need for the information. Applying the rules governing the trade secrets privilege wholesale from civil to criminal proceedings will almost certainly lead to systemic over-claiming and wrongful exclusion of relevant evidence; place an unreasonable burden on criminal defendants; and undermine the legitimacy of criminal proceedings by privileging intellectual property interests over those of due process.

A. Over-claiming and Abuse

To invoke the privilege, one must first establish that a valid trade secret exists. In civil suits that process can be difficult and risky, which deters borderline and fraudulent claims to the privilege.[82] For instance, whether a secret actually qualifies under a state's substantive intellectual property law is a frequent focus of litigation in trade secret misappropriation lawsuits.[83] Plaintiffs must disclose details about their

---

[80] Imwinkelried, *Computer Source Code*, *supra* note__ at 25.

[81] The sole prior reference in the scholarly literature that I have found agreeing with my claim concerns trade secrets protections in Japanese courts. Masashi Chusho, *Protection of Trade Secrets in Lawsuit Procedures in Japan*, 48 LES NOUVELLES 193, 195 (2013) ("In criminal procedures, there is a great need to avoid wrongful convictions and guarantee due process. Therefore, unlike in civil procedures, trade secret privilege is not allowed and a witness may not refuse to give testimony on the grounds that it concerns a trade secret."). Chusho also notes that the Unfair Competition Prevention Act of 2011 added new protections against trade secret disclosure in criminal cases. *Id.*

[82] The initial burden to establish the validity of an alleged trade secret is technically "minimal," but the issue is often the focus of a challenge. Ferolito v. Arizona Beverages, 990 N.Y.S.2d 218, 220 (N.Y. App. Div. 2014).

[83] This is not an easy question. Courts have not settled on precisely what substantive definition of a trade secret should apply to invocations of the privilege. Some judges have

secrets with sufficient particularity for defendants to learn the charges and develop a response.[84] Those disclosures are most risky when the parties are direct business competitors. But even when they are not, there is always the risk that the opposing party will disprove the validity of an alleged trade secret and eviscerate its value.

Those constraints are missing in criminal cases. It is easier and safer to assert the privilege in a criminal case because fewer defendants are likely equipped with the resources to challenge the legitimacy of a trade secret.[85] Because alleged trade-secrets holders can reasonably anticipate that their assertions of privilege will go unchallenged, they will be more likely to over-claim protections where no valid trade secret exists. The rules that govern the trade secrets privilege in civil cases are thus inadequate to protect against borderline or even knowingly false assertions of the privilege in criminal proceedings. The burden on the party claiming the privilege to show the validity of their trade secret is too weak.

---

construed the privilege to cover more than the private law definition of a trade secret, reasoning that the privilege should extend to all "confidential research, development, or commercial information" protected from discovery by Federal Civil Procedure Rule 26(c)(G). Graham, *supra* note__ at § 5644 (noting that the court in Wearly v. F.T.C., 616 F.2d 662 engaged in "doctrinal slide" by "expanding "trade secrets" into broader category of "proprietary information", then converting "proprietary" into "property" so that disclosure constitutes a "taking" which must be compensated for under the Fifth Amendment."). In contrast, Graham suggests that a narrower definition of a trade secret should apply to the privilege than applies in private law because of "the judicial need for evidence." Graham, *supra* note__, at § 5644. Graham also points out that some jurisdictions cabin the scope of criminal liability by applying narrower definitions of a trade secret in criminal prosecutions for trade secrets theft than in civil suits for misappropriation. I contend that extending any of this reasoning to criminal cases is theoretically unsound because it derived ultimately from Rule 26(c)(G), which has no direct corollary in criminal procedure. None of the select exemptions in Federal Criminal Procedure Rule 16, which governs discovery between the government and the defense, nor any of the advisory committee notes discussing Rule 16, mention confidential commercial information.

[84] *See, e.g.*, Nilssen v. Motorola, 963 F. Supp. 664 (N.D. Ill. 1997) ("It is not enough to point to broad areas of technology and assert that something there must have been secret and misappropriated. The plaintiff must show concrete secrets.") *cited in*, ELIZABETH A. ROWE & SHARON K. SANDEEN, CASES AND MATERIALS ON TRADE SECRET LAW 396-406 (2012). *See, also*, CA Civ. P. § 2019.210 (Plaintiffs must disclose information about their alleged trade secret "with reasonable particularity."). In camera disclosure is generally not sufficient in this context because the defendant often seeks to challenge the validity of the trade secret as an element of their defense.

[85] A growing consensus among expert commentators has identified a need for earlier disclosure of expert evidence in criminal trials to assist in evaluating and challenging it. *See* Giannelli, NATIONAL DISCOVERY REFORM COMM.

Examples of blatant over-claiming already exist. New York City's Office of the Chief Medical Examiner (OCME) has argued, repeatedly and successfully, that the source code for a forensic software program developed in house using taxpayer funds should be protected from subpoena by criminal defendants.[86] In one case, OCME asserted that the code "is a copyrighted and proprietary asset belonging exclusively to the City of New York."[87] In another, it acknowledged that the code would be useful to the defense, but withheld it anyway in order to preserve the City's "ownership interest in the . . . program."[88] The court ruled for OCME, neglecting even to consider whether a city agency is entitled to own a trade secret at all under New York's substantive trade secrets law,

---

[86] The program at issue in the OCME cases, called FST, is also a probabilistic DNA profile analysis software. FST has generated some controversy. After a two year *Frye* hearing, one New York trial judge concluded that the program's underlying methodology is "not generally accepted" in the scientific community. People v. Collins, 15 N.Y.S. 3d 564, 582 (N.Y. Sup. Ct. 2015). The court also acknowledged a "general objection" to "the fact that FST software is not open to the public, or to defense counsel [and] cannot be used by defense experts with theories of the case different from the prosecution's." *Collins*, 15 N.Y.S. 3d at 580. Other New York courts have declined to follow this holding. *See, e.g.*, Nick Hillary, NY Times article.

[87] People v. Johnson, Notice of Motion to Quash, No. 502/2014, N.Y. Sup. Ct. Bronx County Criminal Term Part 79 (Feb. 10, 2016), at 8. The OCME also suggested that the defendant's Legal Aid attorneys sought access merely "to further develop a competing FST program." People v. Johnson, Letter to Justice Clancey re: Notice of Judicial Subpoena Duces Tecum from Rebecca Johannesen, Office of Chief Medical Examiner, No. 502/2014, N.Y. Sup. Ct. Bronx County Criminal Term Part 79 (Dec. 17, 2015), at 2.

[88] People v. Esau Johnson, No. 3600/2015, N.Y. Sup. Ct. King's Ct'y Part TAP (Sept. 29, 2016) (letter from Rebecca L. Johannesen to Justice Gubbary) (noting "the value of the source code for unlocking deficiencies in [the defendant's attempt] to replicate FST"). Despite OCME's failure to specify the basis for this asserted 'proprietary' or 'ownership' interest, it must be a trade secrets claim; the only alternatives—copyrights and patents—would both limit any risk from disclosure because they protect intellectual property rights in information even after it has been publically disclosed. *See, e.g.,* Copyright Act of 1976, 17 U.S.C. § 106 (2012) (protecting a copyright holder's right to control information after it has been published). The court found that, "where the materials sought are privileged or confidential, as they are here, given New York City's copyright and proprietary interest in the FST software," *the defense must meet a higher burden* to obtain disclosure. People v. Johnson, Decision on the OCME's Motion to Quash a Subpoena, No. 502/2014, N.Y. Sup. Ct. Bronx County Criminal Term Part 79 (Apr. 21, 2016), at 2-3 (*emphasis added*). That is, the OCME's "proprietary" claim raised the defendant's threshold burden beyond a showing of mere relevance and materiality. People v. Johnson, Decision on the OCME's Motion to Quash a Subpoena, No. 502/2014, N.Y. Sup. Ct. Bronx County Criminal Term Part 79 (Apr. 21, 2016), at 2-3 ("[T]he defense must make a showing that the materials are not just relevant and material, but are reasonably likely to contain information that is exculpatory.").

or whether that particular code would qualify.[89]

It is also likely that at least some of Northpointe's trade secrets claims in the COMPAS risk assessment instrument are baseless. Lauren Kirchner of ProPublica successfully FOIL-ed New York State's contract with Northpointe, which provides that New York owns all data contained within the COMPAS system and also prohibits Northpointe from reselling back to New York any derivative products developed from "any idea, method or other product" provided to Northpointe by the State.[90] Given these limitations, it is plausible that the details of how Northpointe weights input factors for New York in particular—the company customizes the weights for each jurisdiction—do not provide a sufficient economic advantage to qualify as a valid trade secret in the New York state.

Over-claiming and abuse, I contend, can surely be expected if courts and legislatures recognize a trade secrets privilege in criminal cases.

B. Burdens and Exclusions

To challenge the privilege, a party must show that the information is

---

[89] *But cf.* In contrast, in civil cases in New York, the party seeking to claim the trade secrets privilege bears "a minimal initial burden of demonstrating the existence of a trade secret." *See Felito*, at 644. The burden then shifts to the party seeking disclosure to "show that the information demanded appears to be 'indispensable to the ascertainment of truth and cannot be acquired in any other way.'" Deas v. Carson Products Co., 172 A.D.2d 795, 796 (1991). Finally, the court is required to apply a balancing test weighing the need for confidentiality against the need for disclosure. New York law recognizes trade secrets protection for information "which one uses in his business and which gives him an opportunity to obtain an advantage over competitors who do not know or use it." *See*, Ashland Management v. Janien, 82 N.Y.2d 395, 407 (1993) (quoting Section 757 of the Restatement of Torts). The OCME made no showing that it had a legitimate business use for the FST source code and software, or any competitors whom it should seek to gain an advantage over. Nor did the OCME establish that the contents of the FST source code are in fact secret, rather than compilations of code from the public domain, or that the OCME took sufficient protective measures to claim trade secrets status. Moreover, the trade secrets privilege doctrine generally requires courts to examine whether compelled disclosure during litigation—subject to any protective orders the court might impose—would produce a substantial risk of harm. The City did claim that "no NDA can adequately protect [the city's] interest in its proprietary source code once it is disclosed . . . ." People v. Johnson, Notice of Motion to Quash, No. 00502-2014, N.Y. Sup. Ct. Bronx County Criminal Term Part 79 (Feb. 10, 2016), at 9. But the *Johnson* court did not undertake that evaluation. *Id.*

[90] Reservation of Intellectual Property and Other Rights and Restrictions, New York State Division of Criminal Justice Services and Northpointe, Inc. Agreement (Oct. 24, 2009), at 13.

both relevant and necessary to their case. Some courts treat this showing of relevance as a duplicate of the liberal discovery standards from civil procedure.[91] But others apply a more stringent test. For instance, the Texas Supreme Court has asserted that, "a requesting party must establish *more* than mere relevance to discover trade secrets, or the statutory privilege would be 'meaningless'" (emphasis added).[92] The test for necessity in turn requires showing that the information is needed to prove or rebut a theory at trial,[93] that denial would cause a specific injury;[94] and that the information cannot be obtained from any alternate source.[95]

One problem with applying these rules wholesale to criminal proceedings is that the procedural backdrop on which they operate differs dramatically from civil disputes. Criminal discovery and subpoena regimes are miserly compared to their civil counterparts. For example, parties have less of an obligation to disclose the facts, data, and full reports that form the bases of expert opinion testimony in criminal as compared to civil proceedings.[96] Criminal defendants already face a more

---

[91] It has been described by some treatise authors as "reasonably related to the underlying cause of action . . . [or] reasonably calculated to lead to the discovery of admissible evidence." 1 Trade Secrets Law § 5:33. *See also*, Coca-Cola Bottling v. Coca-Cola Co., 107 F.R.D. 288, 293 (D. Del. 1985).

[92] In re Continental General Tire, 979 S.W.2d 609, 611 (TX 1998) (quoting the California appellate court in *Bridegstone*).

[93] *Coca-Cola Bottling*, 107 F.R.D., at 293.

[94] 1 Trade Secrets Law § 5:33. Statutes codifying the privilege generally include exceptions to ensure that "allowance of the privilege will not tend to conceal fraud or otherwise work injustice." *See, e.g.*, Tex. R. Evid. 507.

[95] *See, e.g.*, In re Continental General Tire, 979 S.W. 2d 609 (TX 1998) ("[T]he party seeking to discover a trade secret must make a prima facie, particularized showing that the information sought is relevant and necessary to the proof of, or defense against, a material element of one or more causes of action presented in the case, and that it is reasonable to conclude that the information sought is essential to a fair resolution of the lawsuit."). 1 Trade Secrets Law § 5:33. One might assume that the showing of necessity would be more burdensome than the test for relevance, making the relevance inquiry largely superfluous. However, some courts merge the two evaluations; they either treat relevance as a step in determining necessity or find that need follows automatically from relevance. According to one federal district court in Delaware, "in most disputes over the discoverability of trade secrets . . . the necessity of the discovery of the complete [secret] follows logically from the determination that the [secret is] relevant." *Coca-Cola Bottling*, 107 F.R.D., at 297-98.

[96] Parties in civil suits generally have a pretrial right to depose expert witnesses, and to discover the facts, data and full reports that form the basis of their expert opinions. Fed. R. Civ. P. 26. But the government can often satisfy its parallel criminal discovery obligations by disclosing unsupported and conclusory reports, such as those that merely summarize test results without providing information about the test itself, while the majority of states do not authorize depositions in criminal litigation at all. *See, e.g.*,

challenging burden to obtain information. When the trade secrets privilege ratchets that burden above the baseline procedural default, it is more onerous for criminal defendants than for civil parties. Imposing an unreasonably high burden on criminal defendants in turn exacerbates the risk of wrongfully excluding evidence and threatens the integrity of the truth-seeking process.[97] If evidence is relevant to a criminal investigation, it should be disclosed subject to any protective orders necessary to mitigate risk of harm. The relevance standard should be consistent throughout the criminal process.

The concept of "necessity" also translates poorly from civil to criminal proceedings. Courts often define "need" in this context to mean a total absence of alternative sources. On close inspection, this definition is illogical as applied to trade secrets. In order to qualify as a valid trade secret, information must not be generally known or readily ascertainable. Put differently, as soon as a trade secret has been determined valid, the absence of any alternative sources should follow automatically. It is thus likely that courts intend the test to apply not to alternative sources for accessing the precise trade secret information at issue, but rather to alternative methods of proving a claim. Put this way, the test begins to veer towards a selection of arguments. In a criminal case, whether a defendant does or does not "need" to make a particular argument is the defendant's and only the defendant's prerogative to decide. The Sixth Amendment guarantees a right to present a defense. Defendants should be able to choose what arguments to make without obstruction from third party concerns.

C. Balancing Procedural Justice

Finally, courts weigh the seeking party's need for the information against the likely harm from disclosure subject to a protective order.[98] The disclosure in question is not to the public but rather disclosure in the

---

United States v. Mehta, 236 F. Supp. 2d 150, 155 (D. Mass. 2002) ("While Fed. R. Civ. P. 26(a)(2) requires a 'complete statement' of the expert's opinion, the criminal rule requires only a 'summary of testimony.'"), *quoted in* ROBERT M. CARY, CRAIG D. SINGER, & SIMON A. LATCOVICH, FEDERAL CRIMINAL DISCOVERY 123 (2011). *See also*, United States v. Bentley, 875 F.2d 1114, 1123 (5th Cir. 1989) (dissenting opinion) (describing the discovery granted as a report that "summarized the results of an unidentified test conducted by an anonymous technician"). NATIONAL COMM'N ON FORENSIC SCI., PRETRIAL DISCOVERY, *supra* note__, at 6.

[97] Centurion Indus., Inc. v. Warren Steurer & Associates, 665 F.2d 323, 325 (10th Cir. 1981).

[98] 1 Trade Secrets Law § 5:33.

context of litigation and subject to whatever protective orders the court may apply.[99] Courts presume the risk of harm to be higher if the parties are business competitors and lower in other circumstances.[100] They may also consider the availability of alternative intellectual property protections, such as copyrights or patents, that would mitigate the risks.[101] In most civil cases, courts grant discovery subject to a protective order.[102] In criminal cases, the opposite is true; courts frequently deny discovery altogether.[103]

Ideally, courts in both civil and criminal cases would use the balancing test to effectuate overt policy choices, such as by adopting an express presumption in favor of disclosure.[104] But some judges appear to manifest

---

[99] *Coca-Cola Bottling*, 107 F.R.D., at 293 ("Because protective orders are available to limit the extent to which disclosure is made, the relevant injury to be weighed in the balance is not the injury that would be caused by public disclosure, but the injury that would result from disclosure under an appropriate protective order."). But protective orders are only available upon a showing of "good cause," and do not necessarily continue past commencement of a trial. As Judge Posner explained in *Citizens First National Bank v. Cincinnati Insurance*, "the public at large pays for the courts and therefore has an interest in what goes on at all stages of a judicial proceeding. . . ." Citizens First National Bank v. Cincinnati Insurance, 178 F. 3d 943 (7th Cir. 1999) (citing to Arthur R. Miller, *Confidentiality, Protective Orders, and Public Access to the Courts*). Posner noted explicitly that an order to seal any document believed to contain "'other confidential . . . information,' not further specified" is too broad, and that "either party and any interested member of the public can challenge the secreting of particular documents." *Id.*

[100] United States v. United Fruit Co., 410 F.2d 553, 556 (5th Cir. 1969) (Fisher, J.) (cert denied) ("There is no true privilege against discovery of trade secrets or other 'confidential' business information, but the courts nevertheless will exercise their discretion to avoid unnecessary disclosure of such information, particularly where the action is between competitors.") (quoting 4 Moore's Federal Practice, 2d Ed., pp. 2519-2520).

[101] 2 Trade Secrets Law § 27:13

[102] Fed. Open Mkt. Comm. of Fed. Reserve Sys. v. Merrill, 443 U.S. 340, 363 (1979) ("[O]rders forbidding any disclosure of trade secrets or confidential commercial information are rare. More commonly, the trial court will enter a protective order restricting disclosure to counsel."); *Coca-Cola Bottling*, 107 F.R.D. at 293 ("A survey of the relevant case law reveals that discovery is virtually always ordered once the movant has established that the secret information is relevant and necessary."); Advisory Committee's Notes on Fed. R. Civ. P. 26, 28 U.S.C.App., p. 444 ("The courts have not given trade secrets automatic and complete immunity against disclosure, but have in each case weighed their claim to privacy against the need for disclosure. Frequently, they have been afforded a limited protection.").

[103] Imwinkelried, *Source Code*, *supra* note__.

[104] For instance, one federal district court in Delaware explained that a presumption in favor of disclosure follows from "the absence of an applicable privilege" to alter the general requirements of judicial inquiry. *Coca-Cola Bottling*, 107 F.R.D., at 293("The

their policy judgments by weaving them into earlier stages of the evaluation.[105] For example, if one party makes a particularly strong showing that its alleged trade secret is valid, a judge may apply more searching scrutiny of the other party's need for the information. As the California appeals court explained in *Chubbs*, "while the burden of making a prima facie showing of the particularized need for a trade secret is on the party seeking discovery, the trial court need not ignore evidence presented by the opposing party on the question whether the information sought is a trade secret."[106] One effect of this approach is that the court may incorporate its findings about the validity of a trade secret into its measure of the need for disclosure. That type of fusion of steps of the test is, once again, more problematic in criminal than civil cases because it conflicts with the underlying values of the Sixth Amendment right to a public trial.

Whether manifest in validity ruling or rulings on the need for disclosure, courts' tendency to overvalue trade secret claims in criminal cases is inconsistent with principles of procedural justice. Law and Psychology scholars Allan Lind, Tracey Meares, and Tom Tyler have developed a "group value model" whereby the legitimacy of the criminal justice system depends on the signal that a legal process sends about how government authorities value particular social groups.[107] Under this model, the trade secrets privilege balancing test as applied to criminal cases is suspect, by encouraging courts explicitly to treat intellectual property holders as more important than two other social groups. The first group thus denigrated are all persons affected by a criminal justice proceeding—including the families of the defendant and of any complaining witnesses—who seek and deserve assurance that the government's means of determining an outcome is fair. The balancing test appears to place pure

---

reason for allowing the discovery of trade secrets whenever they are needed to advance the just adjudication of a lawsuit is simple: in the absence of an applicable privilege, judicial inquiry should not be unduly hampered.") (*internal citations omitted*).

[105] A similar ratchet could conceivably occur in the other direction, whereby a judge might demand more convincing evidence of the validity of a trade secret where the party seeking disclosure has established a particularly strong need. I have not identified this reverse pattern in any of the trade secrets privilege cases I have reviewed to date. However, Imwinkelried has noted that courts sometimes apply more searching review of whether a state secret exists when the litigant's need and the public interest in transparent litigation are at their peak. Imwinkelried, *The New Wigmore*, *supra* note __.

[106] *Chubbs* at __.

[107] *See, e.g.*, Tracey L. Meares, *Signaling, Legitimacy, and Compliance: A Comment on Posner's Law and Social Norms and Criminal Law Policy*, 36 U. RICH. L. REV. 407 (2002).

financial interests on par with those of life and liberty.

The second group comprises other persons whose duty to testify may conflict with their interests in property or confidentiality, but who are forced to testify nonetheless under existing law. Compelled disclosure in criminal cases is often challenging; parents are asked to testify against their children and vice versa, and property and financial interests do not generally excuse non-compliance with a subpoena. Indeed, even other intellectual incentive-based interests generally must yield in criminal cases to an accused's need for evidence. For example, Justice White refused to uphold an evidentiary privilege for news reporters in *Branzburg v. Hayes* because nothing protects "the average citizen from disclosing [in a criminal investigation] information that he has received in confidence."[108] His reasoning was not disturbed by the concern that compelling reporters to testify would chill news production.[109] (Justice Powell clarified in concurrence that courts should weigh the competing interests on a case-by-case basis whereby reporters can move to quash a subpoena for information that is not legitimately needed by the investigation.)[110] Such reasoning should apply even more strongly to trade secrets; while the risk of chilling news production implicates the First Amendment, courts are divided as to whether trade secrets are sufficiently property-like for their compelled disclosure to even implicate a constitutional interest.[111] The trade secrets evidentiary privilege thus likely presents constitutional issues on only one side of the conflict: the defendant's. In criminal cases, the

---

[108] Branzburg v. Hayes, 408 U.S. 665, 683 (1972).

[109] *Id.*, at 690-91. The reporters in *Branzburg* had argued for a standard similar to that of the trade secrets privilege:

> [T]he reporter should not be forced either to appear or to testify before a grand jury or at trial until and unless sufficient grounds are shown for believing that the reporter possesses information relevant to a crime . . . [that] is unavailable from other sources, and that the need for the information is sufficiently compelling to override the claimed invasion of First Amendment interests occasioned by the disclosure."

Branzburg, at 680 (1972). Thank you to Owen Fiss for calling Justice White's *Branzburg* opinion to my attention. See also state secrets privilege from REYNOLDS, and United States v. Aref, 533 F.3d 72, as described in "Digital Innocence."

[110] *Branzburg*, at 710.

[111] *See,* Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment* , 58 Hastings L.J. 777, 808-11 (2007) ("When both property and free speech interests cannot be accommodated, it is the quasi-property right that must give way, not the deeply rooted constitutional right to share and acquire information.") (*citations omitted*). Samuelson illustrates this point by comparing *Ruckelshaus v. Monsanto*, 467 U.S. 986 (1984) with *O'Grady v. Superior Court*, 139 Cal. App. 4th 1423 (2013).

trade secrets privilege wrongly singles out the social group of trade secrets holders for special treatment.

III. HISTORIES OF THE TRADE SECRETS PRIVILEGE

At first glance, today's pro-privilege consensus appears to enjoy substantial support in the historical record. This is particularly true of the legislative histories of evidence statutes across the country. The lawmakers and rule-makers who codified the privilege branded it with a venerable pedigree. They referenced legal luminaries and, as time progressed, they began to reference one another. That the leaders of the codification movement sought to weave a legitimizing historical narrative around that process is hardly a surprise. While legislators' policy decisions are not bound by the common law, a showing of historical continuity can lend credence to a proposal and weaken its opponents. The general acceptance of the privilege today is a measure of their success.

On close inspection, however, previously under-scrutinized archival records of the drafters' debates and advisory committee notes ruffle the narrative of longstanding acceptance. This Part develops an intellectual history of the current consensus in favor of the privilege. I draw from newly digitized historical documents and other archival sources to examine how the lawmakers and rule-makers behind the codification movement used historical authority, and how that use changed over time as the privilege began to gain widespread acceptance. Reading the legislative histories against historical case law and commentary, I uncover key historical dissents to the privilege and then trace how those dissents were later obscured from the historical record. Collectively, the legislative and rule-making archives construct not merely a selective but something of a revisionist history of the privilege; its actual evolution was not nearly as certain as legislators later maintained. I conclude that the idea of an unambiguous common law lineage for the trade secrets privilege—even as applied to civil cases—was a late Twentieth Century legislative invention.

In seeking to restore nuance and complexity to this history, I have three main goals. My principal objective is to show that the standards that currently govern the trade secrets privilege developed in and for civil disputes. Whether and how they should apply in criminal proceedings is a recent, unsettled, and under-theorized area of law. I also turn to history with the aim of opening space for debate. Acknowledging that the privilege has not always appeared self-evident, even for civil disputes, should create room for doubt as to the propriety of its application in

criminal proceedings today. My third hope is that mining past debates will throw the stakes of the privilege into relief, and sharpen our present insights.

A. A Civil History

A 1970 note by the Advisory Committee to the Federal Rules of Evidence perhaps best captures the general tone of legislative histories of the trade secrets privilege: "a qualified right to protection against disclosure of trade secrets has found ample recognition, and, indeed, a denial of it would be difficult to defend."[112] The note offers a series of impressive citations to support this claim: to prior codifications of the privilege in Kansas, California, New Jersey, and the Uniform Rules of Evidence; to a series of treatises including John Henry Wigmore's influential treatise on Evidence Law; [113] and to a long list of common law cases "raising trade-secrets problems," including a prominent 1917 opinion by Justice Oliver Wendell Holmes.[114] This story-through-citations soon became a model for others. Subsequent state legislatures referenced the draft federal rules when codifying the privilege themselves.[115] And when state case law offered no domestic precedents, the federal Advisory Committee note and its sources provided a convenient substitute.[116]

Yet, the 1970 note is curious not only for the assurances it spawned

---

[112] Proposed Fed. R. Evid. 508, 56 F.R.D. 183, 250 (1972). Advisory Comm. Note. Congress later rejected Rule 508 amidst heated political charges that it—along with a series of other proposed privileges—served lobbyists and special interests. Imwinkelried has given a gripping account of the history of and political controversies that plagued the doomed privileges in rejected Draft Article V of the proposed federal rules. He argues that the federal courts have largely adopted the proposed privileges anyway. Edward J. , *Draft Article V of the Federal Rules of Evidence on Privileges, One of the Most Influential Pieces of Legislation Never Enacted: The Strength of the Ingroup Loyalty of the Federal Judiciary*, ALABAMA L. REV.

[113] Also cited the following treatises: 4 Moore's Federal Practice 30.12 and 34.14 (2d ed. 1963 and supp. 1965); Barron and Holtzoff, Federal Practice and Procuedure 715.1 (Wright ed. 1961).

[114] Proposed Fed. R. Evid. 508, 56 F.R.D. 183, 250 (1972) Advisory Comm Note. Citing E.I. Du Pont Nemours Powder Company.

[115] *See, e.g.*, La. Code Evid. Ann. art. 513, Comments ("(b) This Article is identical to Federal Rule of Evidence 508, as originally promulgated by the United States Supreme Court on November 20, 1972. It is also similar to Uniform Rule of Evidence 507 (1974).").

[116] For instance, Alabama's rules advisory committee admitted that, "no trade secret privilege, ascertainable at trial, has been recognized under preexisting Alabama law," but cited the federal rules as evidence that the privilege "finds historic recognition nationally." Advisory Committee Note to Ala. R. Evid. Rule 507 (1993).

but also for the misgivings it obscured. The note's citations construct a venerable history for the privilege. But on closer review, these original sources express doubts about the privilege's lineage and propriety that recede in the Advisory Committee note that cites them.[117] It was true that, just a few years earlier, three states—Kansas, California, and New Jersey—and the National Conference on Uniform State Laws had codified a trade secrets privilege. But Kansas had cited no authorities whatsoever to support its legislation. The California Law Review Commission admitted that, "no California case has been found holding evidence of a trade secret to be privileged," and warned of "dangers in the recognition of such a privilege."[118] Indeed, the sole case citation in the California commission's comment was to a civil suit decided nearly forty years earlier in which a California court had ordered the *disclosure* of a trade secret.[119] Even the Uniform Rules had hedged that, "the limits of the privilege are uncertain."[120] And the 1917 opinion by Justice Holmes barely resembles the privilege it is cited to support; the civil defendant in that case already had the information at issue, and Holmes assumed that the judge would also "know the secrets" and have full discretion "to reveal the secrets to others"—including to expert witnesses—where appropriate.[121] After

---

[117] The federal Advisory Committee did concede that trade secrets protection during litigation was "sometimes said not to be a true privilege," and that "competing interests," such as "eliciting facts required for full and fair presentation of a case" and the "dangers of abuse," should be weighed against granting the privilege in any given case. Advisory Comm. Note, REPORT OF THE COMMITTEE ON RULES OF PRACTICE AND PROCEDURE TO THE JUDICIAL CONFERENCE OF THE UNITED STATES (Oct. 12 1970).

[118] The state commission warned that the privilege might "hinder the courts in determining the truth," and produce "a legally sanctioned license to commit" unfair competition, fraud, or the improper use of dangerous materials when wrongdoers claimed the privilege. CALIFORNIA LAW REVIEW COMMISSION, EVIDENCE CODE WITH OFFICIAL COMMENTS 1202-03 (Aug. 1965). Note that as of Feb. 25, 2017, I have been unable to locate the legislative history of the New Jersey statute.

[119] The court in that case had declared that, "[t]he right of the manufacturer to the protection of his trade secret ought to yield to the superior right of an innocent person who has suffered injury through no fault of his own . . . ." The court had noted a trend towards protecting trade secrets, but not recognizing them as privileged. *Wilson v. Superior Court*, 66 Cal. App. 275, 278, 279 (1924), cited in Cal. E. Code 1060 Law Revision Commission Comments ("The general trend of authority, as recognized by text-writers and by courts alike, is to the effect that, while there is no absolute privilege (such as may be present where certain confidential relationships exist) to decline to reveal a so-called trade secret, yet, unless the rights of innocent persons are dependent upon their disclosure, the property right of the possessor of such trade secret should be protected.").

[120] 61ST CONFERENCE HANDBOOK OF THE NATIONAL CONFERENCE ON UNIFORM STATE LAWS AND PROCEEDINGS ANNUAL MEETING 448, 475 (1952).

[121] E.I. DuPont De Nemours Powder Co. v. Masland, 244 U.S. 100, 103 (1917) ("[I]f, in [the judge's] opinion and discretion, it should be advisable and necessary to take

Holmes had determined that the trade secrets status of the information was not at issue, he enjoined the defendant from sharing the information with experts who could evaluate that status. In short, the rule in Holmes's view was not so much a privilege as a protective order.[122]

Moreover, the 1970 note contains another conspicuous omission: its case law citations reach to 1889, but its rule-making references stop short with the Uniform Rules of Evidence of 1953.[123] That fact is striking because it is exceedingly unlikely that the Committee could have thought the Uniform Rules were the first to codify the privilege. The Uniform Rules themselves were based on the American Law Institute's Model Code of Evidence from a decade before,[124] and they expressly credited the Model Code version of the trade secrets privilege as the basis for its Uniform counterpart.[125] Yet, the Model Code appears nowhere in the federal Advisory Committee's citation-based history of the privilege. To understand the significance of this puzzling exclusion, it will be helpful to jump backwards in time to a period well before the inception of the Model Code, when no consensus about a trade secrets privilege existed.

1. Dissensus

Whether or not to excuse a witness from testifying about sensitive financial information was a visible issue to Nineteenth Century courts. But

---

in others, nothing will prevent his doing so.").

[122] Those facts have not stopped numerous post-1970 commentators from continuing to cite to the Holmes opinion as an early exemplar of the trade secrets privilege. *See, e.g.*, Kevin Brown, MEMORANDUM TO ADVISORY COMM. ON EVIDENCE RULES 239 (Apr. 12, 2013) (citing Advisory Comm. Note to Proposed Rule 508).

[123] Advisory Comm. Note, REPORT OF THE COMMITTEE ON RULES OF PRACTICE AND PROCEDURE TO THE JUDICIAL CONFERENCE OF THE UNITED STATES (Oct. 12 1970) (citing *Dobson v. Graham*, 49 F. 17 (E.D. Pa. 1889)).

[124] Model Code of Evidence 130 (1942), Rule 226. The Uniform Rules developed from concerns that the Model Code was too radical for the majority of states to adopt; the National Conference on Uniform State Laws felt that the Model Code contained "departures from traditional and generally prevailing common law and statutory rules of evidence [that were] too far-reaching and drastic for present day acceptance." The Uniform Rules sought to temper those elements in order to achieve greater "acceptability and uniformity" among the states. 61ST CONFERENCE HANDBOOK OF THE NATIONAL CONFERENCE ON UNIFORM STATE LAWS AND PROCEEDINGS ANNUAL MEETING 448, 448 (1952).

[125] The comment to the Uniform trade secrets privilege credits that this rule "follows" a proposed Missouri rule that never passed, and "American Law Institute Model Code of Evidence Rule 226." 61ST CONFERENCE HANDBOOK OF THE NATIONAL CONFERENCE ON UNIFORM STATE LAWS AND PROCEEDINGS ANNUAL MEETING 448, 475 (1952).

instead of framing compelled disclosure as a threat to business and intellectual innovation, as commentators do today, they viewed it as an issue of self-incrimination; the articulated concern at the time was that compelling a witness to testify against their "pecuniary interest" might subject them to civil liability, and thus run afoul of constitutional restrictions against compelling a witness to testify against themselves.[126]

The issue was settled on the side of disclosure for some time, at least in England, by an influential 1806 holding that, "the witness was bound to answer a question, although his answer might render him liable to a civil action."[127] Parliament immediately codified the rule, declaring in The Witnesses Act of 1806 that, "a witness cannot by law refuse to answer a question relevant to the matter in issue . . . on the sole ground that the answering of such question may establish or tend to establish that he owes a debt, or is otherwise subject to a civil suit either at the instance of his Majesty or of any other person or persons."[128] Courts in the United States took note of both the English holding and the Act.[129] Maryland[130] and Pennsylvania[131] each adopted a parallel rule. In 1830, the Massachusetts Supreme Court held that, "a witness may be called and examined in a matter pertinent to the issue, where his answers will not expose him to criminal prosecution, or tend to subject him to a penalty or forfeiture, although they may otherwise adversely affect his pecuniary interest."[132] Competing financial interests did not excuse testimony.[133]

---

[126] *See, e.g.*, Bull V. Loveland, 10 Pick. 9 (Mass. 1830) (providing an overview of the development of the law in England and the United States concerning compelling a witness to testify against their pecuniary interest).

[127] *Bull*, 10 Pick., at 9 (describing *Lord Melville's Case*, House of Lords (1806)).

[128] Witnesses Act, 46 George 3 (May 5, 1806).

[129] *See, e.g.*, *Bull*, 10 Pick., at 9.

[130] Taney v. Kemp, 4 Har. & Johns. 348; Stoddart v. Manning, 2 Har. & Gill, 147.

[131] Baird v. Cochran, 4 Serg. & Rawle, 397.

[132] *Bull*, 10 Pick., at 9. The Massachusetts Supreme Court initially refused in 1810 to compel a witness to testify who claimed a competing financial interest in the outcome of the case. It is unclear whether the court made that determination because the witness would be deemed unreliable, or because the court sought to protect the witness's sensitive financial information from disclosure. Regardless, the case was soon overruled and the rule clarified that no privilege applied to commercial information in Massachusetts. *Appleton v. Boyd*, 7 Mass. 134 (Mass. 1810) *overruled* by *Bull*, 10 Pick., at 9. *See also*, Devoll v. Brownell, 5 Pick. 448 (Mass.) (holding that the state constitutional protection against self-incrimination did not apply to questions of property).

[133] *See also*, Edmund H. Bennett, Russell Gray & Henry W. Swift, *What Questions Witness may Refuse to Answer*, *in* III A DIGEST OF THE REPORTED DECISIONS OF THE SUPREME JUDICIAL COURT OF THE COMMONWEALTH OF MASSACHUSETTS FROM 1804 TO 1879 WITH REFERENCE TO EARLIER CASES 5700-01 (1881) ("A witness is bound to answer a question in a matter pertinent to the issue, where his answer will not expose him

By the early Twentieth Century, courts and commentators in the United States had begun to split on the issue. Two leading treatises—William Mack's Cyclopedia of Law and Procedure and Wigmore's treatise on Evidence Law—acknowledged some form of privilege, but how much was ambiguous.[134] Both expressed concern over the risk that business competitors might exploit a witness's duty to testify regarding trade secrets.[135] But both also cautioned against the excess protection of trade secret evidence. Mack's urged courts to compel disclosure if the interests of justice "imperatively demand it," observing there is "no absolute right to refuse to answer pertinent questions."[136] Kenneth Graham, Jr. has characterized Wigmore's approach to the privilege as a "reluctant embrace."[137] In fact, Wigmore's early writings were arguably hostile. The first 1905 edition of his treatise, published when Wigmore was forty-two years old, recognized a limited form of privilege for trade secrets evidence, which he called an "occasional necessity."[138] But the text also advocated that courts adopt a presumption against the validity of any claimed trade secrets;[139] pointed out that honoring a privilege in certain cases "might amount practically to a legal sanction" of fraud by allowing wrongdoers to withhold information from the courts;[140] and insisted that "no privilege of secrecy should be recognized if the rights of possibly innocent persons depend essentially or chiefly, for their ascertainment, upon the disclosure in question."[141] This first edition of Wigmore's treatise

---

to criminal prosecution, or tend to subject him to a penalty or forfeiture, although it may otherwise adversely affect his pecuniary interest.").

[134] *See, e.g.*, Wigmore at 3002 ("What the state of the law actually is would be difficult to declare precisely.").

[135] William Mack, 40 CYCLOPEDIA OF LAW AND PROCEDURE 2532 (1912) ("[I]t is not the policy of the law that valuable secrets shall be extorted from a witness under the cover of legal proceedings, and accordingly a witness will not be compelled to disclose a trade-secret, where the interests of justice do not imperatively demand it."); 3 Wigmore 3001, 2212(3)(1905) ("[I]t may be of extraordinary consequence to the master of an industry that his process be kept unknown from his competitors, and that the duty of a witness be not allowed to become by indirection the means of ruining an honest and profitable enterprise.").

[136] By suggesting that information should be disclosed if the inquiry were 'pertinent' and 'imperative,' the Mack analysis emphasized a burden on the party seeking disclosure of a trade secret to establish relevance and necessity. Mack, Cyclopedia, at 2532.

[137] Graham offers little explanation for this conclusion. Fed. Practice & Procedure.

[138] 3 Wigmore 3001, Section 2212(3) (1905).

[139] Wigmore at 3002 (1905) ("[A] person claiming that he needs to keep these things secret at all should be expected to make the exigency particularly plain.")

[140] Wigmore at 3002 (1905) ("No privilege at all should there be conceded . . . .").

[141] Wigmore at 3002 (1905) ("[T]estimonial duty to the community is paramount to private interests, and . . . no man is to be denied the enforcement of his rights merely

seems even to question the underlying value of substantive trade secrets law, commenting that, "in an epoch when patent-rights and copy-rights for invention are so easily obtained and so amply secured, there can be only an occasional need for the preservation of an honest trade secret without resort to public registration for its protection."[142]

In fact, in many courts at the time, witnesses called to testify about confidential commercial information were regularly required to answer without any special accommodation. According to one scholarly account from 1905, courts "generally followed" the rule that a witness could not refuse to testify simply because doing so might cause them a "pecuniary loss."[143] Some courts recognized a limited right to refuse to disclose documents in open court "where the evidence is irrelevant or otherwise inadmissible in the case."[144] The key issue to note here is the burden placed on the party seeking disclosure. Judge Learned Hand articulated this issue particularly clearly. Writing for the Southern District of New York in 1920, he refused to raise the burden on parties seeking relevant trade secrets information, reasoning that the right "to bring out the truth must prevail," even if damage to an alleged trade secret holder were "an inevitable incident to any inquiry."[145] Later Southern District decisions followed Hand's lead, as did federal courts in other circuits.[146] One court found that it would be "unusual" to exclude trade secrets information from discovery at trial unless "the information was utterly remote and was not sought in good faith."[147] Another reasoned that, "if [a claimant] has chosen secrecy rather than the protection of the patent law, it must give way before the rights of third parties."[148] The Massachusetts Supreme Court stayed its course from nearly a century before, explaining in 1921 that a full and fair cross-examination "is a matter of absolute right," and

---

because another possesses the facts without which the right cannot be ascertained and enforced.").

[142] 3 Wigmore 3001-02, Section 2212(3) (1905).

[143] *The Privilege of a Witness to Refuse to Disclose Trade Secrets*, 3 MICH. L. REV. 565, 567 (1905) (crediting *Lord Melville's Case*, House of Lords (1806) with establishing this rule).

[144] Crocker-Wheeler Co. v. Bullock, 134 Fed. R. 241 (Dec. 1904).

[145] *Grasselli*, 282 F. 379 (1920) (Hand, J.)

[146] *See, e.g.*, United States Gypsum v. Pacific Portland Cement, 22 F.2d 180, 181 (S.D. Cal. 1927) (ordering pre-trial disclosure of an alleged trade secret after finding that the information at issue was "material and relevant," and mentioning no heightened burden to show relevance or necessity).

[147] 31 F.2d at 988-89 (SD Cal [date?])

[148] Claude Neon Lights v. Rainbow Light, 31 F.2d 988, 988 (SDNY 1927) ("[If a claimant] has chosen secrecy rather than the protection of the patent law, it must give way before the rights of third parties.").

that allowing a witness to refuse to disclose trade secrets that are relevant to a case "is essentially unsound."[149]

Yet some courts had begun to rule the other way. In 1924, the Pennsylvania Supreme Court dubbed the state in which it sat a "great industrial commonwealth," and ruled that if witness testimony would expose a non-party's trade secrets "to the disadvantage and injury of such third persons, the inquiry should not be allowed."[150] The court cited concern that trade secrets not be disclosed unless absolutely necessary.[151] But the opinion did not expressly consider either the relevance and materiality of the information sought or what burden would be required to compel its disclosure. By 1933, in the midst of the Great Depression, the reasoning of the New York Court of Appeals ruling was more robust—and more analogous to applications of the trade secrets privilege today. The court held that a party seeking trade secrets information must meet a higher burden to show relevance than ordinarily required in civil procedure, and must also show that the information was "indispensable for ascertainment of the truth" and "cannot otherwise be obtained."[152]

2. Omissions

Around the same time, the American Law Institute began efforts to unify Evidence Law in courts across the nation. They were to create a Model Code of Evidence. Wigmore, now age seventy-seven, served as Chief Consultant for this mission. Wigmore has a reputation for disliking evidentiary privileges because they hinder the quest for truth.[153] Yet somehow, over the prior quarter-Century, he had become an ardent supporter of the trade secrets privilege in particular. Colleagues at the American Law Institute wrote that he "strenuously insists" on including the privilege in the Model Code. Considering a comment that mirrored his own earlier treatise text—"[t]he extent to which such a privilege should exist is doubtful when patent-rights and copyrights are so readily obtainable,"[154]—Wigmore responded with a rebuke: "There are hundreds

[149] Gossman v. Rosenberg, 129 N.E. 424, 425-26 (Mass. 1921).

[150] Huessener v. Fishel & Marks, 281 Pa. 535, 542 (Pa. 1924).

[151] *Huessener*, 281 Pa., at 542 (quoting Mack's treatise and then also citing 4 Wigmore on Evidence (2d Ed.) sec 2212, 701).

[152] Drake v. Herman, 185 N.E. 685, 686 (N.Y. 1933) ("Generally, disclosure of legitimate trade secrets will not be required except to the extent that it appears to be indispensable for ascertainment of the truth.").

[153] See Imwinkelried.

[154] American Law Institute, COMMENTS REGARDING MODEL CODE OF EVIDENCE Book 3 and 5 (date ?).

of trade-secrets which if patented would allow piracy without the possibility of tracing," he contended. And then he added a short line that may lend insight to his change of heart: "my brother had one such."[155]

Meanwhile, Judge Hand, a decade younger than Wigmore, served first as Advisor and later as Vice President to the American Law Institute's mission. Hand had maintained his opposition to the trade secrets privilege, and tried to purge the Model Code of any reference to it. His position was that, "wherever [trade secrets] are material to any issue in the case disclosure of them must be made." For Hand, the privilege simply did not exist. Wigmore shot back, calling Hand "difficult to understand," and claiming that "no case repudiating" the privilege had ever been found. Of course, had Wigmore bothered to read Hand's own prior opinions, he would have discovered such a case. Apparently he did not feel the need. Neither Hand's ruling on the issue nor the cases it inspired ever made it into Wigmore's comments to the Institute or, for that matter, into any edition of his famed treatise.

The American Law Institute split. Harvard Law Professor Edmund Morgan supported Hand, others Wigmore. The disagreement continued for years until, on the eve of Pearl Harbor in 1943, Wigmore tried a new strategy: spotlight military manufacturers that relied on trade secrets, like aircraft and chemical factories. Wigmore even made it personal, directing his comments to Morgan and implying that he specifically had forgotten the needs of these vital industries. When the Model Code of Evidence was finally published on May 15, 1942, to a nation fully entrenched in World War II, it included a trade secrets privilege. Eleven months later, Wigmore died.

The Model Code set the tone for subsequent policy reforms, although the initial controversies around the privilege never fully subsided. Edward Imwinkelried and Kenneth Graham Jr. have both written vivid histories of the political debates surrounding a proposed (but never passed) trade secrets privilege in Federal Rule of Evidence 508.[156] Among other issues, they document concerns that industry lobbyists had hijacked the rule-making process to advocate for new and expanded privileges that served their interests. There is no reason to repeat that narrative here, and it would be difficult indeed to improve on their accounts.[157] Suffice it to say

---

[155] American Law Institute, COMMENTS REGARDING MODEL CODE OF EVIDENCE Book 5, Comment J.H.W. Nov. 1, 1939.

[156] Graham, *Fed. Practice & Procedure*; Imwinkelried, *Article V*.

[157] Graham actually lived the history, testifying to Congress as a recent law graduate.

that the series of state and federal legislative debates about the trade secrets privilege that followed the passage of the Model Code, including the Uniform Rules, proposed Federal Rule of Evidence 508, Texas Rule of Evidence 507, and California's evidence code, contain no references to the heated clash between Wigmore and Learned Hand. Wigmore's treatise was cited repeatedly. Judge Hand's ruling in opposition was rarely if ever mentioned.[158] And, beginning with the federal Advisory Committee's 1970 note, the Model Code itself dropped from the historical narrative.

Perhaps the Committee sought to purge the disagreement behind the forging of the Model Code, along with any doubts as to the wisdom of the privilege that sore memories might provoke. Such is a matter of speculation. But one thing is clear; mapped over time, the legislative histories of the trade secrets privilege exude greater and greater confidence in its past. The federal Advisory Committee's 1970 note was a pivot in a broader process. The note's own declaration that the privilege had "found ample recognition" helped to produce what it purported to describe.

B. A Criminal History

Prior to the 1990s, case law and legislative histories both evince a dearth of supporting authority for the application of a trade secrets privilege in criminal proceedings. The first edition of Wigmore's treatise did cite two criminal cases amidst a slew of civil disputes, but the secrets in each of those cases had been ordered *disclosed*.[159] In *Trial of Maharajah Nundocomar* (1775), the East India Company refused to produce records during a public trial because they contained secrets.[160] The court found that company papers that contain material evidence must be produced in both civil and criminal cases: "Humanity requires it should be produced when in favor of a criminal, justice when against him."[161] In *Rex v. Webb* (1834), the defendant had allegedly poisoned the deceased, who was

---

He argued that recognizing a trade secrets privilege—even in civil cases—would impose an unreasonable burden on parties seeking to compel disclosure of trade secret evidence,

[158] *See, e.g.*, California Law Review Commission, Tentative Recommendation and a Study relating to The Uniform Rules of Evidence Article V. Privileges 461-62 (Feb. 1964) (recommending adoption of the Uniform Rules trade secrets privilege and citing Wigmore and a series of civil precedents for support, but neither mentioning Judge Learned Hand nor any of his opinions).

[159] Wigmore 1905 (citing 1834, R., v. Webb, 1 Moo. & Rob. 405, 412).

[160] It is ambiguous whether the secrecy claimed was more akin to today's trade secrets or to today's state secrets.

[161] 20 How. St. Tr. 1057 (1775).

already ill, by administering excessive quantities of a purported medicinal pill. When, at trial, the prosecution sought to cross-examine the pill's manufacturer about its ingredients, the witness "declined answering this question, and claimed the protection of the Court, inasmuch as in this mode the secret of his invention (for which he had not any patent) might be made public, to his great loss."[162] The judge ordered an answer anyway, offering neither protective order nor sealing action, and merely "suggested" that the prosecutor limit his questions to those that "the ends of justice required."[163]

I have found no legislative discussion of the status of trade secret evidence in criminal cases until the second half of Twentieth Century. Neither the American Law Institute's comments in drafting the Model Code nor the Conference Handbooks that document the drafting of the Uniform Rules of Evidence mention criminal proceedings. When Kansas became the first state to codify the privilege in 1963, it incorporated the privilege into its Code of Civil Procedure.[164] Even Kenneth Graham, Jr.'s testimony to Congress advocating against the adoption of the privilege into the federal rules omits any consideration of the operation of the privilege in criminal as compared to civil proceedings.[165]

The first hint of change occurred in 1967, when California incorporated the privilege into its evidence statute and expressly provided for its application to criminal cases.[166] Given the novelty of the statutory

---

[162] Rex v. Webb, 174 Eng. Rep. 140, 142 (City of York, 1834).

[163] *Id.* One dynamic that may have influenced this outcome was a widespread problem at the time of fraudsters selling fake drugs.

[164] Kansas Code of Civ. P., K.S.A. 60-432 (effective 1964).

[165] Apart from a footnote acknowledging that the author is unaware of any *federal* criminal cases that apply the privilege, even Graham's contemporary analysis never distinguishes between civil and criminal contexts. Graham section 5641, note 25.

[166] California Evidence Code 1060, Stats 1965, c. 299, section 2, operative Jan. 1, 1967. Section 1060 establishes the privilege in general, including a right of trade secret holders to refuse entirely to disclose protected information, whether to the court or to an opposing party. Cal. Evidence Code 1060. But sections 1061(b) and 1062 distinguish criminal proceedings, presenting additional rules that appear expressly to apply to criminal cases alone.1061(b). The defense in *Chubbs* argued that sections of California's statutory trade secrets privilege that expressly apply to criminal cases appear to presume that defendants will have some form of access to trade secret information even when the privilege is operative. They expressly contemplate that the defendant and defense counsel be present in any hearing the court might hold concerning the validity of a claimed trade secret.1061(b)(3). And they require the court in certain circumstances to issue a protective order "limiting the use and dissemination of" information, such as by requiring that it "be disseminated only to counsel for the parties"; withholding information from

enterprise, it is small surprise that the commission laced its commentary with caveats and offloaded the specifics to the courts. The text of the statute expressly prohibited claims to the privilege that would "tend to conceal fraud or otherwise work injustice."[167] And the commission's comment suggested that information that could adequately be protected by copyright and patent laws should not qualify because "[r]ecognizing the privilege as to such information would serve only to hinder the courts in determining the truth without providing the owner of the secret any needed protection."[168] But, in general, limits on the scope of the privilege were "necessarily uncertain," and it was up to judges to work out the kinks.[169]

As some measure of the privilege's reception by the courts, or of the significance of intellectual property pre-World Wide Web, no such occasion would arise for another quarter century.[170] Not until 1992 in *Bridgestone* (a civil case) did a California appeals court first elaborate standards to govern the trade secrets privilege.[171] And while the *Bridgestone* standards ultimately became the most cited test for evaluating claims to a trade secrets privilege nationwide,[172] no court would address such a claim in a criminal case in California until *People v. Chubbs* in 2015.[173]

---

experts who are economic competitors to the trade secret holder "unless no other experts are available," 1061(b)(4)(A)-(C), and sealing the public docket. 1061(b)(4)(D); 1062. But they never mention denying defense access altogether. TrueAllele's manufacturer responded that the privilege was proper because California's evidence statute generally applies to both civil and criminal cases. *See* People v. Chubbs, Third Party Witness Dr. Mark W. Perlin's Br. in Support of Assertion of Trade Secret Privilege (Jul. 14, 2014), CA Sup. Ct. Los Angeles County, No. NA093179, at 1-2.

[167] California Evidence Code 1060. A similar exception had been include in the Model Code and Uniform Rules.

[168] *Id.*

[169] *Id.*

[170] The twelve cases that raised the issue over those twenty-five years all concerned issues of public disclosure or disclosure to government regulators, not disclosure to a party subject to a protective order. *See, e.g.*, Agricultural Labor Relations Board v. Glass, 175 Cal. App. 3d 703 (1985); San Gabriel Tribune v. Superior Court, 143 Cal. App. 3d 762 (1983); California School Employees v. Sunnyvale Elementary School, 36 Cal. App. 3d 46 (1974); Urive v. Howie, 19 Cal. App. 3d 194 (1971).

[171] Bridgestone/Firestone v. Superior Court, 9 Cal. Rptr. 2d 709 (1992).

[172] See, e.g., TX Sup. Ct, FL, etc.

[173] California courts during the 1990s had but two occasions to consider the relationship between the statute's civil and criminal sections, and in both occasions the courts borrowed standards from the criminal sections to apply in to civil disputes, rather than the other way around. Stadish v. Superior Court, 71 Cal. App. 4th 1130, 1145 (1999) ("We conclude that the procedures called for in section 1061 have a utility in a civil action in protecting the trade secret privilege provided for in section 1060 and

Indeed, the historical record suggests that, before *Chubbs*, legislators and commentators may not even have conceived of the application of the privilege to block criminal defendants' own access to evidence. Rather, the concern at the time it was adopted was keeping trade secrets from *public* disclosure by sealing court records. The individual who initially drafted the statute, Kenneth Rosenblatt of the California District Attorney's Office, described it as an unprecedented "statutory procedure for sealing [trade secrets] in criminal cases."[174] In 1991, Rosenblatt published an article describing the issue of "how to protect confidential information from disclosure during a criminal proceeding without violating a defendant's Sixth Amendment right to a fair trial and the public's First Amendment right to view criminal justice proceedings."[175] While he noted early on that, "the accused enjoys a panoply of constitutional rights," the article focuses almost exclusively on defendants' public trial rights and the public's access rights. Rosenblatt makes no mention of the newly minted privilege as a limit on discovery or subpoena power.[176]

There are a smattering of criminal cases that consider trade secrets disclosures during the 1970s and 1980s, but—as with Rosenblatt's article—they primarily concern issues of sealing and excluding the public from trials. In 1970, the Second Circuit found that a trial court had been in error to deny the defense a copy of a computer program that the government's witness relied on to generate 'figures' used in their testimony.[177] Four years later the Second Circuit ordered a third party's

---

should be followed."); State Farm Fire & Casualty Co v. Superior Court, 54 Cal. App. 4th 625, 650-51 (1997) (applying the criminal sections of the statute in a civil case without comment). In *Chubbs*, all parties recognized that how the privilege applied to a criminal case was an issue of first impression. People v. Superior Court (Chubbs), Petitioner's Reply Br. (Sept. 19, 2014), CA App. Ct. LASC No. NA093179, at 6.

[174] Kenneth Rosenblatt, *Criminal Law and the Information Age: Protecting Trade Secrets from Disclosure in Criminal Cases*, 8 THE COMPUTER LAWYER 17 (1991) (noting that the Uniform Trade Secrets Act had provided for sealing records in civil cases, but had made no parallel provision for criminal proceedings).

[175] Rosenblatt at 15.

[176] Rosenblatt. Also note that he's taking about "trade secrets prosecutions," i.e. prosecutions for trade secrets theft, rather than trade secrets in criminal justice technologies. at 15.

[177] United States v. Dioguardi, 428 F.2d 1033 (2d Cir. 1970) ("We fully agree that the defendants were entitled to know what operations the computer had been instructed to perform and to have the precise instruction that had been given. It is quite incomprehensible that the prosecution should tender a witness to state the results of a computer's operations without having the program available for defense scrutiny and use

trade secret to be disclosed in a criminal proceeding, but closed the proceeding to the public and required all witnesses present to sign a protective order.[178] The trial court in that case had also ordered disclosure but refused even to close the courtroom, citing Sixth Amendment concerns.[179]

Trade secrets barriers to defendants' own access to evidence began consistently to appear in criminal cases in the 1990s and early 2000s. The manufacturers of DNA test kits claimed trade secrets in various aspects of their methodologies, including developmental validation studies[180]; statistical standards[181]; and 'primer sequences.'[182] At least one conviction was reversed because a private laboratory had refused to disclose its statistical standards for determining a DNA 'match.'[183] A Vermont court excluded DNA evidence as a result of the manufacturer's nondisclosures.[184] Early commentators called for national standards "so that the laboratories cannot hide behind 'trade secrets' to withhold

---

on cross-examination if desired.").

[178] Stamicarbon N.V. v. American Cuanamid Co., 506 F.2d 532 (2d Cir. 1974) ("We believe he does have the power at least partially to restrict access to the contempt proceedings when testimony which would reveal Stamicarbon's secrets is received.").

[179] *Id.* ("To ignore the undeniable benefits rendered by the assistance of press and public at criminal proceedings would indicate an unawareness of history as well as legal precedent. In almost all cases the interests which would suffer from publicity will merit less attention than the very real concern that the accused might be prejudiced by restricted attendance. It is only under the most exceptional circumstances that limited portions of a criminal trial may be even partially closed."). *See also*, United States v. Cianfrani, 448 F. Supp. 1102 (E.D. Penn. 1978) (analogizing to court review of trade secrets in camera, but not mentioning denying disclosure to defendants altogether).

[180] People v. Cavin, 2000 WL 35721883 (Mich. App. Ct. 2000) (The manufacturer disclosed its primer sequences under a protective order but refused to disclose its developmental validation data.); People v. Davis, 601 N.Y.S. 2d 174 (Sup. Ct. App. Div. 1993) (finding that "the withholding of the primer sequences does not affect the scientific validity of the kits").

[181] State v. Schwartz, 447 N.W.2d 422, 427 (Minn. 1989) ("The defense request for more specific information regarding its methodology and population data base was denied by Cellmark. Arguably, trade secrets may be at stake for commercial laboratories. Protective measures could be pursued, however, before denial of discovery is appropriate.").

[182] *See, e.g.*, State v. Lynch, 1999 WL 34966936 (AZ 1999). *See also*, Mellon, *supra* note__.

[183] Davis, 601 N.Y.S. 2d 174. Note that it is not clear from the opinion *why* the laboratory refused to disclose its statistical standards, but it is likely that they were considered proprietary.

[184] State v. Pfenning, 2000 WL 35721887 (D. Ct. VT 2000) (excluding DNA evidence under *Daubert* test because of the kit manufacturer's lack of transparency).

information from defendants."[185] In 1992, the National Research Council Committee on DNA Technology in Forensic Sciences published a report admonishing that, "[p]rivate laboratories used for testing should not be permitted to withhold information from defendants on the grounds that 'trade secrets' are involved."[186] But most courts eventually upheld the manufacturers' claims to a trade secrets privilege, and found DNA evidence admissible anyway.[187] By 2007, a general consensus had formed; the American Bar Association proposed its own trade secrets privilege standard specifically for DNA evidence in criminal cases.[188] The Bar Association adopted the language of proposed Federal Rule of Evidence 508 nearly verbatim, quoting the Advisory Committee's 1970 note that privilege had found "ample recognition, and indeed, a denial of it would be difficult to defend."[189]

A second wave of criminal cases challenging trade secrets evidence began around the mid-2000s, when a series of DUI defendants tried to access the source code in breath test devices. They wanted to see for themselves how the devices actually worked, not take the manufacturers at their word or limit their ability to present a defense to black-box validation studies. Some courts ordered the source code disclosed to defense experts, leading to the discovery of some bugs and otherwise to the affirmation of the tools.[190] Others found that the code was not in the government's

---

[185] George J. Annas, *DNA Fingerprinting in the Twilight Zone*, 20 The Hastings Ctr. Report 35-37 (1990).

[186] Comm. on DNA Technology in Forensic Science, National Research Council, DNA Technology in Forensic Science 176 (1992). The committee also cautioned that, "[p]rotective orders should not be used to prevent experts on either side from obtaining all relevant information, which can include original materials, data sheets, software protocols, and information about unpublished databanks." *Id.* at 162. *See also*, William C. Thompson & Simon Ford, *DNA Typing: Acceptance and Weight of the new Genetic Identification Tests*, 75 Va. L. Rev. 45, 60 (1989) (observing the contradiction between asserting that a scientific methodology is "sufficiently known and proven to be regarded as generally accepted by the scientific community," and thus admissible in court, while at the same time arguing that the details of that methodology are "sufficiently unique and innovative to constitute trade secrets.").

[187] State v. Bailey, 677 N.W.2d 380 (Minn. 2004); State v. Traylor, 656 N.W.2d 885, 898-899 (Minn. 2003); State v. Nose, 2003 WL 25906779 (D. Minn. 2003); People v. Garcia, 2001 WL 1464138 (App. Ct. CA 2001); People v. Hill, 89 Cal. App. 4th 48, 56 (App. Ct. CA 2001); State v. Dishmon, 2000 WL 35720025 (D. Ct. Minn. 2000).

[188] American Bar Association, *Standard 16-5.2 Trade Secrets Privilege*, *in* 3 ABA Standards for Criminal Justice DNA Evidence 102-04 (2007).

[189] American Bar Association, *Standard*, *supra* note__ at 103.

[190] The Minnesota Supreme Court granted discovery in 2007, finding "no reason why drivers tested using that instrument should not have full access." In re Com'r of Pub. Safety, 735 N.W.2d 706, 709 (Minn. 2007).

possession, and thus not the prosecutor's to hand over. The rest held that defendants hadn't done enough to show that the source code was relevant or necessary for their case.[191] Judges in that last group sometimes measured defense arguments against a higher burden than they would have applied had the defense sought evidence with no intellectual property strings attached. But none ruled explicitly that they were, or were not, "privileging" the trade secrets evidence.

The *Chubbs* opinion changed all of this in 2015 by applying an explicit evidentiary privilege for trade secrets evidence in a criminal case for the first time in Californian, and likely national, history. The introduction of trade secret evidence in criminal cases is a relatively recent development.

IV. A CRIMINAL TRADE SECRETS PRIVILEGE IS UNNECESSARY

Deeply challenging competing interests are no strangers to criminal courts. Courts must balance defendants' rights to access material evidence against an array of possible counter-weights: an alleged rape victim's privacy rights in their emails or web search history; a parent's resistance to testifying against their child or vice versa; a confidential informant's safety by way of anonymity. Yet none of these types of evidence is categorically privileged. To be sure, when courts weigh competing interests in secrecy and disclosure, they often apply a more searching analysis of the relevance and necessity of the evidence. But this more searching review is different from an evidentiary privilege because it applies across the board to all sensitive information examined on a case-by-case basis, without giving special treatment to one category of witness over another.

This Part addresses non-privilege options for protecting valid trade secrets during criminal cases. It explains that an evidentiary privilege is not necessary because criminal discovery and subpoena procedures already tightly confine defendants' access to information. In addition, courts can deny frivolous or abusive discovery requests and subpoenas without resort to privilege. And, in extreme cases when disclosing relevant information

[191] A 2008 Florida Appeals Court denied discovery absent a "particularized showing" of necessity, a higher threshold for materiality than the court required for discovery of the physical device in the same case. State v. Bastos, 985 So. 2d 37, 43 (Fla. Dist. Ct. App. 3d Dist. 2008). For additional examples, the Georgia Supreme Court vacated a denial of discovery in 2011 because of error in applying an overly stringent threshold showing of materiality, Davenport v. State, 289 Ga. 399, 711 S.E.2d 699 (2011), and that same year a separate Georgia Appeals Court expressed a commitment to assist defendants in discovering code, Yeary v. State, 289 Ga. 394, 711 S.E.2d 694 (2011).

in response to non-frivolous defense requests creates a well-founded concern of harm, limited protective orders are available to safeguard the interests of trade secrets holders to the full extent reasonable. Attorneys Robert M. Cary, Craig D. Singer, and Simon A. Latcovich have written a thorough overview of federal discovery and subpoena rules and practice.[192] I draw on their insightful analysis to show precisely how restrictive the baseline threshold for defendants to access trade secrets evidence already is, without a privilege raising that burden further still. The following discussion focuses on federal criminal discovery, but similar issues arise in many state discovery statutes.[193]

A. Discovery

The first avenue for protecting valid trade secrets without relying on a blanket privilege in criminal cases is through reasonable restrictions on discovery. Criminal discovery was virtually non-existent until the mid-twentieth century. One classic justification was that providing discovery would exacerbate constitutional inequalities that already skewed in favor of the defense,[194] such as the prosecution's burden of proof,[195] or Fifth Amendment limits on the government's power to demand inculpatory information from the accused. If discovery were granted, the argument went, the government would open its files to the defense but receive nothing comparable in return. Withholding information from defendants was seen to level the playing field.[196]

Critics of this anti-discovery perspective noted that numerous other procedural and material powers skew in favor of the state.[197] Prosecutors may issue grand jury subpoenas and search and seizure warrants; may

---

[192] Robert M. Cary, et. al., FEDERAL CRIMINAL DISCOVERY (2011).

[193] *See, e.g.*, John Schoeffel, THE LEGAL AID SOCIETY, CRIMINAL DISCOVERY REFORM IN NEW YORK (April 1, 2009).

[194] Historically, advocates of limited criminal discovery also reasoned that providing information to defendants would incentivize them to commit perjury, or might threaten the safety of government witnesses. *See, e.g.*, Chief Justice Vanderbilt's arguments outlined in Justice Brennan's article *quoted in* Cary et. al., Fed. Criminal Discovery *supra* note __ at 4.

[195] The prosecution carries heightened burdens of production and persuasion as compared either to the accused or to the plaintiff in a civil case. Posner, *An Economic Approach to Evidence*, at 1502-07.

[196] *See, e.g.*, United Stated v. Garsson, 291 F. 646, 649 (S.D.N.Y. 1923) (Hand, J.), *quoted in* Cary et. al., Fed. Criminal Discovery *supra* note __ at 2-3.

[197] *See, e.g.*, William J. Brennan, Jr., *The Criminal Prosecution: Sporting Event or Quest for Truth?*, 1963 Wash. U.L.Q. 279 (1963).

deceive witnesses; or may encourage witness testimony by offering monetary and other benefits.[198] Defendants may not do the same.[199] Prosecutors may effectively depose witnesses by convening a grand jury investigation. Defendants have no such means available.[200] The disparity in resources between the state and an individual accused creates additional perversities. Prosecutors may draw on the full investigative powers of the state, choose whom to indict, and focus government resources on a single trial.[201] Legal scholar Paul C. Giannelli has repeatedly argued that narrow criminal discovery has particularly perverse effects for the adversarial review of expert evidence.[202]

Reflecting these critiques, the classic, narrow understanding of criminal discovery began to shift by 1946 with the adoption of Rule 16 of the Federal Rules of Criminal Procedure, which first provided the defense some minimal rights of access to information about the government's case.[203] The Jencks Act of 1957 later required the government to disclose prosecution witnesses' prior statements, but not until after the witness has testified at trial.[204] *Brady v. Maryland* held in 1963 that the government has a constitutional obligation to disclose exculpatory or material information to the defense.[205] Subsequent discovery reforms have slowly increased access and also imposed reciprocal disclosure requirements on the defense.

---

[198] Cary et. al., Fed. Criminal Discovery *supra* note __ at 5.

[199] *Id.*

[200] Sklansky, *Comparative Law Without Leaving Home*, at 714; Andrew D. Leipold, *Why Grand Juries Do Not (And Cannot) Protect the Accused*, 80 CORNELL L. REV. 260, 314-17 (1995).

[201] *See, e.g.*, Posner, *An Economic Approach*, at 1505 ("The government has enormous prosecutorial resources. It can allocate these across cases as it pleases, extracting guilty pleas by threatening to concentrate its resources against any defendant who refuses to plead and using the resources thus conserved to wallop the occasional defendant who does invoke his right to a trial.").

[202] *See, e.g.*, Paul C. Giannelli, *Pretrial Discovery of Expert Testimony*, 44 CRIM. L. BULL. 7 (2008). *See also*, Erin Murphy, *supra* note__at 751 (noting that "[s]tatutory protections and rules of discovery protect the government's source materials and raw data in specific cases"); NATIONAL COMM'N ON FORENSIC SCI., PRETRIAL DISCOVERY IN FORENSIC EVIDENCE CASES: Policy Recommendation 1-2 (2015) [hereinafter Pretrial Discovery]; *Full Text: Judge's Protest Resignation Letter*, WASH. POST (Jan. 29, 2015).

[203] Cary et. al., *supra* note __ at 2. Most states have followed suit but some still maintain exceptionally narrow criminal discovery statutes. *See, e.g.*, John Schoeffel, THE LEGAL AID SOCIETY, CRIMINAL DISCOVERY REFORM IN NEW YORK (April 1, (2009).

[204] 18 U.S.C 657 (1957).

[205] 373 U.S. 83 (1963). Numerous commentators have argued that *Brady* no longer works because it does not apply to pre-trail proceedings and there is a history of *Brady* violations. *See* Judge Alex Kozinski.

But despite this gradual evolution towards broader criminal discovery, Rule 16 today remains sufficiently restrictive to protect trade secrets from wrongful disclosure without resort to a privilege. It imposes three main limits on disclosure, which I refer to as materiality restrictions; summarization restrictions; and good cause restrictions. First, upon request by the defense, the government must disclose only those documents in its possession that are "material to preparing the defense."[206] As a result, any trade secrets privilege that applies during discovery will necessarily apply to relevant evidence. Unlike civil parties who may access broad categories of documents and then sift through them to determine what to use in a case, criminal defendants cannot obtain immaterial information during discovery.[207] Defendants also carry a substantial burden to establish materiality. They must make a "prima facie" showing" that the information sought has "some abstract logical relationship to the issues."[208] This showing requires more than a "general description of the material sought," and it must not be based on "conclusory" arguments about materiality.[209] While courts have described the threshold showing as "not a heavy burden,"[210] it does require enough specificity to avoid claims that the accused has gone on a 'fishing

---

[206] Fed. R. Crim. P. 16(a)(1)(E).

[207] *Compare* Civ. P. Rule 26 *with* Crim. P. Rule 16. While most courts interpret Rule 16 'materiality' to extend beyond the *Brady* due process minimum requirement that prosecutors disclose known exculpatory information, the materiality standard is still limited in scope. For example, 'materiality' only reaches information that may assist the defense in preparing a 'shield' against the government's case-in-chief, not information that might help defendants to prepare a "'sword,' challenging the prosecution's conduct of the case." 'Materiality' covers only information that is either admissible as evidence or "will lead to the discovery of admissible evidence." Both inculpatory and exculpatory evidence is included, but impeachment materials are not. And 'materiality' may extend to the underlying data and methodology for a scientific test, but only if the government has produced the results of that test under related Rule 16(a)(1)(F). Some courts narrow the materiality standard further still to track the due process minimum of *Brady*. This in turn limits discovery to evidence that would be exculpatory when considered in light of the overall result of a trial, narrows pretrial access, and excludes pretrial plea negotiations altogether. *See* Cary et. al., Fed. Criminal Discovery *supra* note __ at 95-96.

[208] United States v. Ross, 511 F.2d 757, 762 (5th Cir. 1975);.

[209] United States v. Cadet, 727 F.2d 1453, 1466 (9th Cir. 1984); United States v. Carrasquillo-Plaza, 873 F.2d 10, 13 (1st Cir. 1989).

[210] United States v. George, 786 F. Supp. 56, 58 (D.D.C. 1992); United States v. Burr, 25 F. Cas. 187, 191 (C.C.D. Va. 1807) (Marshall, J.) (asking "what statement of [a document's] contents or applicability can be expected from the person who claims its production, he not precisely knowing its contents?"); Fed. R. Crim. P. 16, 1974 Advisory Committee Note ("It may be difficult for a defendant to make this showing if he does not know what the evidence is.").

expedition.' Applying a trade secrets privilege here will raise the preexisting burden further still.[211]

Second, Rule 16 also includes what I call "summarization restrictions," or discovery obligations that the government can fulfill by mere summary rather than by disclosing original documents. For instance, Rule 16(a)(1)(G) obliges the government upon request to disclose only a summary of any expert opinion testimony that it intends to introduce. The summary disclosure can be satisfied by a general description of an expert's underlying methodology.[212] The summarization option limits defense access to in-depth, unfiltered information without any privilege claim. In theory, criminal discovery disclosures must suffice to allow the defense to prepare for cross-examination.[213] But critics have argued that, in practice, such disclosures are inadequate to this preparation. For instance, in August of 2015 a Department of Justice and National Institute for Standards and Technology commission recommended expanding pretrial criminal discovery in order to help ensure that defense attorneys could adequately prepare to challenge potentially invalid or unreliable forensic evidence.[214] Members of the Commission were adamant that expanding

---

[211] Note that some states and individual prosecutors have adopted 'open file' discovery, meaning that the government provides the defense with a wide array of materials without requiring a showing that they qualify. There, defendants may receive immaterial information during discovery. In those cases, my argument about discovery would not apply.

[212] To be sure, this summary must include specific elements, such as "the bases and reasons for [the expert's] opinions," *see* Fed. R. Crim. P. 16(a)(1)(G); an identification of any documents or information that the expert reviewed; a description of the function of any experimental tests that the expert performed; and a description of any other information "that might be recognized as a legitimate basis" for the expert's opinion. *See* Fed. R. Crim. P. 16, 1993 advisory comm. notes. Rule 703 permits expert witnesses to base their opinion testimony on otherwise inadmissible "facts or data," provided that "experts in the particular field would reasonably rely on those kinds of facts or data in forming an opinion on the subject." The Rule 16(a)(1)(G) advisory committee note shows that this permissive 703 admissibility standard relies on, rather than precludes, "advance discovery" by opposing counsel in order to facilitate cross-examination. United States v. Mehta, 236 F. Supp. 2d at 157, n.4. *See also*, Cary et. al, *supra* note__; Paul C. Giannelli; NAS ADVISORY ON DISCOVERY REFORM (2016).

[213] The Rules Advisory Committee was particularly concerned with enabling discovery of the bases of expert opinions that "touch on new or controversial techniques . . . ." See Fed. R. Crim. P. 16(a)(1)(G),1993 advisory committee's notes. *See also*, Cary et. al., Fed. Criminal Discovery *supra* note __ at 125, citing *Day*, 524 F.3d at 1372. Note confusion re: its relationship with Daubert.

[214] NATIONAL COMM'N ON FORENSIC SCI., PRETRIAL DISCOVERY IN FORENSIC EVIDENCE CASES: POLICY RECOMMENDATION 1-2 (2015) [hereinafter PRETRIAL DISCOVERY].

defense access to information about forensic evidence, and granting this access earlier in the pretrial process, are essential steps to prevent the introduction of faulty forensics into trials.[215] In their appraisal, Rule 16(a)(1)(G) summary disclosures do not provide sufficient information to serve this crucial function.[216] Recognizing a trade secrets privilege here will only aggravate these existing disparities.

Third, beyond the materiality burden on defense requests and the power of prosecutors to deflect certain disclosures into mere summaries, trial courts also have broad discretion to prevent abusive, frivolous, or harassing discovery requests. Rule 16(d)(1) grants the district court discretion "for good cause [to] deny, restrict, or defer discovery or inspection, or grant other appropriate relief,"[217] including nondisclosure orders.[218] This additional guarantee applies explicitly to protect "business enterprises from economic reprisals."[219] A court may find "good cause" on its own, without any required showing by the parties, and subject only to abuse of discretion review.[220] Alternately, a moving party may make an ex part submission to the court requesting a "good cause" limit on its disclosure obligations.[221] The rule is designed to protect against abuse of discovery.[222] It guarantees against unnecessary and harmful trade secrets disclosures without resort to any privilege claims.

---

[215] Indeed, Judge Jed S. Rakoff of the Southern District of New York temporarily resigned in protest when it appeared that pretrial discovery reforms might be overlooked. Judge Rakoff rejoined once it became clear that the Commission would address pretrial discovery issues. Spencer S. Hsu, *Judge Rakoff Returns to Forensic Panel After Justice Department Backs off Decision*, WASH. POST (Jan. 30, 2015).

[216] Note that Rule 16(a)(1)(G) disclosures may be narrower than those required for a *Daubert* challenge. United States v. Nacchio, 519 F.3d 1140, 1151 (10th Cir. 2008); Margaret A. Berger, *Procedural Paradigms for Applying the* Daubert *Test*, 78 Minn. L. Rev. 1345, 1360 (1994).

[217] Fed. R. Crim. P. 16(d)(1); Taylor v. Illinois, 484 U.S. 400, 415 n.20 (1988), *cited in* Cary, et. al.

[218] Alderman v. United States, 394 U.S. 165, 185 (1969), *cited in* Cary et. al.

[219] Fed. R. Crim. P. 16, 1966 advisory committee's notes. See also 1974 advisory notes (good clause includes "reason to believe that a witness would be subject to physical or economic harm").

[220] *See* Klein v. Crawford, No. 3:04CV00049, 2006 WL 3833328, at *2 (D. Nev. Dec. 27, 2006); United States v. Annabi, No. 10 Cr. 7, 2010 WL 1253221, at *1 (S.D.N.Y. Mar. 24, 2010); United States v. Delia, 944 F.2d 1010, 1018 (2d Cir. 1991); United States v. Tindle, 808 F.2d 319, 323-24 (4th Cir. 1986), *cited in* Cary et. al.

[221] Fed. R. Crim. P. 16(d)(1).

[222] Fed. R. Crim. P. 16, 1966 advisory committee's notes.

B. Subpoenas

Baked-in procedural limits on criminal subpoenas are even more restrictive than their discovery counterparts, and can guard against inappropriate requests for trade secrets. To obtain a criminal subpoena, the moving party must make a preliminary showing of relevance; of admissibility; and of specificity for the information sought.[223] The relevancy showing is lenient. It tracks Federal Rule of Evidence 401, which defines relevant evidence as "evidence having a tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." [224] But to satisfy the admissibility requirement, the moving party must show that the subpoenaed information itself is directly likely to be evidentiary. That is, mere likelihood that the information will lead to the discovery of other admissible evidence is not enough.[225]

Meeting such a high standard to establish admissibility can be particularly difficult pretrial, when a defendant's theory of the case has not fully developed. To help assuage that difficulty, some courts have interpreted the third prong of the test—the specificity requirement—leniently, finding it to be continuous with a showing of relevance and admissibility.[226] Other courts have taken a more stringent view, requiring an additional showing of what the materials are likely to contain.[227] Regardless, the subpoena must be made "in good faith" and cannot be designed as a "fishing expedition."[228] Parties moving for a pretrial subpoenas must satisfy yet another burden to show that it is necessary to access the documents before trial begins.[229] Finally, as with the "good

---

[223] United States v. Nixon, 418 U.S. 683, 700 (1974).

[224] Fed. R. Evid. 401. *See* Cary et. al., Fed. Criminal Discovery *supra* note __.

[225] United States v. Nixon, 418 U.S. 683, 700-01 (1974); United States v. Shinderman, 432 F. Supp. 2d 157, 159 (D. Me. 2006) ("Rule 17 applies only to admissible *evidence*, not to materials that might lead to discovery of exculpatory evidence."). *See* CARY ET. AL., *supra* note __.

[226] *See* United States v. Libby, 432 F. Supp. 2d at 31 ("[I]t will often be difficult at the pretrial stage to determine with precision the admissibility of certain documents; therefore, if a document is arguably relevant and admissible under the Rules of Evidence, the *Nixon* 'evidentiary' requirement is likely satisfied."). *See* Cary et. al., Fed. Criminal Discovery *supra* note __.

[227] *See* United States v. Caro, 597 F.3d 608, 620 (4th Cir. 2010); Cary et. al., Fed. Criminal Discovery *supra* note __, at 228-29.

[228] *United States v. Iozia*, 13 F.R.D. 335, 338 (S.D.N.Y. 1952) (cited in United States v. Nixon, 418 U.S. 683, 699-700 (1974)).

[229] United States v. Vanegas, 112 F.R.D. 235, 239 (D.N.J. 1986). The factors as outlined in *United States v. Iozia*, are that the documents are: (1) "not otherwise

cause" restrictions on criminal discovery, courts have discretion to "quash or modify [a] subpoena if compliance would be unreasonable or oppressive."[230]

In sum, trade secret information that is not sufficiently likely to produce relevant and admissible evidence is not subject to subpoena, privilege or no. And even evidence that would be admissible will not be subject to subpoena, especially pretrial, unless defendants meet a slew of other challenging hurdles.

C. Protective Orders

Beyond even the limits on criminal discovery and subpoenas, courts can grant additional remedies to mitigate any legitimate risk from the disclosure of trade secret evidence to the defense' courts may bind the parties with nondisclosure orders and seal the records from public view. In extreme cases, they can limit disclosure to opposing counsel or opposing experts, to a court appointed special master, or even to the judge alone via in camera review. Ordering that trade secrets be disclosed subject to a protective order is routine practice in civil cases.[231] Even in the controversial context of public disclosure of toxic torts issues, there has not been a significant problem exposing that sensitive commercial information to the opposing party. Indeed, in advocating to *exclude* the public from these proceedings via docket sealing, legal scholar Arthur Miller has argued that public access and party access are inversely related.[232] And in criminal cases for trade secrets misappropriation, where the defendant is highly likely to be a direct business competitor to a non-party trade secret holder/victim, protective orders are a standard

---

procurable reasonably in advance of trial by exercise of due diligence"; and (2) "the party cannot properly prepare for trial without such production and inspection in advance of trial and that the failure to obtain such inspection may tend unreasonably to delay the trail."

[230] Rule 17(c)(2).

[231] *See, e.g.*, Fed. Open Mkt. Comm. of Fed. Reserve Sys. v. Merrill, 443 U.S. 340, 362 n.24 (1979) ("Actually, orders forbidding any disclosure of trade secrets or confidential commercial information are rare. More commonly, the trial court will enter a protective order restricting disclosure to counsel. . . ."). *See also*, Dustin B. Benham, *Proportionality, Pretrial Confidentiality, and Discovery Sharing*, 71 WASH. & LEE L. REV. 2181, 2251 (2014).

[232] *See, e.g.*, Arthur R. Miller, *Private Lives or Public Access?*, ABA J., August 1991, at 64, 66 ("Wide-angle discovery is central to contemporary civil litigation, and provides the litigants with equal access to all relevant data. But that does not make discovery a public process . . . .").

remedy.[233] Perhaps, then, the trade secrets privilege in criminal cases should be limited to a protective order remedy and nothing more.[234]

Prosecutors have argued against this default solution by voicing concern that a defendant's counsel or experts will themselves steal the trade secret.[235] But disclosure determinations—whether they implicate constitutional rights or mere policy choices—should not hinge on the presumption that defense attorneys, or the experts they hire, are willing to commit crimes. Moreover, this type of risk is at its peak in cases where the parties are direct business competitors, such as misappropriation suits. In criminal misappropriation cases—arguably the highest risk scenario—the privilege is almost always unavailable anyway because the trade secret information is core evidence in the case.[236] In comparison, any risk of theft via judicially compelled disclosure must be diminished in other kinds of criminal cases, where the defendant is less likely to be the business competitor of a forensic device manufacturer; there is less of an issue with co-optation or abuse of the judicial system as a device for business to attack their competitors.

True, defense experts will likely seek to challenge validity, reliability, or some other element of the trade secret information. But adversarial scrutiny, cross-examination and confrontation are not business competition. Finally, concerning forensic technologies in particular, trade

---

[233] *See*, *Your Secrets are Safe with us*, at 480 (detailing common types of pre-indictment, post-indictment, and post-conviction protective orders in federal prosecutions for trade secrets theft under the EEA, and noting that the offer strict controls of *who* gets access, whether defense counsel only or a limited selection of defense experts who are non-competitors to the trade secrets holder, but not contemplating that the defense would be barred access altogether). *See also*, 2010 WL 5158125 (limiting public access to the courtroom during a trial for criminal misappropriation of a trade secret).

[234] This is how Chubbs' counsel interpreted California's Evidence Code.

[235] *See Johnson* re FST source code.

[236] Commentators have noted that the Government often relies on Rule 16(d) protective orders to prosecute criminal trade secrets misappropriation cases while protecting the trade secret itself from *public* disclosure, and that parallel protections work well in civil cases. *See, e.g.*, Brian L. Levine & Timothy C. Flowers, *Your Secrets are Safe with us: How Prosecutors Protect Trade Secrets During Investigation and Prosecution*, 38 Am. J. Trial Advoc. 461, 466-67 (Spring 2015) (citing Hsu). The concern that victims won't cooperate with law enforcement prosecution of criminal trade secrets theft largely centers on concern that the trade secrets information will be *publically* disclosed, not that it will be disclosed to defense attorneys or experts subject to a protective order. *See*, HR Rep. No. 104-788, at 16 (1996) (supporting the enactment of Section 1835 of the EAA in order to address companies hesitation "to cooperate in prosecutions for fear of further exposing their trade secrets to public view, thus further devaluing or even destroying their worth"), *quoted in*, *Your Secrets are Safe with us.*

secrets holders have voluntarily entered a market that serves the needs of the criminal justice system. Waiver of any trade secret privilege claim could even be implied by the owner's decision to enter the forensic science industry and sell her product to government crime laboratories.

It is also true that, at some point, the defense community might seek to override protective orders and share trade secret information with each other in an attempt to pool resources to better understand and rebut complex forensic evidence.[237] Legal scholar Erin Murphy has pointed out that, due to resource and caseload constraints as well as to the decentralized nature of criminal defense work and strategic trade-offs in individual cases, it is often not feasible for defense attorneys to challenge the underlying methodologies of technologically complex forensic science methods.[238] As a result, she proposes a centralized, neutral, national oversight "Board" that would have funding and "access to all private or proprietary data related to a particular technique,"[239] and that could grant limited access to appropriate researchers to answer generalizable questions about a forensic methodology and make the research "available on a broad basis, to the benefit of defendants as a class."[240] That proposal was well thought through, and hopefully we will accomplish it soon.[241] In the meantime, disclosure subject to a protective order is better than no disclosure at all.

V. PREEMPTING THE INNOVATION CONCERN

The strongest argument against my position that no trade secrets

---

[237] *Cf.* Jonathan Abel, *Brady's Blind Spot: Impeachment Evidence in Police Personnel Files and the Battle Splitting the Prosecution Team*, 67 STAN. L. REV. 743 (2015).

[238] Murphy, *supra* note__at 761-62.

[239] *Id.*, at 778.

[240] *Id.*, at 783-84.

[241] *See,* Obama, *Criminal Justice Reform*, Harv. L. Rev. (Jan. 2017). A number of steps have been taken in the direction of implementing Murphy's vision. For instance, the White House Office of Science & Technology Policy Subcommittee on Forensic Science, chartered as a result of the National Academy of Sciences Report, has proposed centralized, universal accreditation, certification, and proficiency testing for forensic practitioners as well as a national code of ethics for forensic providers. NATIONAL SCIENCE AND TECHNOLOGY COUNCIL COMMITTEE ON SCIENCE SUBCOMMITTEE ON FORENSIC SCIENCE, STRENGTHENING THE FORENSIC SCIENCES (2014). And in 2013, the DOJ and the National Institute for Standards and Technology established a national commission "to enhance the practice and improve the reliability of forensic science." Department of Justice, NATIONAL COMMISSION ON FORENSIC SCIENCE (last visited July 24, 2015), http://www.justice.gov/ncfs.

privilege should apply to criminal proceedings is the contention that, without privilege protections, developers will not create robust criminal justice technologies.[242] This is a deeply troubling concern. We need accurate and reliable methods for criminal justice decision-making to protect the safety of our communities, to identify the true perpetrators of crimes, to exonerate the wrongly accused, and to achieve just outcomes for those who have made mistakes.[243]

The need for robust technologies is particularly urgent in the forensic sciences. Unvalidated and unreliable forensic evidence is undermining criminal trials. In 2009, a National Academy of Sciences report identified a, "dearth of peer-reviewed, published studies establishing the scientific bases and validity of many forensic methods," and noted that numerous forensic disciplines lack known accuracy measures or error rates.[244] More recent studies have questioned the scientific foundation of bite mark, arson, hair and fiber evidence, ballistics, blood spatter evidence, shaken baby syndrome diagnoses, and even DNA and fingerprint analysis.[245] In September 2016, President Obama's Council of Advisors on Science and Technology published a report finding a gap in "the need to evaluate specific forensic methods to determine whether they have been scientifically established to be valid and reliable."[246]

But, as this Article has shown, secrecy has been the *status quo*, and it

---

[242] *See, e.g.*, People v. Robinson, (Pa. 2016) (expressing concern that if the judge were to order disclosure of the source code for the TrueAllele genotopying software, companies like Cybergenetics would no longer invest in developing forensic technologies).

[243] Obama, *supra* note __.

[244] COMM. ON IDENTIFYING THE NEEDS OF THE FORENSIC SCIENCES COMMUNITY, STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 8 (2009) [hereinafter STRENGTHENING FORENSIC SCIENCE].

[245] *See, e.g.*, Alex Kozinski, *Criminal Law 2.0*, 44 GEO. L.J. ANN. REV. CRIM. PROC. iii, v (2015) ("[F]ields of forensic expertise, long accepted by the courts as largely infallible . . . have been the subject of considerable doubt."); Debbie Cenziper, *Prosecutors Build Murder Cases on Disputed Shaken Baby Syndrome Diagnosis*, WASH. POST (Mar. 20, 2015), http://www.washingtonpost.com/graphics/investigations/shaken-baby-syndrome ("Testing has been unable to show whether violent shaking can produce the bleeding and swelling long attributed to the diagnosis . . . ."). Yet courts continue to uphold the validity and admissibility of much of this evidence. Radley Balko, *Seventh Circuit Grants Immunity to Bite Mark 'Experts' who put Innocent man in Prison for 23 Years*, WASH. POST THE WATCH (Sept. 8, 2015), https://www.washingtonpost.com/news/the-watch/wp/2015/09/08/seventh-circuit-grants-immunity-to-bite-mark-experts-who-put-innocent-man-in-prison-for-23-years ("[T]he very quackery of the field protects its practitioners from liability.").

[246] PCAST report, *supra* note__, at x.

has not saved us from the current state of affairs. This Part considers the underlying theoretical rationales for both substantive trade secrets law and evidentiary privileges, including innovation-based arguments. I show why neither justifies recognizing a trade secrets privilege in criminal cases.

A. Rationales for Trade Secrets

What counts as a trade secret varies by jurisdiction, but the general requirements are as follows: To qualify, a secret must concern information that is not generally known or readily ascertainable to industry competitors;[247] the secret holder must take reasonable precautions to prevent its disclosure;[248] and the information itself must confer some economic value or competitive advantage.[249] Even when a trade secret is valid under this test, the law does not protect against *any* acquisition of the secret by competitors; rather, only an *improper* one. Thus, while theft, deceit, and "skullduggery" count as misappropriation, independent discovery and reverse engineering do not. If a direct competitor dismantles a product and uncovers the secret, no cause of action exists.[250] Indeed, some states prohibit the government from claiming any trade secrets at all because—the argument goes—the government has no business competitors and thus derives no economic value from secret know-how.[251]

Trade secrets are one solution to the problem underlying intellectual property more generally: because knowledge is nonrivalrous, markets tend to under-produce it.[252] Intellectual property law seeks to address that problem by granting rights to exclude others from knowledge gains.[253]

---

[247] *See, e.g.*, United States v. Hsu, 155 F.3d 189, 196 (3d Cir. 1998) (noting that the UTSA § 1(4) definition of a trade secret requires that it "cannot be generally known by businesspersons or competitors," while the EEA requires that a trade secret "must not be generally known to, or readily ascertainable by, the general public").

[248] *See, e.g.*, Learning Curve Toys, 433 F.3d 952 (7th Cir. 2006) (finding that a trade secret is any information protected in such a way "that the only way the secret can be unmasked is by a breach of contract or a tort")

[249] *See, e.g.*, Metallurgical (5th Cir. 1986) (upholding protection for a secret modification of a generally known process for furnace construction). See also, Latest Fed Stat, Erica cites; EEA 1831/1832; Defend trade secrets act; Uniform Trade secrets Act, 1985 Amendments (UTSA); GATT/TRIPS; Restatement of Torts §757, 758 (1939); FOIA; different state definitions.

[250] *See, e.g.*, Lemley, *supra* note__ at 317-19.

[251] Also see limits on TS protections in human rights/IP context.

[252] Menell, at 1475.

[253] For a helpful overview of a classic account of Intellectual Property Law and its rationales, see A. Mitchell Polinsky & Steven Shavell, eds., 2 HANDBOOK OF LAW AND ECONOMICS 1476-79 (2007);

Utilitarians, often associated with property-like theories of trade secrets,[254] argue that trade secret protections encourage investment in innovation, which generates net knowledge gains over time.[255] To be sure, individuals may suffer dead weight losses in the short-term, but society in the aggregate loses little from a trade secrets regime. Commercial morality or tort-like theories of trade secrecy focus instead on business ethics. This perspective views the law as deterrence for wrongful acts and dignitary violations that might otherwise go unpunished under traditional common law torts or a pure contracts or property regime.[256]

The merits, or lack thereof, of the various justifications for trade secrets law have provoked heated scholarly debate. To give just a taste, legal scholar Mark Lemley challenges that, first, any justification for trade secrets doctrine based in real property law fails because, unlike property in land or chattel, the law grants trade secrets owners the right to control information even when they no longer possess it.[257] Second, tort theories fail when the 'duty' that has been breached is merely contractual; breaching a contract is not a crime, but trade secrets misappropriation triggers both civil and criminal liability.[258] If instead the 'improper means' that constitute misappropriation are already illegal, such as hacking or trespass, then trade secret law is redundant.[259] Considering the redundancy, legal scholar Robert Bone concludes that any cause of action that trade secrets law affords above and beyond existing contract and tort protections is incoherent and unjustified, and thus no trade secrets protections should exist at all.[260]

However, even assuming that substantive trade secrets law is theoretically sound, it is also in some ways a particularly costly form of

---

[254] Lemley, *supra* note__ at 326 ("Treatment of trade secrets as property rights vested in the trade secret "owner" is consistent with a view of trade secret law as providing an additional incentive to innovate beyond those provided in patent law.").

[255] *See, e.g.*, Peter S. Menell & Suzanne Scotchmer, Intellectual Property Law 1475, *in* A. Mitchell Polinsky & Steven Shavell, 2 Handbook of Law and Economics (2007) ("The principal objective of intellectual property [including trade secrets] law is the promotion of new and improved works—whether technological or expressive.").

[256] *See, e.g.*, Lemley, *supra* note__ at 319-28; 327. I'm lumping the tort theories with the commercial morality theories. Explain.

[257] Lemley, *supra* note__ at 325-26.

[258] *Id.*, at 321.

[259] *Id.*, at 321.

[260] Robert G. Bone, *A new Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241 (1998). *See also*, WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 355 (2003). As *cited in* Lemley, *supra* note__.

intellectual property. One concern is that excessive trade secrets protections will conflict with other rights and interests, such as First Amendment free speech protections.[261] Other concerns are innovation-based. Patents and copyrights offer time-limited protections that also incentivize the disclosure and circulation of new ideas. Trade secrets law, in contrast, encourages secret holders to lock up their inventions for as long as possible. In doing so, trade secrets create a risk of perpetual monopolies that impede the free flow of information and obstruct downstream or 'cumulative' innovation. Particular to data and technology-related, diverse commentators from scientists to legal scholars have voiced concerns that excessive secrecy has begun to interfere with both the quantity and the quality of intellectual innovation.[262]

Most relevant to the present discussion, trade secrets law exists somewhere in between a regime of total secrecy and one of no secrecy. Despite its name, a number of scholars have pointed out that trade secrets law actually promotes the disclosure and dissemination of information.[263] Truly secret information needs no legal protection but is expensive to maintain, both in terms of costs of infrastructure and costs to innovation. Trade secrets law helps to alleviate over-investment in alternative forms of secrecy protections that would otherwise stymie the flow of broad swaths of information and skilled individuals.[264] For instance, it enables innovators to offer ideas for sale without destroying the value of the secret in the bargaining process.[265] Simply put, trade secrets law offers more efficient and targeted control over confidential information than pure secrecy alone.

The idea that trade secrets law exists, at least in part, to facilitate controlled disclosures in certain important scenarios suggests that the law should also perform this service in criminal proceedings. If industry may enjoy the benefits of trade secrets-protected disclosures, so too should those defending life or liberty.

---

[261] *See*, Pam Samuelson; Dierdre Mulligan; Rochelle C. Dreyfuss & Katherine J. Strandburg, Eds., *The Impact of Trade Secrecy on Public Transparency*, in THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH (2010).

[262] *See, e.g.*, Amy Kapczynski.

[263] Lemley, *The Surprising Virtue* 61 STAN. L. REV. 311, 312, 332-37 (2008). *See also* Kitch, Friedman, Landes, and Posner.

[264] Lemley, *supra* note__ at 334-35 (citing E.I. du Pont de Nemours v. Christopher).

[265] Lemley, *supra* note__ at 336 (discussing Arrow's Information Paradox).

B. Rationales for Evidentiary Privileges

Evidentiary privileges pit truth seeking against competing values. They exist, at base, to exclude relevant evidence. Privileges are anti-accuracy, anti-transparency, and often unfair. They produce 'unknown unknowns'; with the attorney-client privilege, for instance, parties denied access to privileged communications may not realize that anything relevant is missing, much less know precisely what was denied. A party may lose their case as a result, no matter how righteous their claim nor inequitable the outcome. Privilege law trades off these harms in the name of honoring certain intimate relationships, such as with our spouses, therapists, attorneys, or spiritual counselors.[266]

Legal scholar Edward Imwinkelried has developed a thorough intellectual history of utilitarian and humanistic theories of privilege. As he describes, utilitarians argue that, in the long run, evidentiary privileges cause merely a de minimis loss of relevant evidence because, without privilege protections, people would not disclose the information at issue in the first place.[267] In other words, without privileges, the threat of future compelled disclosure in court would chill intimate communications, even to our most trusted confidants. As a result, there would be nothing left to discover or subpoena. This perspective requires no particular normative view about whether the communications that would otherwise be chilled are good or bad. It simply depends on the idea that they would in fact be chilled—hence unavailable as evidence—so a privilege imposes no real cost to accuracy. The utilitarian view thus harmonizes privilege law as much as possible with truth-seeking objectives. At least in aggregate if not in individual cases, it premises the recognition of a privilege on the theory that the information would not otherwise have existed.[268]

Humanists are more tolerant of the losses that privileges impose, and thus friendlier to their expansive application. This perspective presumes—

---

[266] Privileges are so anathema to fact finding that some theorists resist classifying them as Rules of Evidence at all. *See*, Stein, *Implications for Evidence Theory*, ___, n.47 ("Because privileges protect substantive confidentiality entitlements, they are properly categorized as belonging to substantive law rather than the law of evidence."). I disagree with this assessment. That privileges are a part of Evidence law that limit fact-finding simply means that Evidence Law incorporates principles of self-constraint.

[267] See, e.g., Fisher v. United States, 425 U.S. 391, 403 (1976) (A privilege "protects only those disclosures . . . which might not have been made absent the privilege.").

[268] Edward J. Imwinkelried, *Non-Constitutional Quasi-Privileges*, *in* THE NEW WIGMORE: EVIDENTIARY PRIVILEGES § 3.2.3 (2016).

and accepts—that evidentiary privileges cause significant exclusions of relevant evidence, but finds that competing values justify those losses. Limiting judicial intrusion into particularly significant relationships of trust and intimacy, the argument goes, should outweigh even a loss to truth-seeking. Adopting this view requires no behavioral assumptions about whether, without privilege protections, the communications at issue would be chilled. It simply depends on the idea that some communications are so inherently valuable that they should be privileged no matter the cost to accuracy. Imwinkelried himself argues that modern courts should return to a humanistic perspective.[269]

These existing theories of privilege, while compelling, do not distinguish between how evidentiary rules operate in the vastly divergent structural and procedural environments of civil and criminal proceedings. To begin to develop a theory of privilege that does take these differences in to account, it will be useful to turn to constitutional theory. Legal scholar Akil Reed Amar's theory of "compulsion parity" offers an alternative, under-examined rationale for privileges in criminal cases in particular: structural checks and balances.[270] The Sixth Amendment grants each criminal defendant the right "to have compulsory process for obtaining witnesses in his favor."[271] Amar places this constitutional clause in a longstanding Anglo-American legal tradition granting subpoena parity to the accused.[272] He highlights concerns over "asymmetry" in the Supreme Court's Sixth Amendment jurisprudence.[273] And he concludes that defendants should have access to equal—not greater—compulsion powers as the government.[274] Privileges that deny criminal defendants access to relevant evidence are thus acceptable as long as they also bar the

---

[269] Imwinkelried, at § 2.3. See also Imwinkelried, at § 5.1.2 ("[I]t is desirable to create certain privileges out of respect for personal rights such as autonomy or [information] privacy."). Imwinkelried advocates an autonomy based (decisional privacy) rationale for the privileges, rather than an information privacy based justification. Imwinkelried, at § 5.3.1.

[270] Akhil Reed Amar, *Sixth Amendment First Principles*, at 699. *See also,* Akhil Reed Amar, *Fourth Amendment First Principles*, at 765-66, 779-80 (arguing that defendants' subpoena powers should match law-enforcements' warrant powers).

[271] U.S. CONSTITUTION AMENDMENT VI.

[272] Amar, *Sixth Amendment*, *supra* note__ at 699 (citing founding-era authorities that granted defendants "like" or "same" compulsory process rights as the government).

[273] Amar, *Sixth Amendment*, *supra* note__ at 699, n.229 (citing a series of SCOTUS cases that struck asymmetric evidence rulings as due process violations, and also citing Pennsylvania v. Ritchie, 480 U.S. 39, 57 & n.14 (1987), which rejected the government's claim that a state statutory privilege permitted law-enforcement access to sensitive information but barred defendants' access to the same).

[274] Amar, *Sixth Amendment*, *supra* note__ at 699.

government's access to the same type of information.[275] As articulated by Amar, when the government forsakes "all coercion against certain highly valued social relationships of intimacy and trust (like the one between wife and husband), this self-denial proves that the government really does see a 'compelling interest' against compulsion."[276] Put another way, according to this theory, the requirement of "compulsion parity" will cause the government's own self-restraint to check the scope of privilege exclusions.

Amar's model of checks and balances works beautifully if, in aggregate over time, privileges tend to handicap government investigations as much as those by the defense. This may well be the case for what Amar calls the "true privacy privileges," meaning privileges for intimate relationships such as those between spouses.[277] But the model will falter if the government's incentives to seek out certain types of information systematically differ from those of criminal defendants. If, for instance, a particular category of evidence is likely to weaken the government's case, then recognizing a privilege to protect the secrecy of that type of information is hardly "self-denial."

As Erin Murphy has pointed out, investigative and forensic tools and methods embody precisely such a 'differential incentives' scenario. By implementing these tools and methods in the first place, the government becomes invested in their validity and reliability. A state agency that adopts a risk assessment algorithm or probabilistic genotyping software has already decided, according to its own evaluative standards, that the tool works; the agency has weak incentives to seek out additional information about possible methodological errors or technical vulnerabilities. In sharp contrast, individuals who become the targets of these tools and methods will have had no prior opportunity to evaluate their efficacy, and will be highly motivated to scrutinize the tools for any fault. [278] Privileges that restrict access to information about investigative and forensic technologies will thus systemically aid the government and harm criminal defendants.

Reading Amar and Murphy's work together, then, gives rise to a new

---

[275] *Id.*

[276] *Id.*

[277] Amar, *Sixth Amendment*, *supra* note__ at 699 (distinguishing "true privacy privileges—doctor-patient, spousal, and priest-penitent," from the Fourth Amendment exclusionary rule).

[278] *See, e.g.*, Murphy, *supra* note__ (explaining that the government will have minimal incentive to challenge the validity of forensic methods once adopted).

institutional theory of evidentiary privileges for criminal cases in particular. Constitutional criminal procedure creates a system of checks and balances for many privileges, but not all. When the government's and criminal defendants' incentives for seeking out certain categories of information systematically differ, privileges that restrict access to that particular type of evidence should be suspect as either over- or under-protective. Trade secrets are one such scenario, and thus they should not be privileged in criminal proceedings.

CONCLUSION

This Article has made the case against recognizing a trade secrets privilege in criminal cases. Not only is such a privilege harmful when current standards are applied wholesale from civil to criminal proceedings, but the application of the privilege in criminal contexts is a relatively recent and unnecessary development. Recognizing a trade secrets privilege in criminal proceedings suggests that private actors have a right to own the very means by which the government decides criminal justice outcomes, and implies that the adversarial process is itself a business competition. Courts and legislatures should decline to privilege trade secrets evidence in criminal cases.

More broadly, this Article raises the issue of how evidence rules function differently in civil and criminal cases. A mid-Twentieth Century movement for uniform laws led the federal courts and most states to adopt a single set of evidence rules for different types of disputes. Yet vast procedural differences—as in the scope of civil and criminal discovery—mean that information inputs for each type of case diverge. The following discussion aims to begin to take procedure into account to better understand how the operation of the rules of evidence has likewise diverged, potentially in a more opaque and unreasoned manner. I suggest that this distinction creates a domino effect on the substantive consequences of the rules of evidence. Thus, while the rules appear in the statute books to uniformly apply across civil and criminal cases, the rules in operation are not so uniform, due to asymmetries in access to information. At least some rules of evidence should therefore change depending on the opportunities for accessing information in advance of cross-examination. Perhaps counterintuitively, this sliding-scale approach is key to holding the deeper epistemological thrust of evidence law constant across multiple kinds of disputes.