Stanford Law Review

Volume 70 May 2018

ARTICLE

Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System

Rebecca Wexler*

Abstract. The criminal justice system is becoming automated. At every stage, from policing to evidence to parole, machine learning and other computer systems guide outcomes. Widespread debates over the pros and cons of these technologies have overlooked a crucial issue: ownership. Developers often claim that details about how their tools work are trade secrets and refuse to disclose that information to criminal defendants or their attorneys. The introduction of intellectual property claims into the criminal justice system raises undertheorized tensions between life, liberty, and property interests.

This Article offers the first wide-ranging account of trade secret evidence in criminal cases and develops a framework to address the problems that result. In sharp contrast to the general view among trial courts, legislatures, and scholars alike, this Article argues that trade secrets should not be privileged in criminal proceedings. A criminal trade secret privilege is ahistorical, harmful to defendants, and unnecessary to protect the interests of

* Visiting Fellow, Yale Law School. I am grateful to Amy Kapczynski and Tracey Meares for feedback since the inception of this project. Comments from Andrea Roth and Edward Imwinkelried have been invaluable. For thoughtful responses to earlier drafts, thanks are due to Michael Abramowicz, Ian Ayres, Patrick Ball, Kiel Brennan-Marquez, Bryan Choi, Victoria Cundiff, John Duffy, Jessica Eaglin, Roger Ford, Kenneth Graham Jr., Camilla Hrdy, Dan Kahan, Mark Lemley, Judge Pierre Leval, Sandra Mayson, Erin Murphy, Tejas Narechania, Christina Spiesel, and Katherine Strandburg. For energizing discussions, I am indebted to Akhil Amar, Jack Balkin, Chesa Boudin, Lincoln Caplan, Cynthia Conti-Cook, Owen Fiss, Julie Fry, Peter Galison, William Gibney, Michael Gill, Jessica Goldthwaite, Charles Tait Graves, Jerome Greco, John Hamasaki, Janet Haven, Keith Hiatt, Clinton Hughes, Clay Kaminsky, Sonia Katyal, Alexa Koenig, David Loftis, Rory Van Loo, Erica Newland, Lisa Ouellette, Pamela Samuelson, Barry Scheck, Ravi Shroff, Tom Wolf, and Richard Torres. Thank you to workshop participants at The Legal Aid Society, Data & Society, the Information Society Project, Internet Law Works-in-Progress, and We Robot, as well as at Berkeley, Cardozo, Columbia, Duke, Harvard, Northwestern, NYU, UCLA, Chicago, UVA, and Yale law schools. Thank you David Murdter for primary research assistance; Jade Ford, Darius Namazi, Tor Tarantola, Megan Yan, and Catherine Yuh for additional research assistance; Jordan Jefferson and Julie Krishnaswami for reference assistance; and Gilad Edelman for additional editing. Kevin Soter and the editors of the *Stanford Law Review* provided excellent editorial work.

the secret holder. Meanwhile, compared to substantive trade secret law, the privilege overprotects intellectual property. Further, privileging trade secrets in criminal proceedings fails to serve the theoretical purposes behind either trade secret law or privilege law. The trade secret inquiry sheds new light on how evidence rules do, and should, function differently in civil and criminal cases.

Table of Contents

Introduction

A death penalty defendant in Pennsylvania state court was denied access to the source code for a forensic software program that generated the critical evidence against him; the program's commercial vendor argued that the code is a trade secret.[1] In a federal court in Texas, the federal government claimed that trade secret interests should shield details about how a cybercrime investigative software program operates, even though the information was necessary to determine whether warrantless use of the tool had violated the Fourth Amendment.[2] And in a Wisconsin case, the state supreme court rejected a defendant's claim that he had a right to scrutinize alleged trade secrets in an algorithmic risk assessment instrument used to sentence him.[3] The court reasoned that no due process violation had occurred in part because the judge's own access to the secrets was equally limited.[4]

Cases like these herald a growing trend. Criminal justice decisionmaking is becoming automated. At every stage—policing and investigations, pretrial incarceration, assessing evidence of guilt at trial, sentencing, and parole—machine learning systems and other software programs increasingly guide criminal justice outcomes.[5] Predictive policing technologies identify "hot spot"

[1] *See* Petition for Review Filed by Defendant Michael Robinson at 4, Robinson v. Commonwealth, No. 25 WDM 2016 (Pa. Super. Ct. Mar. 7, 2016) (involving a defendant's challenge to a Cybergenetics software program that "deconvoluted" a complex DNA mixture and determined that the defendant had contributed to the mixture). For one definition of "trade secret," see 18 U.S.C. § 1839(3) (2016) ("[T]he term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information . . . if (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information . . . .").

[2] *See* United States v. Ocasio, No. 3:11-cr-02728-KC, slip op. at 1-2, 11-12 (W.D. Tex. May 28, 2013) (involving a request for the source code related to the software known as the Child Protection System (CPS)). The CPS software at issue is used to investigate peer-to-peer networks. *See* Don Lewis, *Law Enforcement Making Strides in Investigating Peer-to-Peer Networks for Child Pornography*, SEARCH (Feb. 5, 2015), https://perma.cc/8ML4-TKTX.

[3] *See* State v. Loomis, 881 N.W.2d 749, 760-61 (Wis. 2016), *cert. denied*, 137 S. Ct. 2290 (2017).

[4] *See id.* at 761 (distinguishing the due process violations found in *Gardner v. Florida*, 430 U.S. 349 (1977), and *State v. Skaff*, 447 N.W.2d 84 (Wis. Ct. App. 1989), on the ground that "this is not a situation in which portions of a [presentence investigation report] are considered by the circuit court, but not released to the defendant," noting that "[t]he circuit court and [the defendant] had access to the same copy of the risk assessment").

[5] *See* Rebecca Wexler, Opinion, *When a Computer Program Keeps You in Jail*, N.Y. TIMES (June 13, 2017), https://perma.cc/7NYM-XQ4T.

neighborhoods.[6] Social media analytics flag at-risk individuals.[7] Forensic scientists use software programs to analyze crime scene evidence, including DNA,[8] fingerprints,[9] ballistics,[10] and face matches.[11] And judges and parole boards rely on risk assessment instruments, which purport to predict an

[6] *See More Than Just Hot Spot Policing: Hot Spot Policing Gets Predictive*, PREDPOL, https://perma.cc/LY5U-2NQQ (archived Mar. 12, 2018).

[7] For instance, the Chicago Police Department is currently using an algorithmic system to identify individuals at risk for gun violence and has refused to release information about how the system works, claiming the information is "proprietary." *See* Jeff Asher & Rob Arthur, *Inside the Algorithm That Tries to Predict Gun Violence in Chicago*, N.Y. TIMES (June 13, 2017), https://perma.cc/XL35-R7AB (discussing Chicago's Strategic Subject List). Researchers, however, have reported that Chicago's Strategic Subject List, as well as IBM's SPSS Crime Prediction and Prevention system, Hitachi's Visualization Predictive Crime Analytics system, and Intrado's Beware system, all use social media as input data. *See* DAVID ROBINSON & LOGAN KOEPKE, UPTURN, STUCK IN A PATTERN: EARLY EVIDENCE ON "PREDICTIVE POLICING" AND CIVIL RIGHTS 3 tbl.1 (2016), https://perma.cc/BG4T-EAFK. Additional systems that use social media for individualized risk predictions are in development. *See In Effort to Curb Violence in Chicago, a Professor Mines Social Media*, NPR (Sept. 9, 2016, 6:04 PM ET), https://perma.cc/8NHL-B3MB (discussing Desmond Patton's efforts to develop "an algorithm that will monitor [social media] and identify who might be the next victim or shooter").

[8] *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, FORENSIC SCIENCE IN CRIMINAL COURTS: ENSURING SCIENTIFIC VALIDITY OF FEATURE-COMPARISON METHODS 78-79 (2016), https://perma.cc/Q7UZ-T76U (identifying eight forensic software programs for analyzing complex mixtures of DNA).

[9] *See Scientists Automate Key Step in Forensic Fingerprint Analysis*, NAT'L INST. STANDARDS & TECH. (Aug. 14, 2017), https://perma.cc/F52B-UW8C (describing the Automated Fingerprint Identification System (AFIS), which checks prints against a database and returns potential matches, and announcing a new machine learning system that evaluates latent prints before running the AFIS search).

[10] The National Integrated Ballistic Information Network (NIBIN) currently provides a proprietary system that "automates ballistics evaluations and provides actionable investigative leads in a timely manner." *National Integrated Ballistic Information Network (NIBIN)*, BUREAU ALCOHOL, TOBACCO, FIREARMS & EXPLOSIVES, https://perma.cc/XHD8-22PF (archived Mar. 12, 2018); *see NIST 3D Ballistics Research Database Goes Live*, NAT'L INST. STANDARDS & TECH. (July 7, 2016), https://perma.cc/48CW-SH7K (noting that because the NIBIN database is "proprietary," it has hindered research to improve ballistic forensics); *see also* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 8, at 113-14 (describing image analysis algorithms used in forensic firearms analysis).

[11] *See Facial Recognition*, IDEMIA, https://perma.cc/F9J5-QJRY (archived Mar. 12, 2018) (discussing use of face recognition software in the U.S. criminal justice system); David Kravets, *Driver's License Facial Recognition Tech Leads to 4,000 New York Arrests*, ARS TECHNICA (Aug. 22, 2017, 12:05 PM), https://perma.cc/2RSD-RJSX. Jurisdictions may limit the use of automated face matches to investigative leads, requiring that they be confirmed manually by humans and prohibiting arrest or detention solely on the basis of an automated face match. *See* CLARE GARVIE ET AL., GEORGETOWN LAW CTR. ON PRIVACY & TECH., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 46-47, 121, 128, 138 (2016), https://perma.cc/HH7D-BHNR.

individual's future behavior, to decide who will make bail or parole and even what sentence to impose.[12]

Widespread debates over automated criminal justice technologies have focused on whether data-driven systems enhance accuracy, objectivity, and transparency in decisions that would otherwise be made by humans,[13] or whether these same systems in fact exacerbate errors, bias, and opacity,[14] while making such decisions merely *appear* more scientific.[15] Risk assessment instruments are among the most controversial.[16] Advocates claim that these systems can reduce mass incarceration without endangering public safety by identifying low-risk individuals for release.[17] Critics argue that the tools risk reinstating past biases by relying on historical data to make future predictions.[18] Similar hopes and concerns attend automated systems that allocate

[12] *See, e.g.*, Rebecca Wexler, *Code of Silence: How Private Companies Hide Flaws in the Software That Governments Use to Decide Who Goes to Prison and Who Gets Out*, WASH. MONTHLY (June/July/Aug. 2017), https://perma.cc/L6AK-FE3Z (describing the use of risk assessments in bail and sentencing and detailing how a New York inmate was denied parole because of his risk assessment score).

[13] *See, e.g.*, Jennifer Skeem, *Scientific Risk Assessment in Sentencing May Beat the Alternative*, BERKELEY BLOG (Sept. 30, 2014), https://perma.cc/KAB9-BVL3 (noting that judges make decisions that are "opaque" and "virtually impossible to challenge," whereas with risk assessment instruments "the criteria are transparent, consistent, and can be examined for patterns").

[14] *See, e.g.*, Julia Angwin & Jeff Larson, *Bias in Criminal Risk Scores Is Mathematically Inevitable, Researchers Say*, PROPUBLICA (Dec. 30, 2016, 4:44 PM EST), https://perma.cc/8FUR-4AAP (identifying concerns over accuracy, objectivity, errors, and bias).

[15] *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, 982 (warning that racial biases in past policing data will "be even harder to successfully challenge and expose because they are presented as part of the 'hard science' of big data").

[16] *See, e.g.*, Sonja B. Starr, *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, 66 STAN. L. REV. 803, 817-21 (2014) (describing scholarly critiques of, and developing a constitutional challenge to, evidence-based sentencing).

[17] *See, e.g.*, John Monahan, *Risk Assessment in Sentencing*, *in* 4 REFORMING CRIMINAL JUSTICE 77, 78 (Eric Luna ed., 2017) (contending that a "morally constrained form of risk assessment in sentencing offenders" can reduce mass incarceration); Samuel R. Wiseman, *Fixing Bail*, 84 GEO. WASH. L. REV. 417, 420-25 (2016) (arguing that using risk assessment instruments in pretrial release decisions is preferable to leaving decisions entirely to judges, who are often incentivized to deny release); Recent Case, State v. Loomis, *881 N.W.2d 749 (Wis. 2016)*, 130 HARV. L. REV. 1530, 1535-36 (2017) (explaining that the Model Penal Code, judges, and commentators all have endorsed risk assessment instruments for sentencing and noting external pressures on decisionmakers to assume that the tools are reliable).

[18] *See, e.g.*, Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://perma.cc/JRR9-5D29 (finding that one system erroneously categorized black defendants as future criminals at nearly twice the rate as it did for white defendants). *But see* Avi Feller et al., *A Computer Program Used for Bail and Sentencing Decisions Was Labeled Biased Against Blacks. It's Actually Not That Clear.*, WASH. POST: MONKEY CAGE (Oct. 17, 2016), https://perma.cc/7M7V-GPKL (countering that the problem ProPublica identified is

footnote continued on next page

police resources.[19] And software programs used to analyze evidence of guilt have likewise elicited dispute over their reliability and contestability.[20]

These debates are urgent, but they are also incomplete. They have failed to appreciate a crucial issue: *ownership*. Automation is intensifying the privatization of the justice system. In recent years, private prisons have been found to undermaintain safety and security[21] and private police have been found to operate with minimal training and oversight.[22] The emerging criminal justice technologies discussed in this Article are also, for the most part, privately owned.[23] Developers often assert that details about how their

"mathematically guaranteed" given historical data showing disparate recidivism rates for blacks and whites combined with a particular definition of fairness).

[19] *See, e.g.*, Simmons, *supra* note 15, at 950, 953-54 (advocating for predictive algorithms to determine whether legal standards such as reasonable suspicion or probable cause are met, provided there are ways to adequately ensure that the systems do not use prohibited factors such as race and are sufficiently individualized).

[20] *See, e.g.*, Edward J. Imwinkelried, *Computer Source Code: A Source of the Growing Controversy over the Reliability of Automated Forensic Techniques*, 66 DEPAUL L. REV. 97, 101 (2016) ("[A]lthough the prosecution may lay the foundation for admitting testimony based on probabilistic genotyping programs . . . without presenting expert testimony about the program's source code, in some circumstances a criminal accused should have the right to access . . . the program's source code to assess its validity."); Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 2018-48 (2017) [hereinafter Roth, *Machine Testimony*] (identifying forensic DNA analysis software as one example of a "complex system[] [that] raise[s] accuracy issues not adequately addressed by existing evidence law" and proposing means to test and contest machine-generated evidence); Andrea Roth, *Trial by Machine*, 104 GEO. L.J. 1245, 1252, 1300-01 (2016) (theorizing that the mechanization of criminal justice decisionmaking has developed disproportionately to minimize false negatives—that is, undetected crime, wrongful acquittals, and under-punishment—and noting concerns about maintaining adversarial safeguards through scrutiny and contestation); Christian Chessman, Note, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CALIF. L. REV. 179, 186-95 (2017) (identifying "structural" sources of error in computer code that could affect forensic systems); Rebecca Wexler, *Convicted by Code*, SLATE: FUTURE TENSE (Oct. 6, 2015, 12:28 PM), https://perma.cc/ZBD4-BY7G (arguing that criminal defendants should have access to forensic systems' source code to facilitate contestability).

[21] *See, e.g.*, OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, REVIEW OF THE FEDERAL BUREAU OF PRISONS' MONITORING OF CONTRACT PRISONS, at ii (2016), https://perma.cc/HQ2L-NBXU ("[I]n a majority of the categories we examined, contract prisons incurred more safety and security incidents per capita than comparable [Federal Bureau of Prisons] institutions.").

[22] *See, e.g.*, Justin Jouvenal, *Private Police Carry Guns and Make Arrests, and Their Ranks Are Swelling*, WASH. POST (Feb. 28, 2015), https://perma.cc/8AZ2-J44S ("[T]hese armed [private] officers often receive a small fraction of the training and oversight of their municipal counterparts.").

[23] *See, e.g.*, ROBINSON & KOEPKE, *supra* note 7, at 3 tbl.1 (identifying nine leading predictive policing systems that were developed either solely by private industry or through a collaboration between academics and private industry); *see also, e.g.*, *Casework*, CYBERGENETICS, https://perma.cc/SE9L-F2N5 (archived Mar. 15, 2018) (discussing the TrueAllele Casework DNA interpretation system); *COMPAS Classification*, EQUIVANT,

footnote continued on next page

tools function are trade secrets. As a result, they claim entitlements to withhold that information from criminal defendants and their attorneys, refusing to comply even with those subpoenas that seek information under a protective order and under seal.[24]

To date, scholars and practitioners have largely overlooked the fact that new technologies entering criminal proceedings are bringing intellectual property claims with them.[25] But conflicts surrounding this trend are likely to multiply. The Defend Trade Secrets Act (DTSA) of 2016 established the first federal cause of action for trade secret misappropriation,[26] while the U.S. Supreme Court's 2014 decision in *Alice Corp. v. CLS Bank International* made it harder to patent software.[27] Future developers of data-driven systems are therefore likely to depend more heavily on trade secret protections.[28]

This Article documents the introduction of trade secret evidence into criminal cases and develops a framework to address the resulting tensions between life, liberty, and property interests. Specifically, it turns to evidence law to resolve the conflict between transparency and trade secrecy with respect to emerging criminal justice technologies. The intellectual propertization of core aspects of the criminal justice system is hardly an isolated

https://perma.cc/PL6H-CXKF (archived Mar. 15, 2018) (discussing the COMPAS risk assessment system). STRmix, a forensic technology platform used by the Federal Bureau of Investigation (FBI), is sold for profit around the world, though it is owned by one of New Zealand's Crown Research Institutes. *See* INST. OF ENVTL. SCI. & RESEARCH, 2017 ANNUAL REPORT 2, 7, 12, 38 (2017), https://perma.cc/F72W-U7Z5.

[24] *See infra* Part I.

[25] An urgent new scholarly conversation is just beginning to develop around the intersection of criminal justice and intellectual property concerns. *See generally* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 101 (2017) (examining the influence of proprietary interests over policing technologies); Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CALIF. L. REV. 721 (2007) (raising proprietary interests as one of a number of problems with the oversight of new forensic techniques); Natalie Ram, *Innovating Criminal Justice*, 112 NW. U. L. REV. 659 (2018) (identifying harms of trade secrets in criminal justice technologies and arguing for alternative innovation incentives for criminal justice tools); Katherine L. Moss, Note, *The Admissibility of TrueAllele: A Computerized DNA Interpretation System*, 72 WASH. & LEE L. REV. 1033 (2015) (identifying trade secret issues with the admissibility of forensic DNA analysis software programs).

[26] *See* Skadden, Arps, Slate, Meagher & Flom LLP, New Federal Trade Secrets Act Becomes Law (2016), https://perma.cc/P4LQ-F63S; *see also* Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified in scattered sections of 18 and 34 U.S.C.). For the civil cause of action, see 18 U.S.C. § 1836 (2016).

[27] 134 S. Ct. 2347, 2355-60 (2014).

[28] *See* Gregory V. Novak & Matthew Frontz, *Tipping the Scales: Weighing IP Protection Options Post-DTSA and Post-"Alice,"* TEX. LAW. (Dec. 1, 2016, 12:00 AM), https://perma.cc/W5EQ-94RC (noting that because *Alice* made certain patent rights in algorithmic systems unenforceable, owners might "turn to trade secret protection").

phenomenon. Legal scholars have debated the clash between black-box methods in algorithmic tools and values of transparency and accountability in a wide array of public and private domains.[29] The debate over secrecy and disclosure has touched intelligence surveillance,[30] public infrastructure,[31] commercial activities,[32] healthcare,[33] administrative decisionmaking,[34] and to some extent criminal procedure.[35] But the manifestations of these tensions in evidence law have gone almost entirely unexamined.[36] This lack of scrutiny is

[29] *See, e.g.*, FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 12-15 (2015).

[30] *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, 865 (2014) (documenting failures to notify criminal defendants of secret electronic surveillance programs).

[31] *See, e.g.*, David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135, 177-87 (2007) (arguing against trade secret protections for public infrastructure).

[32] *See, e.g.*, Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 8 (2014) (arguing for "technological due process" to subject trade secret automated scoring systems to expert review).

[33] *See, e.g.*, Roger Allan Ford & W. Nicholson Price II, *Privacy and Accountability in Black-Box Medicine*, 23 MICH. TELECOMM. & TECH. L. REV. 1, 29-31 (2016) (noting tensions between patient privacy and the transparency and accountability of data-driven medicine).

[34] *See, e.g.*, Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1281-88 (2008) (arguing that automated systems that can terminate liberty or property interests such as Medicaid benefits endanger the beneficiaries' rights to notice and the opportunity to be heard); Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 GEO. L.J. 1147, 1177-213 (2017) (considering whether machine learning tools in administrative rulemaking and adjudication could offend principles of nondelegation, due process, antidiscrimination, or transparency); 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 at issue"); Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1777-84 (2015) (arguing that the lack of notice and opportunity to appeal inaccuracies in data-driven administrative lists—such as voter registration rolls—creates a de facto "guilty until proven innocent" burden).

[35] *See, e.g.*, Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 1032-38 (2014) (identifying barriers unrelated to intellectual property, such as the state secrets privilege, that impede defense access to evidence); Brandon L. Garrett, *Big Data and Due Process*, 99 CORNELL L. REV. ONLINE 207, 211-13 (2014) (considering how big data evidence interacts with the government's due process disclosure obligations under *Brady v. Maryland*, 373 U.S. 83 (1963), and *Kyles v. Whitley*, 514 U.S. 419 (1995)).

[36] Welcome exceptions to this general lack of scrutiny include Imwinkelried, *supra* note 20, at 111-24 (evaluating the need for source code review in admissibility determinations and cross-examination); Jennifer L. Mnookin, *Of Black Boxes, Instruments, and Experts: Testing the Validity of Forensic Science*, 5 EPISTEME 343, 352-55 (2008) (discussing source code transparency issues in admissibility hearings); Roth, *Machine Testimony*, *supra* note 20, at 1983-85 (showing how automated systems can

footnote continued on next page

all the more troubling given that privilege law, which applies to all judicial proceedings including those before trial and after conviction,[37] has remained relevant even as the number of trials has plummeted.[38]

The dearth of scholarly attention has been accompanied by uncritical acceptance of trade secret evidence in criminal cases. Today, the general view among legislators, judges, and scholars alike is that some form of trade secret evidentiary privilege both does and should exist, at least in civil proceedings. At least twenty-one states have codified a trade secret privilege in their evidence rules.[39] Courts in many of the remaining jurisdictions recognize some common law variation of it.[40] A few scholars have taken a measured approach. Kenneth Graham Jr. calls the privilege "controversial,"[41] observing that mid-twentieth century authorities "all seem to have thought that there was no privilege for trade secrets," though courts had equitable discretion to protect against undue disclosures in litigation.[42] But much existing literature treats the

present testimonial infirmities similar to those underlying hearsay concerns, such as falsehood, inarticulateness, and analytical error); Chessman, *supra* note 20, at 215-19 (arguing that the evidence law standards for admitting expert testimony should require source code disclosure); and Jennifer N. Mellon, Note, *Manufacturing Convictions: Why Defendants Are Entitled to the Data Underlying Forensic DNA Kits*, 51 DUKE L.J. 1097, 1112-20 (2001) (considering proprietary elements of DNA test kits and noting the tension between the trade secret privilege and criminal discovery).

[37] *See* FED. R. EVID. 1101(c).

[38] *Compare* U.S. Sentencing Comm'n, Fiscal Year 1996 Guideline Sentences: National Data (n.d.), https://perma.cc/J9LS-5JAQ (showing that trials accounted for 8.3% of criminal convictions in "guideline sentences" in fiscal year 1996 (capitalization altered)), *with* U.S. Sentencing Comm'n, Fiscal Year 2016 Guideline Sentences: National Data (n.d.), https://perma.cc/BVT5-3L7D (showing that trials accounted for 2.7% of similar convictions in fiscal year 2016). One study of twenty-eight counties in the early 1960s indicated that guilty pleas accounted for 48-74% of convictions. *See* WILLIAM J. STUNTZ, THE COLLAPSE OF AMERICAN CRIMINAL JUSTICE 326 n.56 (2011). By 2014, 91% of federal felony convictions terminated in a guilty plea. *See* Bureau of Justice Statistics, U.S. Dep't of Justice, Federal Justice Statistics, 2013-2014 (2017), https://perma.cc/9F6D-SEPS.

[39] *See* ALA. R. EVID. 507; ALASKA R. EVID. 508; ARK. R. EVID. 507; CAL. EVID. CODE § 1060 (West 2018); DEL. R. EVID. 507; FLA. STAT. § 90.506 (2017); HAW. R. EVID. 508; KAN. STAT. ANN. § 60-432 (2017); LA. CODE EVID. ANN. art. 513 (2017); ME. R. EVID. 507; NEB. REV. STAT. § 27-508 (2017); NEV. REV. STAT. § 49.325 (2017); N.H. R. EVID. 507; N.J. R. EVID. 514; N.M. R. EVID. 11-508; N.D. R. EVID. 507; OKLA. STAT. tit. xii, § 2508 (2017); S.C. CODE ANN. § 39-8-60 (2017); S.D. CODIFIED LAWS § 19-19-507 (2018); TEX. R. EVID. 507; WIS. STAT. § 905.08 (2017).

[40] *See* EDWARD J. IMWINKELRIED, THE NEW WIGMORE: A TREATISE ON EVIDENCE § 9.2.1, at 1456 (Richard D. Friedman ed., 2d ed. 2010); 26 CHARLES ALAN WRIGHT & KENNETH W. GRAHAM, JR., FEDERAL PRACTICE AND PROCEDURE §§ 5641-5642 (1992) [hereinafter WRIGHT & GRAHAM]. Massachusetts is an exception. *See* SUPREME JUDICIAL COURT ADVISORY COMM. ON MASS. EVIDENCE LAW, MASSACHUSETTS GUIDE TO EVIDENCE: 2017 EDITION § 517 (2017), https://perma.cc/L59M-2LUK.

[41] *See* 26 WRIGHT & GRAHAM, *supra* note 40, § 5642, at 320.

[42] *See id.* at 289 & nn.12-14.

privilege as self-evident.[43] Some commentators have also presumed that the privilege should apply to criminal as well as civil cases.[44]

This Article challenges the common view in favor of the trade secret privilege by arguing that none should exist in criminal proceedings.[45] As with other kinds of sensitive information, such as witnesses' medical records, courts may issue protective orders to limit the use and distribution of trade secrets beyond the needs of the proceeding.[46] But trade secret holders should wield no special power to block criminal defendants' access to evidence altogether.[47] Courts should refuse to extend the privilege wholesale from civil to criminal cases, and legislatures should pass new laws that limit safeguards for trade secret evidence in criminal proceedings to protective orders and nothing more.[48]

[43] *See, e.g.*, Jessica Ring Amunson & Sam Hirsch, *The Case of the Disappearing Votes: Lessons from the* Jennings v. Buchanan *Congressional Election Contest*, 17 WM. & MARY BILL RTS. J. 397, 418 (2008) (criticizing the manner in which Florida courts had applied the privilege but not challenging its existence); Timothy S. Durst & Cheryl L. Mann, *Behind Closed Doors: Closing the Courtroom in Trade Secrets Cases*, 8 TEX. INTELL. PROP. L.J. 355, 365-66 (2000) (discussing safeguards against unnecessary disclosure).

[44] For instance, Edward Imwinkelried asserts 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." Imwinkelried, *supra* note 20, at 126. To be sure, Imwinkelried also states that companies' "assertion of the right should not end the analysis," but his conclusion that "[a] party seeking discovery of the trade secret information can defeat the privilege claim by demonstrating that the information is highly relevant and necessary for trial," *id.*, is a fairly strong articulation of the privilege.

[45] *Cf.* Masashi Chusho, *Protection of Trade Secrets in Lawsuit Procedures in Japan*, 48 LES NOUVELLES 193, 195 (2013) (stating that trade secrets are not privileged in criminal proceedings in Japanese courts).

[46] This Article briefly raises the potential conflict between protective orders and Sixth Amendment public trial rights, which is a ripe issue for future scholarly contribution. *See* OFFICES OF THE U.S. ATTORNEYS, CRIMINAL RESOURCE MANUAL § 1139 (1997), https://perma.cc/LGW6-RZBX (presenting a legal basis for limiting disclosure of trade secrets during criminal trials for trade secret theft "without necessarily violating the defendant's right to a public trial under the Sixth Amendment"); *see also* 1 PETER S. MENELL ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE: 2017, at 142 n.12 (2017) (noting "constant battles" in criminal trade secret cases over courtroom disclosures and defendants' public trial rights); Kristin Saetveit, Note, *Close Calls: Defining Courtroom Closures Under the Sixth Amendment*, 68 STAN. L. REV. 897, 909-19, 922-32 (2016) (identifying circuit splits over the definition of a courtroom closure for Sixth Amendment purposes).

[47] This Article is primarily concerned with invocations of the privilege in criminal cases other than prosecutions of trade secret theft because the evidence in trade secret theft cases is likely too essential for the privilege to be sought. *See infra* note 379 and accompanying text.

[48] I use the term "protective order" broadly here to including sealing and other practical protections against public disclosure during trial. For a detailed discussion of practical safeguards, see text accompanying note 375 below.

This Article begins by describing recent criminal cases in which developers have claimed entitlements to withhold trade secret information from the accused. A California defendant's attorney was denied access to trade secret evidence under a protective order despite insisting, "I've been a lawyer for 30 years and I've never violated a court order."[49] A company that sells an audio surveillance system for gunshot alerts refused to comply with a defense subpoena for trade secret information that could have helped to determine whether the system violates state wiretap laws.[50] A New York inmate was denied parole because of a flawed risk assessment score; he discovered an error in the input data used to generate his score but could not prove the significance of that error because the developer considers the weights of input variables to be trade secrets.[51]

This Article is structured as follows. Part I presents a compendium of trade secret issues at different stages in the life cycle of a criminal proceeding, from investigations to sentencing. It concludes by explaining and addressing

[49] *See* Transcript of Record at 4096, People v. Johnson, No. BF151825A (Cal. Super. Ct. Kern Cty. May 19, 2015). The trial court, relying on the statutory trade secret privilege, denied the attorney access. *See id.* at 4111 ("[The prosecutor:] I'd ask the Court to . . . uphold the trade privilege, and deny defendant's motion in this case. The Court: . . . There's been no particularized showing under [the trade secret privilege provision] as to how the TrueAllele source code is *necessary* to defense's ability to test the reliability of its results. Therefore, respectfully deny the motion." (emphasis added) (capitalization altered)). The defendant has appealed, arguing that "[a]pplication of the trade secret privilege to deny access to evidence in criminal cases jeopardizes the accused's right to a fair trial." *See* Appellant's Reply Brief at 9-12, People v. Johnson, No. F071640 (Cal. Ct. App. Aug. 30, 2017).

[50] *See* Letter from Mike Will, Senior Dir., Tech. & Customer Support, SST, to Jeff Adachi & Michelle Tong, Deputy Pub. Defs., S.F. Pub. Def. 3 (Oct. 17, 2016) (on file with author) (citing the trade secret privilege as justification for refusing to comply with a defense request for the source code of "software that allows the sensors to distinguish between gunshots and ambient noise"). For information about longstanding concerns that SST's ShotSpotter gunshot alert system may continually record human voices at normal speech decibels, see Jay Stanley, *Shotspotter CEO Answers Questions on Gunshot Detectors in Cities*, ACLU (May 5, 2015, 9:15 PM), https://perma.cc/FE6N-TB9G. Defense attorneys in Massachusetts previously considered moving to suppress ShotSpotter recordings under the theory that they violate the state wiretapping law. *See* Erica Goode, *Shots Fired, Pinpointed and Argued Over*, N.Y. TIMES (May 28, 2012), https://perma.cc/2ETN-LUPH. The San Francisco public defenders seeking SST source code may have been considering a similar argument.

[51] *See* Wexler, *supra* note 12 (documenting Rodríguez's efforts to identify and correct the error in his COMPAS assessment); Letter from Glenn Rodríguez to Inmate Grievance Resolution Comm. 2 (Jan. 10, 2017) (on file with author); *see also* State v. Loomis, 881 N.W.2d 749, 761 (Wis. 2016) ("Northpointe, Inc., the developer of COMPAS, considers COMPAS a proprietary instrument and a trade secret. Accordingly, it does not disclose how the risk scores are determined or how the factors are weighed."), *cert. denied*, 137 S. Ct. 2290 (2017).

arguments that developers in these cases have made to justify their trade secrecy claims.

Part II argues that a broad trade secret privilege in criminal cases is ahistorical. The standards governing the privilege developed in, and for, civil disputes. By mining previously underscrutinized archival records, I recover key dissenting voices rejecting a trade secret privilege—even in civil cases—that have been obscured from the historical record. I then use those unearthed views to develop a more thorough intellectual history of the privilege, which in turn exposes legislative efforts to manufacture a general consensus in its favor. Finally, I show that despite widespread acceptance of a trade secret privilege during the mid-twentieth century, its application to criminal proceedings was virtually unprecedented until 2015. Whether and to what extent a trade secret privilege applies in criminal cases remains an open legal question.

Part III describes the rules that currently govern the privilege and assesses those rules in relation to criminal procedure, trade secret law, and broader privilege law. Reasoning from the perspective of criminal procedure, Part III.A shows that privileging trade secrets is both particularly harmful and unnecessary in criminal cases. As applied to criminal proceedings, the existing privilege rules do not adequately safeguard against overclaiming and abuse, and will almost certainly lead to the wrongful exclusion of probative evidence. Recognizing the privilege in this context further offends procedural justice by signaling that the government values trade secret holders more than those whose life or liberty is at stake.

Part III.B then argues that the privilege is also unnecessary because narrow criminal discovery and subpoena powers already tightly restrict defendants' access to immaterial information. And when nonfrivolous defense requests for material information create a credible risk of harm, courts can issue protective orders instead of barring access to the evidence altogether.

Part III.C contends that, compared to substantive trade secret law, the privilege overprotects intellectual property. Trade secret law protects secret information[52] from "misappropriation," meaning improper use or acquisition.[53] Individuals who assert the privilege—in both civil and criminal cases—

[52] For instance, under the Uniform Trade Secrets Act, to qualify as trade secret subject matter, information must "derive[] independent economic value . . . from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use," and it must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy." UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985).

[53] *See id.* § 1(1)-(2). For example, under the DTSA, misappropriation includes unauthorized disclosure by a person who used "improper means" to acquire the secret, *see* 18 U.S.C. § 1836(b)(2)(A)(ii)(IV)(AA)-(BB) (2016), which "includes theft, bribery, misrepresenta-

footnote continued on next page

already enjoy the standard ex post remedies that trade secret law affords for misappropriation. Layering on a privilege thus grants "protection plus." In addition, the privilege creates an ex ante injunction on the use of trade secret information without any showing of actual, threatened, or inevitable misappropriation—an extreme protection that is not available under substantive trade secret law. Moreover, the underlying theoretical rationales for the existence of trade secret law—that it encourages innovation and promotes fair business practices—can't justify a privilege that overwhelmingly shields trade secrets from people who will most likely never be business competitors. The privilege also undermines trade secret law's goal of facilitating controlled information disclosures. That goal is better served by allowing discovery subject to a protective order.

I suggest in Part III.D that courts may lack the power to recognize a criminal trade secret privilege due to an absence of controlling authority on the issue combined with rules requiring narrow construction of evidentiary privileges. Further, to the extent that evidentiary privileges exist to balance truth-seeking in adjudication against competing policy preferences that are extrinsic to the courts, it does not serve the purpose of privilege law to grant trade secrets *more* protection within evidence law than they enjoy outside of it. Finally, I draw from Akhil Reed Amar's theory of "compulsion parity" as a method for evaluating the propriety of evidentiary privileges in criminal proceedings and from Erin Murphy's institutional analysis of scientific evidence to argue that privileges in criminal cases are more likely to be unjustified when the government has an incentive not to seek out the protected category of information. A criminal trade secret privilege is one such scenario.

This Article concludes with thoughts about how the trade secret inquiry sheds new light on how evidence rules do, and should, function differently in civil and criminal proceedings.

I. Trade Secrets in the Criminal Justice System

This Part presents a series of criminal cases that have given rise to trade secret issues at different stages of the proceedings. It describes defense challenges to, judicial reasoning about, and developers' justifications for the lack of transparency in new criminal justice-related technologies. I begin with examples of trade secret claims concerning evidence of guilt at trial. Trial is an instructive starting point because it marks the zenith of defendants'

tion, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means," *id.* § 1839(6)(A).

constitutional and statutory rights.[54] Consequently, if defendants fail to pierce trade secret privilege claims at trial, they will be exceedingly unlikely to do so at any other stage of a case. Next, this Part addresses trade secret technologies defendants may encounter during pretrial or postconviction proceedings, where their procedural rights are weaker. Unsuccessful challenges to trade secret barriers at these stages of a proceeding may normalize, and ease the acceptance of, these new technologies throughout the criminal justice system as a whole. This Part concludes by describing and responding to arguments technology developers have made to justify withholding trade secrets from the accused.

A note on methods is appropriate. The cases in this Part are drawn from online databases such as Westlaw and Lexis, from technology company newsletters and press coverage, and from direct personal communications with defense attorneys across the country. These collection methods necessarily fall short of a comprehensive empirical strategy to quantify trade secret privilege claims in criminal proceedings, but they are the best available. More exhaustive methods are currently unattainable because, while criminal prosecutions overwhelmingly occur in state trial courts,[55] there is no centralized repository of records from these courts.[56] That despite these limitations anecdotal examples of trade secret interference with defense strategy are readily apparent suggests that the problem is substantial.

[54] A plurality of the U.S. Supreme Court has characterized the Sixth Amendment right to confrontation as a "trial right." *See* Pennsylvania v. Ritchie, 480 U.S. 39, 52 (1987) (plurality opinion) (emphasis omitted). In that case the Court contemplated, but did not answer, the question whether the Compulsory Process Clause applies before trial. *See id.* at 56 (majority opinion); *see also* U.S. CONST. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right . . . to have compulsory process for obtaining witnesses in his favor . . . ."). The Fifth and Sixth Amendments do not require prosecutors to disclose impeachment evidence before entering into plea agreements with defendants. *See* United States v. Ruiz, 536 U.S. 622, 625, 633 (2002). Therefore, in jurisdictions with narrow criminal discovery laws, defendants' statutory discovery rights may not mature until just before trial. *See, e.g.*, N.Y. CRIM. PROC. LAW § 240.45 (McKinney 2018). And the Jencks Act, which requires the government to disclose a witness's prior statements, only applies *after* the witness has testified on direct examination at trial. *See* 18 U.S.C. § 3500(a)-(b); *see also* Jencks Act, Pub. L. No. 85-269, 71 Stat. 595 (1957) (codified as amended at 18 U.S.C. § 3500).

[55] *Cf.* Peter Wagner & Wendy Sawyer, *Mass Incarceration: The Whole Pie 2018*, PRISON POL'Y INITIATIVE (Mar. 14, 2018), https://perma.cc/3VG8-RNCQ (comparing state and federal prison populations).

[56] Westlaw and Lexis lack comprehensive coverage of state trial court records. Even federal trial court coverage is incomplete.

A. Evidence of Guilt at Trial

The first category of criminal justice technologies in which developers have claimed trade secrets concerns evidence of guilt presented at trial. For example, a death penalty defendant in California named Martell Chubbs was denied access to the source code for a forensic software program used to convict him because the developer claimed that it was a trade secret.[57] The program was a statistical tool used to calculate the likelihood that Chubbs's DNA was present in a complex sample of DNA evidence from the crime scene.[58] A California trial court had ordered that the program's source code be disclosed subject to a protective order, reasoning that without the code, Chubbs would be denied his "right to confront and cross-examine witnesses."[59] But the software developer refused to comply with the trial court's order, arguing that the code was protected under California's statutory trade secret privilege.[60] In

[57] *See* People v. Superior Court (*Chubbs*), No. B258569, 2015 WL 139069, at *3, *7, *9-10 (Cal. Ct. App. Jan. 9, 2015).

[58] *See id.* at *1. This type of likelihood calculation is used to assess the probative weight of DNA evidence in determining guilt or innocence. *See, e.g.*, Mark William Perlin, *Inclusion Probability for DNA Mixtures Is a Subjective One-Sided Match Statistic Unrelated to Identification Information*, J. PATHOLOGY INFORMATICS 2 (2015), https://perma.cc/FNE2-ZZM8.

[59] *Chubbs*, 2015 WL 139069, at *4. The trial court's 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 defendants "should not have to rely solely on the government's word that further discovery is unnecessary . . . [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." United States v. Budziak, 697 F.3d 1105, 1111-13 (9th Cir. 2012). Note that the defense in *Budziak* did not seek access to source code, and no trade secret interests were raised. *See* United States v. Budziak, 612 F. App'x 882, 884 (9th Cir. 2015).

[60] *See Chubbs*, 2015 WL 139069, at *4; Third Party Witness Dr. Mark W. Perlin's Brief in Support of Assertion of Trade Secret Privilege at 1-2, People v. Chubbs, No. NA0931709 (Cal. Super. Ct. L.A. Cty. July 14, 2014) (arguing that the statutory provision "may be properly asserted in a criminal proceeding" (capitalization altered) (citing CAL. EVID. CODE §§ 1060-1061)). Before the California Court of Appeal's decision in *Chubbs*, the privilege had only been reviewed by appellate courts in civil proceedings. *See* Petitioner's Reply Brief at 6, *Chubbs*, No. B258569 (Cal. Ct. App. Sept. 19, 2014) (describing the issue as "essentially an issue of first impression on how the trade secret privilege applies to criminal cases"). As of April 1, 2018, a Westlaw search for appellate documents citing section 1060 of the California Evidence Code returned two criminal cases other than *Chubbs*, both currently pending appeal.

In *People v. Johnson*, the parties contest the application of the trade secret privilege in the criminal context. *Compare* Respondent's Brief, People v. Johnson, No. F071640 (Cal. Ct. App. Aug. 8, 2017), 2017 WL 5495137, at *74-81 (arguing for application of section 1060's civil standard), *with* Appellant's Reply Brief at 8, *Johnson*, No. F071640 (Cal. Ct. App. Aug. 30, 2017) (arguing that the civil standard should not apply in criminal cases).

footnote continued on next page

2015, a California appeals court ruled for the developer,[61] likely becoming the first appellate court in the nation's history to extend a trade secret evidentiary privilege to a criminal case.[62]

The privilege had two effects. First, it raised the burden to obtain discovery from California's standard "showing of good cause"[63] to the more onerous "particularized showing that the [information] is . . . *necessary* to the defense,"[64] thus ensuring that some relevant evidence otherwise discoverable would no longer be because of its trade secret status. Second, the court held that the privilege entitled the developer to withhold information *entirely* from the accused rather than merely to obtain a protective or sealing order that would restrict who can access the information and for what purpose.[65] Neither effect was clearly required by the statutory text.[66] The burden-raising "necessity"

In *People v. Bertsch*, the trade secret privilege is not at issue on appeal. *See* Appellant's Opening Brief at i-xix, People v. Bertsch, No. S093944 (Cal. Dec. 1, 2016), 2016 WL 7665570 (describing the issues on appeal). The trial court in *Bertsch* expressly declined to apply the trade secret privilege to information about the "primer sequences" in a DNA test kit, noting that "[t]he bulk of the pleadings that were filed in the Court [on the trade secret privilege] really spoke to the civil standards . . . [and] may have been inappropriate." Transcript of Record at 20,375-77, People v. Bertsch, No. 94F07295 (Cal. Super. Ct. Sacramento Cty. Oct. 20, 1999).

[61] *Chubbs*, 2015 WL 139069, at *10. For a detailed history of trade secret privilege claims in both civil and criminal cases, see Part II below.

[62] *See infra* note 286 and accompanying text.

[63] *See* People v. Superior Court, 96 Cal. Rptr. 2d 264, 274 (Ct. App. 2000) (noting that a criminal defendant is normally entitled to subpoena unprivileged evidence "on a showing of good cause—that is, specific facts justifying discovery").

[64] *Chubbs*, 2015 WL 139069, at *6 (emphasis added). The *Chubbs* court reasoned that "it makes no sense" to require disclosure of trade secrets without a showing of necessity. *Id.* As a result, the court declined to apply the normal good cause standard for third-party subpoenas. *See id.* Instead, the court imported a different, heightened standard from a civil case that had construed California's statutory trade secret privilege to require a showing of necessity for third-party subpoenas. *See id.*; *see also* Bridgestone/Firestone, Inc. v. Superior Court, 9 Cal. Rptr. 2d 709, 713, 715 (Ct. App. 1992) (holding that "it is not enough that a trade secret might be useful" and that parties seeking to discover trade secrets must "make a prima facie showing that the [secrets] in fact were relevant and necessary to their proofs"). Note that the word "relevant" in the "relevant and necessary" standard, *see, e.g.*, *Bridgestone*, 9 Cal. Rptr. 2d at 713, is superfluous because a showing of relevance without necessity is insufficient, while a showing of necessity presupposes relevance.

[65] *See Chubbs*, 2015 WL 139069, at *5-6 (acknowledging but declining to adopt the defense's argument that in criminal proceedings, the privilege "does not permit the owner of the trade secret to refuse to disclose" and instead merely provides a right to a protective order and courtroom closure).

[66] Section 1060 of the California Evidence Code grants trade secret owners "a privilege to refuse to disclose the secret." CAL. EVID. CODE § 1060 (West 2018). Sections 1061 and 1062, in turn, apply "whenever the owner of a trade secret wishes to assert his or her trade secret privilege, as provided in section 1060, during a criminal proceeding," *see id.* § 1061(b), and offer more limited remedies: protective orders, *see id.* § 1061, and

footnote continued on next page

provision is a doctrinal creature that developed in civil litigation.[67] The court could have chosen not to apply the heightened burden at all. Alternatively, it could have raised the burden solely for those challenging the restrictions of a particular protective order, or moving to unseal records, rather than for criminal defendants' own discovery and subpoena motions.[68] And as Chubbs's counsel argued, the statute could have been construed to offer protective orders and nothing more.[69] Instead, the court granted trade secret owners a total withholding entitlement: a right to keep relevant evidence secret from criminal defendants because it is the owners' intellectual property.[70]

Chubbs is now being cited in criminal proceedings across the country to justify withholding trade secret evidence from the accused.[71] Other courts have adopted similar reasoning, whether via an explicit evidentiary privilege or by

exclusion of the public from a proceeding, *see id.* § 1062. Section 1063 provides for sealing orders, which are available for assertions of the privilege under either section 1060 or section 1061. *See id.* § 1063.

[67] *See Bridgestone*, 9 Cal. Rptr. 2d at 710, 713, 716 (reversing the trial court's order that would have required the defendant in a civil personal injury action to disclose trade secret formulas for manufacturing tires under a protective order, finding that the plaintiffs had merely shown relevance but had failed to show necessity).

[68] Thank you to John Hamasaki for suggesting this alternative burden-shifting approach.

[69] Chubbs's counsel argued that the sections of the California Evidence Code that expressly apply to criminal cases, *see supra* note 66, appear to presume that defendants will have some access to trade secret information even when the privilege is operative. *See Chubbs*, 2015 WL 139069, at *5. A number of textual arguments can be made to support Chubbs's counsel's view. For instance, section 1061 contemplates on its face that the defendant and defense counsel will be present at any hearing the court holds concerning the validity of an alleged trade secret. *See* CAL. EVID. CODE § 1061(b)(3) (referring to evidentiary hearings, either in open court or in camera). And section 1061 requires the court in certain circumstances to issue protective orders "limiting the use and dissemination of the trade secret," *id.* § 1061(b)(4), such as by requiring that information "be disseminated only to counsel for the parties," *id.* § 1061(b)(4)(A); withholding information from experts who are economic competitors of the trade secret holder "unless no other experts are available," *id.* § 1061(b)(4)(C)(iii); and sealing the public docket, *id.* § 1061(b)(4)(D). *Cf. id.* § 1062(a) (providing for courtroom closures to exclude the public). The protective order and courtroom closure sections of the statute never mention denying defense access altogether.

[70] *See Chubbs*, 2015 WL 139069, at *6.

[71] The *Chubbs* decision is unpublished and thus uncitable in California. *See* CAL. R. CT. 8-1115(a) ("[A]n opinion of a California Court of Appeal . . . that is not certified for publication or ordered published must not be cited or relied on by a court or a party in any other action."). Nonetheless, prosecutors and developers are relying on it as persuasive authority in other jurisdictions, and some courts have referred to the decision in opinions. *See, e.g.*, State v. Fair, No. 10-1-09274-5 SEA, slip op. at 3 n.1 (Wash. Super. Ct. King Cty. Jan. 12, 2017); State's Response to Defense Motion to Compel TrueAllele Source Code at 12-13, *Fair*, No. 10-1-09274-5 SEA (Wash. Super. Ct. King Cty. Apr. 4, 2016) [hereinafter *Fair* State's Response]; Letter Regarding Motion to Quash at 2, United States v. Johnson, No. 1:15-cr-00565-VEC (S.D.N.Y. June 15, 2016).

more loosely incorporating the trade secret status of evidence into their evaluations of defendants' discovery and subpoena motions. In 2017, a Washington court refused to order forensic software source code disclosed.[72] The court found both that the defense had failed to show the materiality of code review and that "the usefulness of disclosing the source code [was] outweighed by a substantial risk of financial harm" to the developers, who "ha[d] a legitimate interest in keeping the source code, a trade secret, confidential."[73] There, the state had argued that the risk of leaks in future cases should persuade the court to deny disclosure of the trade secret information in that case.[74] In another California case currently on appeal, the defendant's attorney sought trade secret source code under the federal Confrontation Clause.[75] The attorney agreed to a protective order that would prohibit his client from seeing the information and further informed the court that in his thirty years as an attorney he had never violated a court order.[76] Nevertheless, the court allowed the software developer to withhold the information, applying a statutory trade secret privilege.[77] A death penalty defendant in Pennsylvania, a "family guy" with no prior criminal record, was acquitted on all counts[78]—but not before being forced to undergo trial without the opportunity to review or challenge the source code of the forensic software used to analyze the evidence against him.[79] In the past five years, courts in at

[72] State v. Fair, No. 10-1-09274-5 SEA, slip op. at 9 (Wash. Super. Ct. King Cty. Jan. 12, 2017).

[73] *Id.* The state had argued that code review was unnecessary; that disclosure "could cause irreparable harm to the company, enabling competitors to easily copy the company's proprietary products and services"; and that a protective order would provide an insufficient safeguard because "protective orders are violated." *Fair* State's Response, *supra* note 71, at 21-22.

[74] *Fair* State's Response, *supra* note 71, at 22 ("As a matter of logic, if the defendant in this case is entitled to the TrueAllele source code, then every defendant in cases involving TrueAllele is also entitled to the source code. If the TrueAllele source code is disclosed hundreds of times, the danger that it will be leaked certainly rises. If a leak occurs, it is unlikely that [the software developer] would be able to establish who leaked the source code, or recover any damages for any financial loss.").

[75] U.S. CONST. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him . . . .").

[76] Transcript of Record, *supra* note 49, at 4091-92, 4096.

[77] *See id.* at 4105-11 (relying on sections 1060, 1061, and 1062 of the California Evidence Code to deny the defendant's Confrontation Clause objection and ignoring the defense attorney's argument that "there's no trade secret exception to the Sixth Amendment").

[78] *See "Hard-Working Family Guy" Found Not Guilty of Double Homicide in Duquesne*, ASSOCIATED PRESS (updated Feb. 7, 2017, 5:38 PM EST), https://perma.cc/N5FW-APKE; Paula Reed Ward & Torsten Ove, *Jury Acquits Duquesne Man in Double Homicide Case*, PITT. POST-GAZETTE (Feb. 7, 2017, 2:25 PM), https://perma.cc/X9VJ-P8J8.

[79] Commonwealth v. Robinson, No. CC 201307777, slip op. at 1 (Pa. Ct. C.P. Allegheny Cty. Feb. 4, 2016).

least five states have similarly denied defense motions to gain access to trade secret evidence.[80]

[80] These cases often involve determinations about the *relevance* of the information sought, but in each case the alleged trade secret status of the information affected the court's reasoning. The five states are California, New York, Ohio, Pennsylvania, and Washington.

For California, see People v. Superior Court (*Chubbs*), No. B258569, 2015 WL 139069, at *6 (Cal. Ct. App. Jan. 9, 2015); and Transcript of Record, *supra* note 49, at 4096, 4111.

For New York, see People v. Carter, No. 2573/14, 2016 WL 239708, at *1, *7 (N.Y. Sup. Ct. Jan. 12, 2016) (denying the defendant's discovery motion for Forensic Statistical Tool (FST) source code because "the source code is proprietary software copyrighted by the city of New York" and because it found "no reason to believe that [the] defendant's right to cross-examine witnesses or present a defense will be curtailed by the court's refusal to order the People to obtain and disclose [Office of Chief Medical Examiner (OCME)] proprietary software"). *See also* Letter Regarding Notice of Judicial Subpoena *Duces Tecum* at 1-2, People v. Johnson, No. 3600/2015 (N.Y. Sup. Ct. Sept. 29, 2016) [hereinafter *Johnson* Subpoena Letter] (refusing to comply with a defense subpoena for the FST source code and emphasizing "OCME's ownership interest in the FST program"); Memorandum at 5, People v. Pelt, No. 2607/2013 (N.Y. Sup. Ct. July 28, 2015) (denying the defendant's demand for disclosure of FST source code on similar grounds); *cf.* People v. Lopez, 23 N.Y.S.3d 820, 823, 829 (Sup. Ct. 2015) (observing that in a related case, "the specific drop-in and drop-out rates used in the FST were considered proprietary to the developers of that program" and denying a defense motion seeking an executable copy of the FST program for independent testing because "the computer program itself is proprietary and the Court is not ordering its disclosure").

For Ohio, see State v. Shaw, No. CR-13-575691, slip op. at 25-26 (Ohio Ct. C.P. Cuyahoga Cty. Oct. 9, 2014) (denying the defendant's motion to compel production of source code because the court had "previously established that the TrueAllele methodology and the State's witness are reliable without the use of the source code"). While this denial does not on its face mention the trade secret privilege, the explanation is incomplete. The defendant brought two motions: the first to exclude the results of the TrueAllele analysis as unreliable under the framework established in *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), and the second to compel discovery of the source code for purposes of confrontation and cross-examination. *See Shaw*, No. CR-13-575691, slip op. at 1; Defendant's Motion to Compel Discovery at 1, *Shaw*, No. CR-13-575691 (Ohio Ct. C.P. Cuyahoga Cty. June 6, 2014); Supplemental Motion to Compel Discovery of TrueAllele's Source Code at 5, *Shaw*, No. CR-13-575691 (Ohio Ct. C.P. Cuyahoga Cty. Aug. 14, 2014). The court rightfully acknowledged that its own assessment of reliability went to admissibility, not to the scope of cross-examination for "shaky, but admissible[,] evidence." *Shaw*, No. CR-13-575691, slip op. at 6. Therefore, the court's determination of reliability cannot, without more, justify denying the defendant's motion to compel. The court may have been influenced by the parties' briefing on the trade secret evidentiary privilege. *See* Motion to Quash at 7-9, *Shaw*, No. CR-13-575691 (Ohio Ct. C.P. Cuyahoga Cty. June 19, 2014) [hereinafter *Shaw* Motion to Quash] (arguing that the requested "information is privileged and protected" under a trade secret theory).

For Pennsylvania, see *Robinson*, No. CC 201307777, slip op. at 1-3 (denying the defense request for TrueAllele source code that the court deemed to be "the intellectual property of Cybergenetics," reasoning in part that the code was immaterial and in part that ordering disclosure would be unreasonable because it "would cause irreparable harm to the company, as other companies would be able to copy the code and potentially put [the developer] out of business").

footnote continued on next page

Notably, courts sometimes do not admit evidence produced by trade secret systems in the first place. For example, in one recent case, a court found that the alleged trade secret status of a forensic method should weigh against the admissibility of its results.[81] In that case, it was the defendant, not the prosecutor, who sought to introduce the evidence.[82] The defendant was charged with child molestation and moved to introduce the results of an automated assessment showing that he was not sexually attracted to children.[83] The California appeals court excluded the evidence, finding that the "closely-guarded proprietary" nature of the test was one of three factors that "undermine[d] the evidentiary value" of the results.[84]

Trade secret claims are not limited to any particular category of forensic technology. The algorithms that generate candidate matches for latent

For Washington, see State v. Fair, No. 10-1-09274-5 SEA, slip op. at 9 (Wash. Super. Ct. King Cty. Jan. 12, 2017) ("[T]he usefulness of disclosing the source code is outweighed by a substantial risk of financial harm to [the developers, who] have a legitimate interest in keeping the source code, a trade secret, confidential.").

Federal courts have been notably less receptive to trade secret privilege claims in criminal cases. *See, e.g.*, United States v. Johnson, No. 1:15-cr-00565-VEC, slip op. at 1 (S.D.N.Y. July 6, 2016) (ordering FST source code information disclosed and questioning even the need for a protective order); United States v. Diakhoumpa, 171 F. Supp. 3d 148, 151 (S.D.N.Y. 2016) (ordering discovery, subject to a protective order, for "valuable trade secret information" that formed the basis of an expert witness's opinion); United States v. Durst, No. 15-091, 2015 WL 4879465, at *3-4 (E.D. La. Aug. 14, 2015) (ordering disclosure, under a protective order, of Marriott's employee handbook, despite Marriott's argument that it was a trade secret whose disclosure "could put it at disadvantage with its competitors," because "Rule 17(c) does not address this issue, and there is no rule of criminal procedure that addresses it either," and because Marriott had failed to show the validity of the trade secret (citing FED. R. CRIM. P. 17(c))); United States v. Ocasio, No. EP-11-CR-2728-KC, 2013 WL 2458617, at *5 (W.D. Tex. June 6, 2013) ("[T]he Court finds any claim of trade secret privilege to be inappropriate."); United States v. Grace, 455 F. Supp. 2d 1140, 1147-48 (D. Mont. 2006) (ordering disclosure of documents that the government had sought to withhold under a trade secret theory); *see also* 26 WRIGHT & GRAHAM, *supra* note 40, § 5641, at 287 ("So far as we can tell, there are no federal criminal cases recognizing [a trade secret] privilege.").

[81] *See* People v. Fortin, 218 Cal. Rptr. 3d 867, 873-74 (Ct. App. 2017).

[82] *Id.* at 869.

[83] *Id.*

[84] *Id.* at 873. The court found that because the developer "exercises proprietary rights and refuses to share his formula with other scientists," the test had not been peer-reviewed. *Id.* And because "[t]he process of analyzing responses is closely-guarded proprietary information," the expert witness who sought to testify in reliance on those results was personally unable to analyze them and "would simply be a surrogate for [the developer], instead of providing his '*individual interpretation*' of the test." *See id.* at 874-75 (quoting People v. Stoll, 783 P.2d 698, 705 (Cal. 1989)); *cf. In re* CDK, 64 S.W.3d 679, 683-84 (Tex. App. 2002) (holding, in a civil proceeding for termination of parental rights, that it was error to admit expert testimony about a sex offender risk assessment score where the third-party commercial vendor of the scoring service had disclosed no information about the algorithm or the methods used to produce the score).

fingerprint analysis are proprietary.[85] The algorithms used to search ballistic information databases for firearm and cartridge matches are secret and inaccessible to independent auditors.[86] Trade secrecy is a primary intellectual property protection for source code.[87] So trade secret privilege claims are likely to multiply with the increasing automation of criminal justice decisionmaking.[88]

The examples above show that defendants have struggled unsuccessfully to overcome claims to a trade secret evidentiary privilege even at trial, where their procedural rights are strongest. The next two Subparts describe trade secret technologies that defendants may encounter either before or after trial, when their procedural rights are thin. While defendants' discovery and subpoena powers fluctuate over a case's lifetime,[89] the trade secret evidentiary privilege applies with full force in all judicial proceedings.[90]

B. Pretrial Suppression Hearings

A second category of criminal justice technologies for which developers have claimed trade secrets involves law enforcement investigations. Defendants are likely to rely on pretrial discovery motions and subpoenas to seek information about law enforcement technologies, which defendants could then use in suppression hearings. Because evidentiary privileges apply before trial,[91] developers can assert the trade secret privilege to block these efforts.

For instance, in *United States v. Ocasio*, a software program that scans online networks for files associated with child pornography flagged defendant Angel Ocasio's computer.[92] Ocasio argued that the program violated the Fourth

[85] PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 8, at 89 nn.250-51.

[86] *Id.* at 132-33.

[87] *See* Pamela Samuelson, *The Uneasy Case for Software Copyrights Revisited*, 79 GEO. WASH. L. REV. 1746, 1758 (2011) ("[M]ost of the commercially valuable know-how embedded in programs [is] protected as trade secrets."); *see also* Pamela Samuelson, *Functionality and Expression in Computer Programs: Refining the Tests for Software Copyright Infringement*, 31 BERKELEY TECH. L.J. 1215, 1220-21, 1239-40, 1285 n.390 (2016) (describing elements of computer programs that are uncopyrightable and observing controversies over the "patentability of computer program innovations").

[88] *See, e.g.*, PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 8, at 103 (predicting automated fingerprint analysis).

[89] For instance, defendants may have statutory rights to certain information at arraignments or parole hearings. *See, e.g.*, FED. R. CRIM. P. 10(a) (entitling defendants to arraignment in "open court" and to "a copy of the indictment or information"); N.Y. EXEC. LAW § 259-i(2)(a) (McKinney 2018) (entitling inmates to "be informed in writing . . . of the factors and reasons for . . . denial of parole").

[90] *See* FED. R. EVID. 1101(c).

[91] *See id.*

[92] United States v. Ocasio, No. 3:11-cr-02728-KC, slip op. at 3 (W.D. Tex. June 16, 2013).

Amendment by scanning private folders on his hard drive.[93] To develop this claim, he sought information about how the program works, including its source code and documentation, operation manuals, and training materials.[94] The developer conceded that "[w]ithout the source code, it is not possible to authenticate the function of the application or validate its 'calibration.'"[95] Nonetheless, the federal government and the developer both argued that the information was shielded from subpoena by trade secret laws.[96] In that case, a federal judge found "any claim of trade secret privilege to be inappropriate" and ordered the requested materials disclosed subject to a protective order.[97]

Ocasio illustrates the risk that law enforcement agencies and third-party developers will try to use intellectual property law as a shield against judicial scrutiny, preventing the courts from determining the constitutionality and lawfulness of new investigative technologies.[98] While the strategy ultimately failed in federal court in *Ocasio*, it is arguably succeeding in state jurisdictions. In a California case, defendant Michael Reed tried to subpoena source code for an audio surveillance system called ShotSpotter in order to determine whether the system violated local wiretapping laws by secretly recording conversations spoken at normal speech decibels.[99] ShotSpotter's developer refused to comply,

[93] *See id.* Similar issues are playing out across the country in a series of cases in which the FBI deployed a malware tool to circumvent a computer program that masks the user's IP address. *See, e.g.*, Cyrus Farivar, *Feds May Let Playpen Child Porn Suspect Go to Keep Concealing Their Source Code*, ARS TECHNICA (Jan. 9, 2017, 1:39 PM), https://perma.cc/4HQM-JQRK. At least one federal judge has found that the FBI's malware program constitutes a Fourth Amendment search in that it places trespassory code onto a defendant's computer. *See* United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *3 (W.D. Tex. Sept. 9, 2016).

[94] *See* Motion to Compel Production of Materials Pertaining to Peer-to-Peer Investigative Software at 7, *Ocasio*, No. 3:11-cr-02728-KC (W.D. Tex. Apr. 8, 2013).

[95] Affidavit of William S. Wiltse ¶ 8, *Ocasio*, No. 3:11-cr-02728-KC (W.D. Tex. Apr. 15, 2013).

[96] *See* United States v. Ocasio, No. EP-11-cr-02728-KC, 2013 WL 2458617, at *4 (W.D. Tex. June 6, 2013); United States v. Ocasio, No. 3:11-cr-02728-KC, slip op. at 2 (W.D. Tex. May 28, 2013).

[97] *Ocasio*, 2013 WL 2458617, at *5-6.

[98] Private companies may claim that they are not state agents and are thus free from Fourth Amendment and other constitutional restrictions, are beyond the reach of discovery statutes, and are exempt from disclosure obligations under *Brady v. Maryland*, 373 U.S. 83 (1963). But these arguments may not prevail. *Cf.* United States v. Ackerman, 831 F.3d 1292, 1295-96 (10th Cir. 2016) (Gorsuch, J.) (applying the Fourth Amendment to the search of an email attachment by a private entity, the National Center for Missing and Exploited Children (NCMEC), in part because the NCMEC has statutory obligations that give it a type of quasi-governmental status).

[99] *See* Letter from Mike Will to Jeff Adachi & Michelle Tong, *supra* note 50, at 1, 3 (refusing to comply with a defense request for source code for "any and all software that allows the sensors to distinguish between gunshots and ambient noise"); *see also* *Shot-Spotter Is Listening to More Than Just Gun Violence*, PRIVACY SOS (Jan. 12, 2012),

footnote continued on next page

claiming that the information was privileged as a trade secret.[100] Defendant Todd Gillard also tried to subpoena alleged trade secret information about ShotSpotter's methodology.[101] ShotSpotter argued for the same heightened privilege burden that was ultimately adopted in *Chubbs*,[102] contending that while Gillard had shown that the types of documents he requested "may be broadly *relevant* to challenge or impeach evidence derived from the Shotspotter System, he ha[d] not established that they are *necessary* for such purpose."[103] The court ultimately found that Gillard's "Sixth Amendment rights to compulsory process, to call witnesses, to cross-examine the People's witnesses, and to present a defense" required the information to be disclosed under a protective order, but in the process the court also endorsed ShotSpotter's legal theory of the trade secret privilege in criminal proceedings.[104]

In addition to facilitating law enforcement evasion of judicial scrutiny, trade secret claims may also motivate—or even compel—such evasion; companies may require law enforcement agencies to conceal the use of their products or engage in "parallel construction," in which police disguise the actual methods they use by describing alternative ones, in order to protect sensitive information from courtroom disclosure.[105] In a recent example that has been well analyzed by Elizabeth Joh, the Federal Bureau of Investigation (FBI) required police departments to sign nondisclosure agreements promising to conceal information about cellphone surveillance tools known as "stingrays"—including how the devices work and even the mere fact that they

https://perma.cc/XDY3-6FER (identifying the legal theory that ShotSpotter might violate state wiretapping laws).

[100] *See* Letter from Mike Will to Jeff Adachi & Michelle Tong, *supra* note 50, at 1, 3.

[101] *See* Protective Order at 1, People v. Bernstine, No. 1-164044-0 (Cal. Super. Ct. Contra Costa Cty. Jan. 17, 2014).

[102] *See supra* notes 63-68 and accompanying text.

[103] *See* Proposed Order at 3, People v. Gillard, No. 1-164044-0 (Cal. Super. Ct. Contra Costa Cty. Jan. 16, 2014) (emphasis added). The defense attorney in *Gillard* informed me that the proposed order was filed with the court on January 16, 2014. Email from John Hamasaki to author (Apr. 22, 2018) (on file with author).

[104] *See* Protective Order, *supra* note 101, at 3 ("[T]he party seeking discovery 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 in the case . . . ." (emphasis added)).

[105] *See* HUMAN RIGHTS WATCH, DARK SIDE: SECRET ORIGINS OF EVIDENCE IN US CRIMINAL CASES 40-41, 57-58 (2018), https://perma.cc/L8LM-AB3L (hypothesizing that government agencies may consider parallel construction to be legal if their alternative sources for evidence are sufficiently attenuated but concluding that parallel construction violates constitutional rights to a fair trial). My proposal to eliminate any criminal trade secret privilege could increase pressure on law enforcement to use parallel construction in order to avoid disclosure of trade secrets in court.

exist—from defendants, courts, legislatures, and the public alike.[106] Two local police departments in Florida established a policy of describing stingrays as "confidential informants."[107] When the information finally surfaced, multiple judges held that using a stingray requires a warrant supported by probable cause.[108] Secrecy around these devices thus enabled police to perform what some courts later deemed unconstitutional searches—for nearly a decade and as a matter of course—while evading judicial review.[109] Of course, that secrecy may have been motivated in part by a desire to ensure the efficacy of the tool; as with algorithms that flag Internal Revenue Service filings for audits, concealing information about how law enforcement investigative tools work is sometimes necessary to prevent would-be criminals and fraudsters from circumventing them.[110] But with stingrays, trade secrecy was also a factor. As Joh points out, when the developer submitted the device for regulatory approval, it requested that details about how the technology works be kept secret "to protect its proprietary information from competitors."[111]

Other areas where developers may assert trade secret evidentiary privileges before trial include defense challenges to face recognition systems and predictive policing tools.[112] Police departments have cited trade secrets as reason to deny open records requests for face recognition user manuals and audit information.[113] User manuals could reveal information relevant to

[106] *See* Joh, *supra* note 25, at 103, 105-08, 111; *see also* Spencer McCandless, Note, *Stingray Confidential*, 85 GEO. WASH. L. REV. 993, 1006 (2017) (discussing how "prosecutor[s] avoid[] the disclosure of stingray surveillance by asserting the informant's privilege" and thus "deliberately mislead[] the court[s] to believe that the information gained from the surveillance originated from a human source who was not a state actor").

[107] *See* Joh, *supra* note 25, at 111.

[108] *See, e.g.*, United States v. Ellis, 270 F. Supp. 3d 1134, 1142-46 (N.D. Cal. 2017); United States v. Lambis, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016); Jones v. United States, 168 A.3d 703, 707 (D.C. 2017); People v. Gordon, 68 N.Y.S.3d 306, 310-11 (Sup. Ct. 2017).

[109] *See NYPD Has Used Stingrays More Than 1,000 Times Since 2008*, NYCLU (Feb. 11, 2016), https://perma.cc/M2KA-DGNA.

[110] *See* Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 658 (2017); *see also* 5 U.S.C. § 552(b)(7) (2016) (exempting from Freedom of Information Act requests any "records or information compiled for law enforcement purposes" to the extent such records "would disclose techniques and procedures for law enforcement investigations or prosecutions"). For the Freedom of Information Act, see Pub. L. No. 89-487, 80 Stat. 250 (1966) (codified as amended at 5 U.S.C. § 552).

[111] *See* Joh, *supra* note 25, at 106.

[112] *See, e.g.*, *id.* at 119, 124-25.

[113] *See* Letter from Jordan S. Mazur, Records Access Appeals Officer, Police Dep't, N.Y.C., to Clare Garvie, Ctr. on Privacy & Tech. 1 (Jan. 4, 2017) (on file with author); Letter from Nathaniel McQueen, Jr., Superintendent, Div. of State Police, State of Del., to Clare Garvie, Ctr. on Privacy & Tech. 2 (Nov. 9, 2016) (on file with author); Letter from Tonya Peters, Police Legal Advisor, Lincoln Police Dep't, City of Lincoln, to Clare Garvie, Ctr. on Privacy & Tech. 1 (Jan. 22, 2016) (on file with author); Letter from

footnote continued on next page

determining a system's error rate and potential for bias, such as whether it 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 but not others.[114] Predictive policing systems, which may rely on historical data to model the likelihood of future crimes, can be similarly opaque.[115] Defendants seeking to challenge the accuracy or privacy-invasiveness of these systems,[116] to argue that police may not rely on these systems to satisfy reasonable suspicion for a stop or probable cause for an arrest,[117] or to contend that these systems are systematically biased on the basis of race or other factors[118] should anticipate trade secret barriers to developing their claims.

C. Bail and Sentencing

The third branch of criminal justice technologies that could implicate the trade secret privilege involves actuarial "risk assessment instruments" that purport to predict recidivism. Decisionmakers use these tools to help determine whether to set bail before trial and what sentence to impose.[119] Most rules of evidence do not apply in bail or sentencing hearings.[120] For instance,

Roxann M. Ryan, Comm'r, Iowa Dep't of Pub. Safety, to Clare Garvie, Ctr. on Privacy & Tech. 2 (Apr. 1, 2016) (on file with author).

[114] *See* GARVIE ET AL., *supra* note 11, at 54-55.

[115] *See generally* Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103 (2018). Predictive systems may rely on historical data, which in itself can be opaque. *See* Ezekiel Edwards, *Predictive Policing Software Is More Accurate at Predicting Policing Than Predicting Crime*, HUFFPOST (Aug. 31, 2016, 2:58 PM ET), https://perma.cc/UJA8-H2G7.

[116] *Cf.* GARVIE ET AL., *supra* note 11, at 1 (noting that face recognition poses risks "to privacy, civil liberties, and civil rights"); Nissa Rhee, *Study Casts Doubt on Chicago Police's Secretive "Heat List,"* CHICAGO (Aug. 17, 2016), https://perma.cc/YC55-DH4P.

[117] *Cf.* Andrew Guthrie Ferguson, *Crime Mapping and the Fourth Amendment: Redrawing "High-Crime Areas,"* 63 HASTINGS L.J. 179, 209 (2011) ("[B]y predetermining a place of expected generalized criminal activity, the high-crime area designation leads to a lower standard of suspicion in practice."); Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259, 304-05 (2012) (examining how courts may take predictive policing results into account when conducting reasonable suspicion analysis).

[118] *Cf.* Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 909, 922 & n.357 (2016).

[119] *See, e.g.*, SHARON LANSING, OFFICE OF JUSTICE RESEARCH & PERFORMANCE, N.Y. STATE DIV. OF CRIMINAL JUSTICE SERVS., NEW YORK STATE COMPAS-PROBATION RISK AND NEED ASSESSMENT STUDY: EXAMINING THE RECIDIVISM SCALE'S EFFECTIVENESS AND PREDICTIVE ACCURACY 1 (2012), https://perma.cc/U256-NE45 (introducing COMPAS as a software package that helps officials make decisions at various stages in the criminal justice system, including pretrial release, probation supervision, and punishment).

[120] *See, e.g.*, FED. R. EVID. 1101(d)(3).

judges resolving factual disputes at sentencing may consider hearsay statements and scientific evidence even of the variety that would be inadmissible at trial.[121] Evidentiary privileges are the exception in that they "apply to all stages of a case or proceeding."[122] Thus, to the extent defendants have statutory or constitutional rights to view or introduce evidence during these proceedings, the trade secret evidentiary privilege would apply.[123]

I have not yet encountered examples of cases where the evidentiary privilege was claimed in a bail or sentencing hearing. However, as the use of trade secret risk assessment instruments increases, I anticipate that defendants will try to subpoena developers at these stages and that developers will assert the privilege in response. Defendants have already faced trade secret obstacles to challenging their risk assessment scores that were not explicitly privilege based. For example, Eric Loomis was sentenced to six years in prison based on a predictive computer system that indicated he had a "high risk of recidivism."[124] Loomis suspected that the tool considered gender as a factor in assessing risk and accordingly brought a due process challenge.[125] But the developer claimed that details about how the system weights and calculates input variables are trade secrets.[126] The Wisconsin Supreme Court acknowledged that the trade secret barriers prevented Loomis from determining precisely how the system accounts for gender but found that his due process challenge nonetheless failed because, among other reasons, Loomis and the judge had equally limited access to the trade secret information.[127] The opinion did not mention that a

[121] *See, e.g.*, United States v. Malone, 828 F.3d 331, 336-37 (5th Cir. 2016) (holding that to be admissible during sentencing hearings, scientific studies need not meet the standard introduced in *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993)); United States v. Martin, 287 F.3d 609, 618 (7th Cir. 2002) (holding that uncorroborated hearsay statements are admissible at sentencing hearings).

[122] *See, e.g.*, FED. R. EVID. 1101(c).

[123] The Federal Rules of Criminal Procedure contemplate witness testimony at preliminary hearings, suppression hearings, sentencing hearings, probation and supervised release hearings, and detention hearings in addition to trial. *See* FED. R. CRIM. P. 26.2(g). At sentencing hearings, defendants may be able to subpoena evidence or witness testimony, subject to the discretion of the sentencing court. *See, e.g.*, United States v. Olhovsky, 562 F.3d 530, 544 (3d Cir. 2009) (holding that the trial "court's determination that it could not allow [a defense expert witness] to be subpoenaed for the sentencing hearing was erroneous" and observing that Rule 17 of the Federal Rules of Criminal Procedure "governs the issuance of subpoenas in criminal cases," including at sentencing).

[124] *See* State v. Loomis, 881 N.W.2d 749, 755, 756 n.18 (Wis. 2016), *cert. denied*, 137 S. Ct. 2290 (2017).

[125] *See id.* at 757, 765. Loomis also argued that the use of the risk assessment violated due process in his case because it violated his "right to be sentenced based upon accurate information" along with his "right to an individualized sentence." *Id.* at 757.

[126] *See id.* at 761.

[127] *See id.* at 761, 765.

defendant's and a judge's incentives to scrutinize such a system might differ, or that only one chooses to rely on the system while blind to its methodology.

There are at least two additional types of claims I anticipate defendants will make to challenge risk assessment scores. With each, defendants seeking to subpoena trade secrets will likely encounter assertions of the evidentiary privilege in response. First, defendants may argue that the tools are inappropriate for use with certain subpopulations. Similar arguments have already been made in noncriminal proceedings, and parties making such arguments have encountered trade secret obstacles. For instance, a New York judge determined that a risk assessment instrument sold by the same company as the one at issue in *State v. Loomis* was not adequately tailored for individuals with mental illness.[128] But when the Urban Justice Center—which represents mentally ill clients—tried to obtain instruction manuals, training guides, and scoring information for that tool, its request was denied under the trade secret exemption from the state freedom-of-information law.[129]

Second, defendants will likely claim that they need access to the tools' input weights and calculation methods in order to prove the significance of individual input errors. Again, similar arguments have already been made in noncriminal proceedings. When inmate Glenn Rodríguez was denied parole, he had a statutory right to be informed in writing of the "factors and reasons" for the denial.[130] Rodríguez filed a grievance showing that there was an error in one of the inputs used to generate his risk assessment score.[131] The tool relies on manual inputs from surveys filled out by a human evaluator.[132] In Rodríguez's case, the evaluator had checked "yes" where he should have checked "no" in one survey response.[133] Rodríguez knew that when another

[128] *See* Hawthorne v. Stanford, No. 0811-14, 2014 WL 4054013, slip op. at 6 (N.Y. Sup. Ct. May 27, 2014) ("Respondent's misuse of the COMPAS failed to accommodate for Petitioner's severe and ongoing mental illness in measuring his prison misconduct and violence scores . . . ."), *aff'd in part, rev'd in part*, 22 N.Y.S.3d 640 (App. Div. 2016).

[129] *See* Letter from Chad Powell, Admin. Assistant, N.Y. State Dep't of Corr. & Cmty. Supervision, to Jennifer Parish, Urban Justice Ctr. (Mar. 6, 2014) (on file with author); *see also* N.Y. PUB. OFF. LAW § 2(d) (McKinney 2018) (exempting trade secrets and similar commercially valuable information).

[130] *See* N.Y. EXEC. LAW § 259-i(2)(a) (McKinney 2018). For a discussion of Rodríguez's case, see Wexler, *supra* note 12.

[131] Letter from Glenn Rodríguez to Inmate Grievance Resolution Comm., *supra* note 51, at 1-2.

[132] *See, e.g.*, LANSING, *supra* note 119, app. A at 20-28.

[133] *Compare* N.Y. State Dep't of Corr. & Cmty. Supervision, Risk Assessment of Glenn Rodríguez 2 (2016) (on file with author) (wrongly indicating that Rodríguez "appear[ed] to have notable disciplinary issues"), *with* N.Y. State Dep't of Corr. & Cmty. Supervision, Disciplinary History of Glenn Rodríguez (2016) (on file with author) (showing that Rodríguez "ha[d] not had any disciplinary infractions over the past decade (2006-2016)").

inmate had received a reassessment to correct the same error, that person's final risk score dropped significantly.[134] But Rodríguez could not prove that the error had any significant effect in his own case because the weights of the input variables are alleged trade secrets.[135] Ultimately, he was unable to convince anyone to correct the mistake and had to return to the parole board six months later with the same erroneous score.[136]

Like automated forensic methods and investigative technologies, trade secret claims concerning the details of risk assessment methodologies are likely to be made more frequently in the future. One reason is that aspects of automated tools may be deemed nonpatentable subject matter, making trade secret protections comparatively attractive.[137] Both private and public developers may also be wary of sharing information about criminal justice technologies for fear that their tools will be deemed weak or vulnerable to challenge.[138] Private commercial vendors, nonprofit foundations, and government agencies have all developed risk assessment instruments.[139] Even noncommercial entities have refused to fully disclose information about how their tools are built.[140]

D. Arguments Favoring Secrecy

The owner of the company that manufactures the software at issue in *Chubbs*[141] and other trade secret privilege cases has outlined three main

[134] *See* Wexler, *supra* note 12.

[135] *Cf.* State v. Loomis, 881 N.W.2d 749, 761 (Wis. 2016), *cert. denied*, 137 S. Ct. 2290 (2017) (noting that "COMPAS does not disclose" how "risk scores are determined or how the factors are weighed").

[136] *See* Wexler, *supra* note 12; Telephone Interview with Glenn Rodríguez (Mar. 13, 2017).

[137] *See, e.g.*, Novak & Frontz, *supra* note 28.

[138] *See* Jessica M. Eaglin, *Constructing Recidivism Risk*, 67 EMORY L.J. 59, 111-12 (2017).

[139] *See, e.g.*, Interview by Ctr. for Court Innovation with Jerry McElroy, Exec. Dir., Criminal Justice Agency (July 2012), https://perma.cc/J5Y6-XA6Z; Northpointe, Northpointe Suite (n.d.), https://perma.cc/QW2F-SL74; *Public Safety Assessment*, LAURA & JOHN ARNOLD FOUND., https://perma.cc/6Q9N-ZXE7 (archived Apr. 5, 2018); *Special Order S09-11: Strategic Subject List (SSL) Dashboard*, CHI. POLICE DEP'T (July 14, 2016), https://perma.cc/TPF2-2MZ2.

[140] *See, e.g.*, Tom Simonite, *When Government Rules by Software, Citizens Are Left in the Dark*, WIRED (Aug. 17, 2017, 7:00 AM), https://perma.cc/W4QD-ZJE8 (stating that according to a spokesperson from the John and Laura Arnold Foundation, "the foundation initially required confidentiality from jurisdictions to inhibit governments or rivals from using or copying the tool without permission"). The Arnold Foundation is "a Texas nonprofit that works on criminal-justice reform." *Id.*

[141] *See supra* notes 57-60 and accompanying text.

arguments in support of the pro-secrecy position.[142] The first details the tragic nature of the crimes that the defendants in these cases allegedly committed and touts the benefits of its technology in fighting such crimes.[143] A firm tenet of the U.S. criminal justice system, however, is that neither the details of a criminal charge nor the benefits of a new technology lessen an accused's rights to procedural protections. This Article seeks to address a different question: whether intellectual property rights should limit those procedural safeguards.

The company's second contention warrants deeper discussion. It claims that defendants do not *need* to review the trade secret source code for its software system because that system has been scientifically validated in peer-reviewed studies and because the company has disclosed other information about the system's methodology for defendants to review.[144] I address below whether *necessity*, as opposed to relevance or materiality, is the proper legal burden to apply to defendants' discovery and subpoena motions.[145] Here, I offer an initial response to the company's reliance on scientific arguments from beyond the legal domain.

The sufficiency of existing validation studies for forensic DNA analysis systems, like the one at issue in *Chubbs*, is subject to expert debate. Forensic software programs used to analyze DNA in complex scenarios—such as with minute "low copy" DNA samples, degraded samples, or mixtures of DNA from multiple contributors—are emerging methods that push the boundaries of established DNA science.[146] Competing software programs have produced divergent results from identical test samples.[147] In a recent homicide case, two software programs reached different conclusions regarding whether a defendant's DNA was included in a crime scene sample.[148] And existing

[142] *See Computers Are Helping Justice*, CYBERGENETICS (June 16, 2017), https://perma.cc/XNW3-Q4A6 (reproducing an op-ed that a Cybergenetics doctor submitted to the *New York Times* in response to Wexler, *supra* note 5). The company has presented similar arguments in court. *See, e.g.*, Declaration of Mark W. Perlin ¶¶ 74, 82, State v. Fair, No. 10-1-09274-5 SEA (Wash. Super. Ct. King Cty. Apr. 1, 2016).

[143] *See Computers Are Helping Justice*, *supra* note 142.

[144] *See id.*

[145] *See infra* Part III.A.2.

[146] *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 8, at 82 (observing that probabilistic software programs that analyze complex DNA mixtures are "new and promising" but that "[e]mpirical evidence is required to establish the foundational validity of each such method within specified ranges").

[147] *See* 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: GENETICS SUPPLEMENT SERIES 422, 423 (2015).

[148] *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 8, at 79 n.212 (noting that examiners' use of two different DNA software programs, STRmix and TrueAllele, produced different conclusions); *see also* President's Council of Advisors on Sci. & Tech., An Addendum to the PCAST Report on Forensic Science in Criminal Courts 8 (2017),

footnote continued on next page

validation studies have been critiqued for their limited independence and scope.[149] Further, there is no universally accepted statistical method to analyze this kind of complex DNA sample.[150] Software developers must therefore choose not only how to implement a statistical model through code but also which model of the underlying biological phenomena to use.[151] Given the uncertainties surrounding these forms of DNA analysis, defendants have been particularly concerned with their ability to scrutinize the source code that purports to implement these methods.[152]

Whether and when source code access can be valuable is also a matter of expert debate. On the one hand, some argue that source code transparency should be required for scientific peer review and experimental reproducibility;[153] that analyzing source code can reveal significant facts about a program;[154] and that using source code in conjunction with test inputs is a powerful method to find bugs and to ensure correct functioning.[155] On the other hand, code review could be insufficient: It can be extraordinarily difficult

https://perma.cc/VQ32-J6RB [hereinafter PCAST Report Addendum] (same). The developer of STRmix observed that "STRmix included [while] TrueAllele [was] inconclusive" and commented that there was some uncertainty about the sample tested. Email from John Buckleton, STRmix, to author (Feb. 22, 2017, 2:20 PM) (on file with author).

[149] *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 8, at 80 ("[M]ost of the studies evaluating software packages have been undertaken by the software developers themselves . . . [and] have adequately explored only a limited range of mixture types . . . .").

[150] *See, e.g.*, Garofano et al., *supra* note 147, at 422 (noting that scientists have not reached consensus on the methodology for interpreting low-template DNA).

[151] PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 8, at 79 ("[T]he programs employ different mathematical algorithms and can yield different results for the same mixture profile.").

[152] *See, e.g.*, Matt Tusing, *Machine-Generated Evidence: Preserving an Appealable Issue*, 43 REPORTER, no. 1, 2016, at 13, 15-17 (describing cases in which courts have ordered review of the source code in forensic devices); Lauren Kirchner, *Where Traditional DNA Testing Fails, Algorithms Take Over*, PROPUBLICA (Nov. 4, 2016, 8:00 AM EDT), https://perma.cc/K6W9-SJF7.

[153] *See, e.g.*, Darrel C. Ince et al., Perspective, *The Case for Open Computer Programs*, 482 NATURE 485, 485 (2012) ("[A]nything less than release of actual source code is an indefensible approach for any scientific results that depend on computation . . . ."); A. Morin et al., *Shining Light into Black Boxes*, SCIENCE, Apr. 13, 2012, at 159, 159-60 ("In the absence of source code, the inner workings of a program cannot be examined, adapted, or modified.").

[154] *See, e.g.*, Kroll et al., *supra* note 110, at 648 n.41 (asserting that code analysis can reveal different conditional behaviors for inputs above or below a threshold).

[155] *See, e.g.*, *id.* at 661 & n.91 (noting the benefits of a technique called "white-box testing"); Sean Gallagher, *Microsoft Launches "Fuzzing-as-a-Service" to Help Developers Find Security Bugs*, ARS TECHNICA (Sept. 27, 2016, 8:21 AM), https://perma.cc/PN47-D37G.

even for experts;[156] it cannot guarantee the absence of all types of flaws;[157] and it is ill suited to auditing machine learning systems.[158] That said, common alternatives to code review also have limits. For instance, "black-box testing"—which uses known inputs, outputs, and knowledge of the general function of a system but not of its internal contents or implementation—is limited by the volume and scope of known test inputs,[159] the difficulty of testing for unforeseen circumstances,[160] and the possibility of fraud if systems can be programmed to perform differently when tested.[161] Similar debates exist over the utility and necessity of transparency for different elements of machine learning systems, including training data, algorithms, and models that are expressions of the data and algorithms combined.[162]

[156] *See* Kroll et al., *supra* note 110, at 649-50.

[157] *See, e.g.*, *id.* at 659 (observing the limits of code review for detecting flaws in systems that incorporate "some element[s] of randomness").

[158] *See id.* at 638, 659-60. Code review could be unnecessary if systems are designed with alternative computational accountability mechanisms that provide functional guarantees. *See, e.g.*, *id.* at 665-67 (describing "cryptographic commitments" as a mechanism that locks in the current secrets of a program so that the code and inputs used in a particular case can be unsealed and reviewed at a later time); *id.* at 668-72 (describing "zero-knowledge proofs" as a mechanism to guarantee that the system's actual actions fit a description, without requiring transparency as to the system's source code or inputs and outputs).

[159] *See, e.g.*, Imwinkelried, *supra* note 20, at 123 (proposing the concept of a "range of validation" to evaluate the limits of black-box validation studies in certain cases); John Logan Koepke & David G. Robinson, *Danger Ahead: Risk Assessment and the Future of Bail Reform*, 93 WASH. L. REV. (forthcoming 2018) (manuscript at 24-31) (on file with author) (noting problems with validating risk assessment instruments using obsolete or foreign data); *see also* Simson Garfinkel et al., *Bringing Science to Digital Forensics with Standardized Forensic Corpora*, 6 DIGITAL INVESTIGATION S2, S2 (2009) (identifying a crisis in the reproducibility of digital forensic research results because researchers lack standardized data sets necessary to validate new techniques).

[160] *See, e.g.*, Kroll et al., *supra* note 110, at 650 (observing that a finite number of test inputs cannot verify all possible situations).

[161] *See, e.g.*, Megan Geuss, *A Year of Digging Through Code Yields "Smoking Gun" on VW, Fiat Diesel Cheats*, ARS TECHNICA (May 28, 2017, 9:00 AM), https://perma.cc/BW8M-WVN6 (discussing a source code "defeat device" that allowed Volkswagen and Audi to cheat emissions tests).

[162] *See, e.g.*, Simmons, *supra* note 15, at 994-99, 997 n.202 (disavowing the need for source code transparency but advocating for transparency when it comes to training data, algorithms, and model input factors and weights, arguing that such transparency is necessary to improve accuracy, guarantee that decisions are sufficiently individualized, "reassure" the public and the courts, and ensure that systems do not rely on forbidden factors such as race). Black-box validation studies may be ill suited to identify racial bias in risk assessment instruments because systemic biases in historical data can incorrectly appear to validate those same biases in present tests. *See* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 3, 96-97 (2016); *see also* Laurel Eckhouse et al., Layers of Bias: A Unified Approach for Understanding Problems with Risk Assessment 21-24 (Jan. 19,

footnote continued on next page

Expert debates around these issues highlight that what is relevant to scientists and what is relevant to legal decisionmakers are not always coextensive.[163] Scientific conclusions about the reliability of a technology—whether drawn from validation studies, code review, or otherwise—affect the *admissibility* of expert evidence in court.[164] For instance, Jennifer Mnookin, writing about an earlier wave of litigation concerning the disclosure of source code in breath test devices, concluded that courts determining the admissibility of scientific evidence should prioritize validation studies over scrutinizing the inner workings of "black box" methods.[165] But admitted evidence is still subject to challenge and cross-examination as to weight;[166] additional information may be *legally relevant* to vindicate that process. Therefore, evaluating new technologies exclusively from the perspective of scientific peer review does not adequately account for criminal defendants' interests in contesting those tools.

Put another way, scientific relevance is a floor, not a ceiling, with respect to legal relevance. This distinction is well founded; the incentives that shape the production of scientific consensus differ from the risks and obligations inherent in criminal cases.[167] Scientists may care about accuracy, validity, error rates, funding, and perhaps commercialization. Lawyers may care about some of those but may also care about other issues such as fairness, contestability, equality, and privacy. Relevance must therefore expand from a scientific to a legal context. If the scientific method marked the limits of criminal procedure, the adversarial justice system would not be necessary.

In terms of legal relevance to claims about admitted evidence, Edward Imwinkelried, Natalie Ram, Andrea Roth, and Christian Chessman have each

2018) (unpublished manuscript) (on file with author) ("Transparency in *both* risk scoring and training data is a necessity for researchers to be able to vet risk assessment instruments.").

[163] *Cf.* Scott Brewer, *Scientific Expert Testimony and Intellectual Due Process*, 107 YALE L.J. 1535, 1570 (1998) ("The facts that are salient from [scientific] expert points of view will by no means always be the same as the facts that are salient from some practical point of view, such as a legal or moral point of view.").

[164] *See, e.g.*, Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 592-95 (1993) (presenting a nonexclusive list of factors—including scientific testing, peer review, known or potential error rate, and widespread acceptance by a relevant scientific community—a judge may consider in determining whether to admit expert testimony).

[165] *See* Mnookin, *supra* note 36, at 344, 351-56.

[166] *See* FED. R. EVID. 702 advisory committee's note to 2000 amendment (observing that "rejection of expert testimony is the exception rather than the rule" and that the court's gatekeeper function should not substitute for the role of the adversary system); *Daubert*, 509 U.S. at 596 ("Vigorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence.").

[167] Thank you to Jack Balkin for this point.

detailed scenarios in which access to source code could be relevant to maintaining procedural rights to cross-examination and due process as well as to determining a forensic software program's accuracy and reliability.[168] Richard Torres has argued that the Confrontation Clause requires access to source code in forensic technologies because code is a form of speech that can be testimonial.[169] I have also previously asserted that defendants should be granted access to source code.[170] More transparent testing may be rhetorically persuasive; when a leading vendor of predictive policing software, PredPol, published its algorithm in a peer-reviewed journal,[171] independent data scientists were able to reimplement the algorithm and produce the first empirical evidence illustrating how such systems can exacerbate racial biases in historical data.[172] But scientists need not consider any of the legal concerns presented by criminal prosecutions. Hence, arguments from the scientific domain do not settle the degree of transparency required in law.

This Article does not purport to resolve these debates. It simply proposes that the trade secret status of information should not affect the analysis whether that information is legally relevant. In other words, I do not advocate for special discovery rules that would require extra transparency in source code, data, algorithms, or models. Rather, I argue that these elements of computer systems, like other kinds of trade secrets, should not receive special protections from disclosure solely by virtue of their status as intellectual property. Normal discovery and subpoena rules, not privilege rules, should apply.

[168] *See* Imwinkelried, *supra* note 20, at 120-24 (arguing that for cases whose facts lie at the edge of the range of validation, "access to an automated forensic technique's source code would be one of the most effective ways to enable the opponent" to adequately conduct cross-examination); Ram, *supra* note 25, at 32, 40 (arguing that "lack of access to source code yields lower quality code, lower confidence in that code, and less follow-on innovation to create better code" and that "source code should be disclosed for purposes of . . . cross-examination and impeachment"); Roth, *Machine Testimony*, *supra* note 20, at 2027-28; Chessman, *supra* note 20, at 199-219.

[169] *See* Richard Torres, The Legal Aid Soc'y, Is Source Code Speech Under the Confrontation Clause? 13 (n.d.), https://perma.cc/XJ6Y-JANE; *see also* Crawford v. Washington, 541 U.S. 36, 51-53 (2004) (developing the Court's modern Confrontation Clause doctrine, which prohibits admitting "testimonial" hearsay evidence against a criminal defendant unless certain conditions are met).

[170] *See* Wexler, *supra* note 20.

[171] *See* G.O. Mohler et al., *Randomized Controlled Field Trials of Predictive Policing*, 110 J. AM. STAT. ASS'N 1399, 1400-02 (2015).

[172] Kristian Lum & William Isaac, *To Predict and Serve?*, SIGNIFICANCE, Oct. 2016, at 14, 16-19; *cf.* ROBINSON & KOEPKE, *supra* note 7, at 5 (cautioning that predictive systems "may not account for the [race-based] inaccuracies reflected in historical data, leading to a cycle of self-fulfilling prophecies").

Returning, then, to the technology at issue in *Chubbs*: The company's third key contention is that "privileged information benefits society" and that just like privileges for attorney-client and reporter-source communications, the "same law protects trade secrets."[173] The remainder of this Article addresses that claim. My interest lies in evaluating whether and how trade secrets in new criminal justice technologies may impede modes of argument that were previously available to defendants. One way trade secrets might do so is by shifting the legal burden that a defense discovery or subpoena motion must meet from an easier showing of relevance to a more onerous showing of necessity. If evidence is *certain* to be irrelevant, then denying defendants access to it can do little harm. But when evidence *might* be relevant, the precise ex ante burden defendants must meet in order to compel disclosure can matter a great deal. In my view, intellectual property should not receive such special treatment.

In the next Part, I outline the history of the trade secret privilege, first in civil disputes and then more recently in criminal proceedings. I call into question the foundations of the general acceptance that the privilege currently enjoys in civil proceedings and show that its application in criminal cases remains doctrinally undetermined. I then argue in Part III that the privilege should not extend to criminal cases.

II. Histories of the Trade Secret Privilege

At first glance, today's pro-privilege view 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 rulemakers who codified the privilege branded it with a venerable pedigree. They referred to legal luminaries and, as time progressed, they began to refer to 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 opposition. The general acceptance of the privilege today is a measure of their success.

On close inspection, however, previously underscrutinized 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 view in favor of the privilege. I draw from newly digitized historical documents and other archival sources to assess how the lawmakers and rulemakers behind the codification movement used historical authority as

[173] *Computers Are Helping Justice*, *supra* note 142.

well as how those uses 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 rulemaking 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 secret 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 two main goals. My principal objective is to show that the standards currently governing the trade secret privilege developed in and for civil disputes. Whether and to what extent these standards do or should apply in criminal proceedings is a recent, undertheorized, and open legal question. Criminal trial courts have presumed that because these standards apply in civil cases, they should necessarily extend to criminal cases. But in fact, in most common law jurisdictions no binding appellate authority yet requires courts to apply the privilege to criminal cases. And even in statutory jurisdictions, it is often unclear whether the privilege requires a total withholding remedy or merely entitles trade secret holders to protective or sealing orders that limit the distribution of evidence after it has been disclosed to the defense.

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.

A. The Civil Trade Secret Privilege

A 1970 note by the Advisory Committee on the Rules of Evidence perhaps best captures the general tone of legislative histories of the trade secret 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."[174] The note offers a series of impressive citations to support this claim: to prior codifications of the privilege in California, Kansas, New Jersey, and the Uniform Rules of Evidence; to a series of treatises including John Henry

[174] Proposed Fed. R. Evid. 508 advisory committee's note, 56 F.R.D. 183, 250 (1972). Congress later rejected the proposed Rule 508 amid heated political charges that the rule—along with other proposed privileges—served lobbyists and special interests. *See* Edward J. Imwinkelried, *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*, 58 ALA. L. REV. 41, 47-52 (2006).

Wigmore's influential treatise on evidence law; and to a long list of common law cases "raising trade-secrets problems," including a prominent 1917 opinion authored by Justice Oliver Wendell Holmes.[175] This story-through-citations soon became a model for others. Subsequent state legislatures themselves referred to the draft federal rules when codifying the privilege.[176] And when state case law offered no precedents, the Advisory Committee's note provided a convenient substitute.[177]

Yet the Advisory Committee's note is curious not only for the assurances it spawned 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—doubts that vanish from view in the Committee's note. It was true that just a few years earlier, three states—California,[178] Kansas,[179] and New Jersey[180]—and the Uniform Law Commission had codified a trade secret privilege.[181] But Kansas and New Jersey had cited no authorities whatsoever to support their legislation. And the California Law Revision 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."[182]

Indeed, the sole case citation in the California commission's comment was to a civil suit decided forty-one years earlier in which a court of that state had ordered the *disclosure* of a trade secret.[183] Given the novelty of the statutory

[175] *See* Proposed Fed. R. Evid. 508 advisory committee's note, 56 F.R.D. at 250-51 (citing E.I. Du Pont de Nemours Powder Co. v. Masland, 244 U.S. 100 (1917)).

[176] *See, e.g.*, ALA. R. EVID. 507 advisory committee's note ("[T]he drafters of the proposed, but never enacted, Federal Rule of Evidence 508 furnished a comprehensive summary of case law examples . . . ."); LA. CODE EVID. ANN. art. 513 cmt. b (2017) ("This Article is identical to Federal Rule of Evidence 508 . . . ."). Alaska, Hawaii, Nebraska, Nevada, New Mexico, Texas, and Wisconsin adopted near-verbatim versions of the proposed federal Rule 508. *See* ALASKA R. EVID. 508; HAW. R. EVID. 508; NEB. REV. STAT. § 27-508 (2017); NEV. REV. STAT. § 49.325 (2017); N.M. R. EVID. 11-508; TEX. R. EVID. 507; WIS. STAT. § 905.08 (2017); *see also* 26 WRIGHT & GRAHAM, *supra* note 40, § 5641, at 285 n.16.

[177] For instance, Alabama's rules advisory committee admitted that "no trade secret privilege, assertable at trial, has been recognized under preexisting Alabama law" but cited the Wigmore treatise as evidence that the privilege "finds historic recognition nationally." *See* ALA. R. EVID. 507 advisory committee's note.

[178] *See* Act of May 18, 1966, ch. 299, 1965 Cal. Stat. 1297, 1335 (codified at CAL. EVID. CODE § 1060 (West 2018)).

[179] *See* Act of Feb. 27, 1963, ch. 303, 1963 Kan. Sess. Laws 601, 680 (codified at KAN. STAT. ANN. § 60-432 (2017)).

[180] *See* Act of June 20, 1960, ch. 52, 1960 N.J. Laws 452, 459 (codified at N.J. STAT. ANN. § 2A:84A-26 (West 2018)).

[181] UNIF. R. EVID. 32 (1953) (current version at UNIF. R. EVID. 507).

[182] *See* CAL. EVID. CODE § 1060 law revision commission's comments.

[183] *See id.* (citing Willson v. Superior Court, 225 P. 881 (Cal. Dist. Ct. App. 1924)).

enterprise, it is small surprise that the commission laced its commentary with caveats and offloaded the specifics to the courts. The text of California's provision expressly prohibits claims to the privilege that would "tend to conceal fraud or otherwise work injustice."[184] And the commission's comment suggested that information that could adequately be protected by copyright and patent laws should not qualify for the trade secret privilege 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."[185] But in general, limits on the scope of the privilege were "necessarily uncertain," and it was up to judges to work out the kinks.[186]

Even the comment to the Uniform Rules of Evidence had hedged that "[t]he limits of the privilege are uncertain."[187] 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 Justice 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.[188] After the Court determined that the trade secret status of the information was irrelevant to the case, it held that the defendant could be enjoined from sharing the information with expert witnesses for purposes of assessing that same irrelevant trade secret status.[189] In short, the rule in Holmes's opinion was not so much a privilege as a protective order.[190]

[184] *See id.* § 1060.

[185] *See id.* § 1060 law revision commission's comments.

[186] *See id.* As some measure of the privilege's reception by the courts, no such occasion would arise for another quarter-century. The eleven cases that raised the issue over those twenty-five years (identified using Westlaw's Citing References tool) all concerned issues of public disclosure or disclosure to government regulators, not disclosure to a party subject to a protective order. *See, e.g.*, Agric. Labor Relations Bd. v. Richard A. Glass Co., 221 Cal. Rptr. 63, 70 (Ct. App. 1985); San Gabriel Tribune v. Superior Court, 192 Cal. Rptr. 415, 416 (Ct. App. 1983); Cal. Sch. Emps. Ass'n v. Sunnyvale Elementary Sch. Dist., 111 Cal. Rptr. 433, 445 (Ct. App. 1973); Uribe v. Howie, 96 Cal. Rptr. 493, 494, 501-04 (Ct. App. 1971). Not until 1992 in *Bridgestone/Firestone, Inc. v. Superior Court*—a civil case—did a California appeals court first elaborate standards to govern the trade secret privilege as applied to disclosure to a party. *See* 9 Cal. Rptr. 2d 709, 713 (Ct. App. 1992). The *Bridgestone* standards ultimately became a frequently cited test nationwide for evaluating claims to a trade secret privilege. *See, e.g.*, Bridgestone Ams. Holding v. Mayberry, 878 N.E.2d 189, 193 (Ind. 2007); Laffitte v. Bridgestone Corp., 674 S.E.2d 154, 163 (S.C. 2009); *In re* Cont'l Gen. Tire, Inc., 979 S.W.2d 609, 611 (Tex. 1998).

[187] *See* UNIF. R. EVID. 32 cmt. (1953).

[188] *See* E.I. Du Pont de Nemours Powder Co. v. Masland, 244 U.S. 100, 103 (1917).

[189] *See id.* at 102-03.

[190] Those facts have not stopped numerous commentators from citing the Holmes opinion as an early exemplar of the trade secret privilege. *See, e.g.*, Memorandum from Ken Broun, Consultant, to Advisory Comm. on Evidence Rules (Apr. 12, 2013), *in* ADVISORY

footnote continued on next page

Moreover, the Advisory Committee's note contains another conspicuous omission: Its case law citations reach to 1889, but its rulemaking references stop short with the Uniform Rules of Evidence of 1953.[191] That fact is striking because it is exceedingly unlikely that the Committee could have thought that the Uniform Rules were the first to codify the privilege. The Uniform Rules themselves were based on the Model Code of Evidence, created by the American Law Institute (ALI) a decade earlier,[192] and they expressly credited the Model Code version of the trade secret privilege as the basis for its Uniform Rule counterpart.[193] Yet the Model Code appears nowhere in the Advisory Committee's citation-based history of the privilege. To understand the significance of this puzzling exclusion, it will be helpful to jump backward in time to a period well before the inception of the Model Code, when no consensus about a trade secret privilege existed.

1. Debates over the existence of the privilege

Whether or not to excuse a witness from testifying about sensitive financial information was a visible issue to nineteenth century courts. But commentators, instead of framing compelled disclosure as a threat to business and innovation as commentators tend to do today, viewed compelled disclosure as an issue of self-incrimination; the articulated concern at the time was that compelling witnesses to testify against their "pecuniary interest" might subject them to civil liability and thus run afoul of constitutional restrictions against compelling witnesses to testify against themselves.[194]

At least in England, the issue was settled for some time on the side of disclosure by an influential 1806 holding that "the witness was bound to answer a question, although his answer might render him liable to a civil

COMMITTEE ON EVIDENCE RULES: MAY 2013 229, 239 (2013), https://perma.cc/P2L8-BPGQ ("The Advisory Committee Note [to the proposed federal evidentiary privilege for trade secrets] traces the qualified privilege back at least to [*Masland*] . . . .").

[191] *See* Proposed Fed. R. Evid. 508 advisory committee's note, 56 F.R.D. 183, 250-51 (1972) (citing Dobson v. Graham, 49 F. 17 (C.C.E.D. Pa. 1889)).

[192] *See* MODEL CODE OF EVIDENCE r. 226 (AM. LAW INST. 1942). The Uniform Rules sought to address concerns that the Model Code was too radical for most states to adopt and to temper those elements to achieve greater "acceptability and uniformity." *See* UNIF. R. EVID. prefatory note at 161.

[193] *See* UNIF. R. EVID. 32 cmt. ("This rule follows American Law Institute Model Code of Evidence Rule 226.").

[194] *See, e.g.*, Bull v. Loveland, 27 Mass. (10 Pick.) 9, 12-14 (Oct. Term 1830) (describing English and U.S. cases grappling with the issue while noting—and rejecting—the concern with constitutional protection against being compelled to "furnish evidence against [oneself]" (quoting MASS. CONST. pt. 1, art. XII)). *Bull* overruled the earlier Massachusetts case *Appleton v. Boyd*, 7 Mass. (7 Tyng) 131 (1810).

action."[195] Parliament immediately codified the rule, declaring in the Witnesses Act 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."[196] Courts in the United States took note of both the English holding and the Act.[197] Maryland and Pennsylvania courts each adopted a parallel rule.[198] In 1830, the Supreme Judicial Court of Massachusetts 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."[199] Competing financial interests did not excuse testimony.[200]

Shortly thereafter, substantive trade secret law began to take modern form; mid-nineteenth century courts initially recognized a damages remedy for trade secret misappropriation and later afforded injunctive relief.[201] By the early twentieth century, courts and commentators in the United States had split on whether trade secrets warranted an evidentiary privilege. Two leading treatises—William Mack's *Cyclopedia of Law and Procedure* and Wigmore's *A Treatise on the System of Evidence in Trials at Common Law*—acknowledged some form of the privilege, but its scope was ambiguous.[202] Both expressed concern over the risk that business competitors might exploit a witness's duty to testify

[195] *See Bull*, 27 Mass. (10 Pick.) at 13 (describing the 1806 impeachment trial of Lord Melville in the House of Lords).

[196] 46 Geo. 3 c. 37 (Gr. Brit.).

[197] *See, e.g.*, *Bull*, 27 Mass. (10 Pick.) at 13.

[198] *See* Taney v. Kemp, 4 H. & J. 348, 350 (Md. 1818) (holding that a witness is bound to answer a question touching the issue in the case, even if doing so may expose him to civil action); Stoddert's Lessee v. Manning, 2 H. & G. 147, 158 (Md. 1828) (citing *Taney* for the rule that "no person shall be exempted from giving testimony on the ground that his answer may affect his interest"); Baird *ex rel.* M'Donnell v. Cochran, 4 Serg. & Rawle 397, 400 (Pa. 1818) (holding that neither any "act of assembly" nor "considerations drawn from general policy and the good of society" protect a witness from answering a question that "may affect his interest").

[199] *Bull*, 27 Mass. (10 Pick.) at 14; *see also* Devoll v. Brownell, 22 Mass. (5 Pick.) 448, 448 (1827) (per curiam).

[200] *See Bull*, 27 Mass. (10 Pick.) at 14.

[201] *See* Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 315 (2008) (noting that the Supreme Judicial Court of Massachusetts first recognized a damages remedy in *Vickery v. Welch*, 36 Mass. (19 Pick.) 523, 527 (1837), and that injunctive relief came later).

[202] *See* 40 WILLIAM MACK, CYCLOPEDIA OF LAW AND PROCEDURE 2532 (1912); 4 JOHN HENRY WIGMORE, A TREATISE ON THE SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW § 2212 (1905).

regarding trade secrets.[203] But both also cautioned against the excess protection of trade secret evidence. Mack urged courts to compel disclosure if "the interests of justice . . . imperatively demand it," observing that there is "no absolute right to refuse to answer pertinent questions."[204] Graham has characterized Wigmore's approach to the privilege as a "reluctant embrace."[205] In fact, Wigmore's early writings were arguably hostile to the privilege. The first edition of his treatise, published in the first decade of the twentieth century when Wigmore was in his early forties, recognized a limited form of privilege for trade secret evidence, which he called an "occasional necessity."[206] But the text also advocated that courts adopt a presumption against the validity of any claimed trade secrets; 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; 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."[207] This first edition of Wigmore's treatise seems even to question the underlying value of substantive trade secret law, commenting: "[I]n an epoch when patent-rights and copyrights 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."[208]

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 witnesses could not refuse to testify simply because doing so might cause them a "pecuniary loss."[209] Some courts recognized a limited right to refuse to disclose documents in open court if the evidence was "irrelevant or otherwise inadmissible" in the case.[210] A key

[203] *See* 40 MACK, *supra* note 202, at 2532 ("[I]t is not the policy of the law that valuable secrets shall be extorted from a witness under the cover of legal proceedings . . . ."); 4 WIGMORE, *supra* note 202, § 2212, at 3001 ("[T]he duty of a witness [should] be not allowed to become by indirection the means of ruining an honest and profitable enterprise.").

[204] *See* 40 MACK, *supra* note 202, at 2532.

[205] *See* 26 WRIGHT & GRAHAM, *supra* note 40, § 5642, at 323 n.258.

[206] *See* 4 WIGMORE, *supra* note 202, § 2212, at 3001. Wigmore was born in 1863. *John Henry Wigmore: American Legal Scholar*, ENCYCLOPÆDIA BRITANNICA, https://perma.cc/3DLD-LEWT (archived Apr. 9, 2018).

[207] *See* 4 WIGMORE, *supra* note 202, § 2212, at 3002.

[208] *Id.* at 3001-02.

[209] *See* Note and Comment, *The Privilege of a Witness to Refuse to Disclose Trade Secrets*, 3 MICH. L. REV. 565, 567 (1905).

[210] *See* Crocker-Wheeler Co. v. Bullock, 134 F. 241, 245 (C.C.S.D. Ohio 1904).

issue here was the burden placed on the party seeking disclosure. Judge Learned Hand articulated this issue particularly clearly. Writing in 1920, he refused to require parties seeking relevant trade secret information to meet a high burden, 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 in such a case."[211] Later decisions from the Southern District of New York followed Judge Hand's lead,[212] as did decisions from other federal district courts.[213] One court found that "it would be unusual" to exclude trade secret information from discovery at trial unless "the information was utterly remote and was not sought in good faith," reasoning that "if [a claimant] ha[s] chosen secrecy rather than the protection of the patent law, it must give way before the rights of third parties."[214] The Supreme Judicial Court of Massachusetts stayed its course from nearly a century before, explaining in 1921 that "fair and full cross-examination . . . is a matter of absolute right" and that allowing a witness to refuse to disclose trade secrets that are relevant to a case "is essentially unsound."[215]

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 nonparty's trade secrets "to the disadvantage and injury of such third persons, the inquiry should not be allowed."[216] The court cited a concern that trade secrets not be disclosed unless absolutely necessary.[217] But the opinion did not expressly consider either the relevance of the information sought or the precise burden that would be required to compel its disclosure. When the Court of Appeals of New York reached the issue in the midst of the Great Depression in 1933, it adopted a more robust formulation of the privilege—one more analogous to its formulation today. The court held that a party seeking trade secret information must meet a higher burden to show relevance than ordinarily required in civil procedure; the party must show that the information "appears to be indispensable for ascertainment of the truth" and "cannot otherwise be obtained."[218]

[211] *See* Grasselli Chem. Co. v. Nat'l Aniline & Chem. Co., 282 F. 379, 381 (S.D.N.Y. 1920).

[212] *See, e.g.*, Claude Neon Lights, Inc. v. Rainbow Light, Inc., 31 F.2d 988, 988-89 (S.D.N.Y. 1927).

[213] *See, e.g.*, U.S. Gypsum Co. v. Pac. Portland Cement Co., 22 F.2d 180, 181 (S.D. Cal. 1927) (ordering pretrial disclosure of an alleged trade secret that was "material and relevant" without imposing any heightened burden of showing its necessity to the case).

[214] *See Claude Neon Lights*, 31 F.2d at 988-89.

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

[216] Huessener v. Fishel & Marks Co., 127 A. 139, 141 (Pa. 1924).

[217] *See id.*

[218] *See* Drake v. Herrman, 185 N.E. 685, 686 (N.Y. 1933).

2. The Wigmore-Hand duel

As courts diverged over the trade secret privilege, Wigmore emerged as its primary advocate. Around this time, the ALI began efforts to unify evidence law across the nation; they were to create a Model Code of Evidence.[219] Wigmore, now in his late seventies, served as chief consultant for this mission.[220] Wigmore has a reputation for disliking evidentiary privileges, believing they hinder the quest for truth.[221] Yet somehow, over the prior quarter-century, he had become an ardent supporter of the trade secret privilege in particular. Colleagues at the ALI wrote that he "strenuously insist[ed]" on including the privilege in the Model Code.[222] When 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"[223]—Wigmore responded with a rebuke: "There are hundreds of trade-secrets which if patented would allow piracy without [the] possibility of tracing," he contended.[224] And then he added a short line that may lend insight into his change of heart: "[M]y brother had one such."[225]

Meanwhile, Judge Hand staked out a position against the privilege, in direct conflict with Wigmore. Judge Hand, a decade younger than Wigmore, served first as a member of the ALI Executive Committee and later as the organization's vice president.[226] Judge Hand had maintained his opposition to

[219] *See* Eleanor Swift, *One Hundred Years of Evidence Law Reform: Thayer's Triumph*, 88 CALIF. L. REV. 2437, 2457-61 (2000).

[220] *See id.* at 2457.

[221] *See* IMWINKELRIED, *supra* note 40, § 3.2.2, at 154; 23 WRIGHT & GRAHAM, *supra* note 40, § 5422, at 677 & n.61 (1980).

[222] *See* CODE OF RULES OF EVIDENCE r. 222 cmt. at 85 (AM. LAW INST., Council Draft No. 3, 1941).

[223] *See* Am. Law Inst., Comment on Rule 48 (n.d.) (on file with author).

The primary source materials cited in this Article are drawn from the comments regarding the Model Code of Evidence available through HeinOnline. *See Model Code of Evidence, 1939-1945*, HEINONLINE, https://perma.cc/LJ2T-54S2 (archived Apr. 30, 2018).

[224] *See* J.H. Wigmore, Comments on Draft Code of Rules of Evidence Rules 21-39, at 1 (1939) (on file with author). Note that the ALI's comment that "[t]he extent to which such a privilege should exist is doubtful" applied to what was then numbered rule 48. *See* Am. Law Inst., *supra* note 223, at 48. By the time of Wigmore's reply, the trade secret privilege was then part of rule 23, and it appears that Wigmore misquoted the ALI's original comment. *See* Wigmore, *supra*, at 1 (quoting the ALI's comment as saying "it is doubtful whether such a privilege should exist"). In searching the Model Code archives, the closest matching comment I found is the ALI's as cited in note 223 above, so I assume that this is the comment to which Wigmore was referring.

[225] Wigmore, *supra* note 224.

[226] *See* Herbert F. Goodrich, *Judge Learned Hand and the Work of the American Law Institute*, 60 HARV. L. REV. 345, 345-46 (1947); *Learned Hand: United States Jurist*, ENCYCLOPÆDIA BRITANNICA, https://perma.cc/QPS5-PHHF (archived Apr. 9, 2018).

the privilege and tried to purge the Model Code of any reference to it.[227] His position was that "[w]herever [trade secrets] are material to any issue in the case[,] disclosure of them must be made."[228] For Judge Hand, the privilege simply did not exist.[229] Wigmore shot back, stating that "Judge Hand's belief that 'there is no privilege for trade secrets' is difficult to understand" and claiming that "[e]xcept for names of customers, no case repudiating the privilege" had ever been found.[230] Of course, Judge Hand's own prior opinions included such a case.[231] Neither Judge Hand's ruling on the issue nor the cases it inspired ever made it into Wigmore's comments to the ALI or, for that matter, into any edition of his famed treatise.

The ALI split. Professor Edmund Morgan of Harvard Law School supported Judge Hand, others Wigmore.[232] The disagreement continued for years until, on the eve of Pearl Harbor in 1941, Wigmore tried a new strategy: Spotlight military manufacturers that relied on trade secrets, like aircraft and chemical factories.[233] Wigmore even made it personal, directing his comments to Morgan and implying that he specifically had forgotten the needs of these vital industries.[234] 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 secret privilege.[235] Eleven months later, Wigmore died.[236]

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 enacted) federal trade

[227] *See* CODE OF EVIDENCE r. 222 cmt. at 99 (AM. LAW INST., Tentative Draft No. 1, 1940).

[228] CODE OF RULES OF EVIDENCE r. 222 cmt. at 85 (AM. LAW INST., Council Draft No. 3, 1941).

[229] *See id.*

[230] *See* J.H. Wigmore, Comments on Code of Rules of Evidence, Preliminary (Tpw.) Draft No. 14, r. 222 cmt. (1941) (on file with author).

[231] *See* Grasselli Chem. Co. v. Nat'l Aniline & Chem. Co., 282 F. 379, 381 (S.D.N.Y. 1920).

[232] *See* CODE OF RULES OF EVIDENCE r. 222 cmt. at 85 (AM. LAW INST., Council Draft No. 3, 1941) (noting that Morgan, the Reporter, supported Judge Hand's position). The fact that Wigmore ultimately prevailed, *see infra* note 235 and accompanying text, supports the inference that others on the committee endorsed Wigmore's view.

[233] *See* Wigmore, *supra* note 230, r. 222 cmt. ("Has the fact been kept in mind by the Reporter that many important industries operate on trade secrets deemed so vital that the various parts of the process are strictly committed to different operators,—e.g. some aircraft factories, some Dupont processes, and some Solway chemical processes?").

[234] *See id.*

[235] MODEL CODE OF EVIDENCE r. 226 (AM. LAW INST. 1942) ("The owner of a trade secret has a privilege . . . to refuse to disclose the secret and to prevent other persons from disclosing it if the judge finds that the allowance of the privilege will not tend to conceal fraud or otherwise work injustice.").

[236] Editorial, *John Henry Wigmore*, 34 J. CRIM. L. & CRIMINOLOGY 3, 3 (1943).

secret privilege: proposed rule 508 of the Federal Rules of Evidence.[237] Among other issues, Imwinkelried documents concerns that industry lobbyists had hijacked the rulemaking process to advocate for new and expanded privileges that served their interests.[238] There is no reason to repeat that narrative here, and it would be difficult indeed to improve on their accounts.[239] Suffice it to say that the series of state and federal legislative debates about the trade secret privilege that followed the passage of the Model Code, including debates surrounding the Uniform Rules of Evidence, proposed federal rule 508, Texas Rule of Evidence 507, and California's evidence code, contain no references to the heated clash between Wigmore and Judge Hand. Wigmore's treatise was cited repeatedly. Judge Hand's ruling in opposition was rarely if ever mentioned.[240] And beginning with the federal Advisory Committee's 1970 note, the Model Code itself dropped from the historical narrative.[241]

[237] *See* 26 WRIGHT & GRAHAM, *supra* note 40, § 5642, at 320-24; Imwinkelried, *supra* note 174, at 44-59.

[238] *See* Imwinkelried, *supra* note 174, at 46; *see also Proposed Rules of Evidence: Hearings Before the Spec. Subcomm. on Reform of Fed. Criminal Laws of the H. Comm. on the Judiciary*, 93d Cong. 168, 175 (1973) [hereinafter *Rules of Evidence Hearings*] (statement of Charles R. Halpern & George T. Frampton, Jr., Washington Council of Lawyers) ("The Rules of privilege also favor, or appear to favor, special interests.").

[239] Graham actually lived the history, sending letters to Congress arguing that recognizing a trade secret privilege—even in civil cases—would impose an unreasonable burden on parties seeking to compel disclosure of trade secret evidence. *See Rules of Evidence Hearings*, *supra* note 238, at 175 (quoting Graham's July 28, 1971 letter to the Standing Committee). For Graham's letter, see *id.* at 195 (statement of Kenneth W. Graham, Jr., Professor of Law).

[240] *See, e.g.*, Willson v. Superior Court, 225 P. 881, 882 (Cal. Dist. Ct. App. 1924) (citing Wigmore but not Judge Hand in discussing the "general trend of authority" as to the existence of a civil trade secret privilege); Putney v. Du Bois Co., 226 S.W.2d 737, 741-42 (Mo. Ct. App. 1950) (citing Wigmore but not Judge Hand in discussing the existence and proper application of a civil trade secret privilege); Spain v. U.S. Rubber Co., 54 A.2d 364, 365 (N.H. 1947) (citing Wigmore but not Judge Hand in discussing the existence and limits of a civil trade secret privilege); *Proposed Rules of Evidence: Hearings Before the Spec. Subcomm. on Reform of Fed. Criminal Laws of the H. Comm. on the Judiciary*, 93d Cong. 318, 325 (Supp. 1973) (statement of Charles Doyle, American Law Division) (citing Wigmore but not Judge Hand in reporting that contemporaneous federal case law's treatment of the trade secret privilege differed from Wigmore's treatment); UNIF. R. EVID. 32 cmt. (citing Wigmore and civil precedents but not Judge Hand); CAL. LAW REVISION COMM'N, TENTATIVE RECOMMENDATION AND A STUDY RELATING TO THE UNIFORM RULES OF EVIDENCE: ARTICLE V; PRIVILEGES 461-62 (1964) (citing Wigmore and a series of civil precedents but not Judge Hand); *see also* 1 STEVEN GOODE & OLIN GUY WELLBORN III, GUIDE TO THE TEXAS RULES OF EVIDENCE § 507.1 (4th ed. 2016) (citing Wigmore but not Judge Hand to support the existence of a qualified trade secret privilege); 3 LEO H. WHINERY, OKLAHOMA EVIDENCE: COMMENTARY ON THE LAW OF EVIDENCE § 42.03 (2d ed. 2000) (citing Wigmore but not Judge Hand).

[241] *See supra* notes 191-93 and accompanying text.

Perhaps the Advisory 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 secret privilege exude greater and greater confidence in its past. The Committee's note was a pivot in a broader process.[242] The note's own declaration that the privilege had "found ample recognition"[243] helped to produce what it purported to describe.

B. The Criminal Trade Secret Privilege

Prior to the 1990s, case law and legislative histories both evince a dearth of supporting authority for the application of a trade secret privilege in criminal proceedings.

Early historical sources suggest that the privilege was unavailable in criminal proceedings. The first edition of Wigmore's treatise did cite two criminal cases amid a slew of civil disputes, but the secrets in each of those cases had been ordered *disclosed*.[244] In the 1775 trial of Maha Rajah Nundocomar, the East India Company refused to produce records during a public trial because they contained secrets.[245] The court found that company papers containing material evidence must be produced because "[h]umanity requires it should be produced, when in favour of a criminal, justice when against him."[246] In the

[242] Substantive trade secret law also evolved over the twentieth century. From as early as 1917 until at least 1939, trade secrecy was viewed as a tort-like doctrine. *See* Lemley, *supra* note 201, at 316. By about 1980, an alternative property-like view of trade secrecy "was on the ascendancy." *See id.* This evolution does not appear to explain the Model Code debates over the evidentiary privilege, which occurred before the property-like theory of trade secrecy gained prominence. However, treatments of the privilege later in the twentieth century could reflect changes to the substantive law. *Compare* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW INST. 1939) (defining a trade secret as "information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it" and as "a process or device for continuous use in the operation of the business"), *with* UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985) (defining a trade secret as information that "(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy").

[243] Proposed Fed. R. Evid. 508 advisory committee's note, 56 F.R.D. 183, 250 (1972).

[244] *See* 4 WIGMORE, *supra* note 202, § 2212, at 3003 n.1 (1905) (citing The King v. Nundocomar (1775) 20 How. St. Tr. 923; and R v. Webb (1834) 174 Eng. Rep. 140, 1 M. & Rob. 405).

[245] *See Nundocomar*, 20 How. St. Tr. at 1057. It is ambiguous from the trial report whether the secrecy claimed was more akin to what we today call trade secrets or to what we call state secrets.

[246] *Id.*

1834 case *Rex v. Webb*, the defendant was a quack doctor who had allegedly poisoned the deceased by administering excessive amounts of a purportedly medicinal pill.[247] When the prosecution sought at trial 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."[248] The judge ordered him to answer anyway, with neither protective order nor sealing action, and merely "suggested" that the prosecutor limit his questions to those that "the ends of justice required."[249]

Although some states began to codify the trade secret privilege in the second half of the twentieth century, I have found no criminal cases directly invoking the privilege until the twenty-first century. For instance, New Jersey and Kansas became the first states to codify the privilege in 1960 and 1963, respectively,[250] and neither state's statute has ever been invoked in a criminal case.[251] Texas's trade secret privilege was not cited in a criminal case until 2016, where it was deemed irrelevant to the ruling.[252] And the trade secret privilege incorporated into Florida's Rules of Evidence in 1972[253] was not invoked in a criminal case until 2005.[254] At a national level, neither the ALI's comments in

[247] 174 Eng. Rep. at 141, 1 M. & Rob. at 405-06.

[248] *Id.* at 142, 1 M. & Rob. at 412.

[249] *See id.*

[250] *See* Act of Feb. 27, 1963, ch. 303, 1963 Kan. Sess. Laws 601, 680 (codified at KAN. STAT. ANN. § 60-432 (2017)); Act of June 20, 1960, ch. 52, 1960 N.J. Laws 452, 459 (codified at N.J. STAT. ANN. § 2A:84A-26 (West 2018)); *see also* Proposed Fed. R. Evid. 508 advisory committee's note, 56 F.R.D. 183, 251 (1972) (recognizing three states that as of 1972 had enacted a trade secret privilege: New Jersey, Kansas, and California).

[251] According to Westlaw's Citing References tool, as of February 26, 2018 neither New Jersey's nor Kansas's statutory trade secret privilege had ever been cited in a criminal case. Note that I ran Citing References searches only on the modern codified sections, not on any statutory predecessors.

[252] *See* Wright v. State, No. 02-15-00399-CR, 2016 WL 6520189, at *5 (Tex. Ct. App. Nov. 3, 2016) (noting briefly that a third party did not invoke the trade secret privilege against disclosure and rejecting the defendant's argument that in camera review should have been held to determine whether the documents were privileged trade secrets); *see also* TEX. R. EVID. 507.

[253] *See* Act of June 23, 1976, ch. 76-237, 1976 Fla. Laws 556, 566 (codified at FLA. STAT. § 90.506 (2017)).

[254] *See* State v. Bjorkland, No. 2004 CT 014406 SC, 2005 WL 4062673, at *1 (Fla. Cir. Ct. Nov. 2, 2005) (holding that even where a defense expert agreed that source code for a breath test device "constitutes a trade secret," the prosecution must produce the code because it would be "contrary to the purpose" of the privilege to prevent defendants "from obtaining information relevant to the instrument that is used to prove their guilt"). Two criminal cases in Florida cited section 90.506 in the 1980s, but the privilege was not invoked in either. *See* Hope v. State, 449 So. 2d 1319, 1320 (Fla. Dist. Ct. App. 1984) (including section 90.506 in a list of statutes in order to demonstrate that another privilege—a father-son privilege—did not exist under state law); Moreno v. State, 418

footnote continued on next page

drafting the Model Code[255] nor the Uniform Rules of Evidence and accompanying comments expressly mention criminal proceedings.[256] Even Kenneth Graham Jr.'s letter to Congress in 1971 advocating against the adoption of the privilege omits any consideration of the privilege in criminal as compared to civil proceedings.[257]

The first hint of change occurred in 1990, when California modified its evidence statute to expressly apply its trade secret privilege in criminal cases.[258] No appeals court in the state would address such a claim in a criminal proceeding until *Chubbs* in 2015.[259] In fact, the historical record suggests that before *Chubbs*, legislators and commentators may not even have conceived of applying the privilege to block criminal defendants' own access to evidence. Rather, at the time the criminal privilege was adopted, the concern was keeping trade secrets from *public* disclosure by sealing court records, granting protective orders, or permitting closure of court proceedings. The individual who initially drafted California's 1990 amendment, Kenneth Rosenblatt of the Office of the District Attorney for Santa Clara County, described it as an unprecedented statutory "procedure for protecting trade secrets in criminal

So. 2d 1223, 1225 n.2 (Fla. Dist. Ct. App. 1982) (listing section 90.506 as an example of a type of privilege).

[255] *See supra* note 223 (explaining the archival source of documents from the ALI surrounding the creation of the Model Code).

[256] *Compare* UNIF. R. EVID. 2 & cmt. (establishing that the rules apply to both criminal and civil proceedings), *with id.* 32 & cmt. (making no reference to criminal proceedings). The two cases cited in the comment on the trade secret privilege, *see id.* 32 cmt., are both civil. *See* Putney v. Du Bois Co., 226 S.W.2d 737, 737 (Mo. Ct. App. 1950); Spain v. U.S. Rubber Co., 54 A.2d 364, 365 (N.H. 1947).

[257] *See Rules of Evidence Hearings*, *supra* note 238, at 195-99 (statement of Kenneth W. Graham, Jr., Professor of Law); *cf.* 26 WRIGHT & GRAHAM, *supra* note 40, § 5642, at 328 & nn.295-97 (discussing the "proper role" for the trade secret privilege as it relates to restrictions on discovery under Rule 26 of the Federal Rules of Civil Procedure but notably omitting any reference to criminal procedure).

[258] *See* Act of June 18, 1990, ch. 149, 1990 Cal. Stat. 1215 (codified as amended at CAL. EVID. CODE §§ 1061-1062 (West 2018)). The 1990 act established two entitlements granted by the trade secret privilege in criminal proceedings: protective orders, *see id.* § 1, 1990 Cal. Stat. at 1215-16 (codified as amended at CAL. EVID. CODE § 1061), and closures of court proceedings, *see id.* § 2, 1990 Cal. Stat. at 1216-18 (codified as amended at CAL. EVID. CODE § 1062). Soon thereafter, the California legislature also added sealing procedures. *See* Act of Sept. 10, 1990, ch. 714, § 3, 1990 Cal. Stat. 3316, 3319-20 (codified as amended at CAL. EVID. CODE § 1063).

[259] *See* People v. Superior Court (*Chubbs*), No. B258569, 2015 WL 139069, at *5-6 (Cal. Ct. App. Jan. 9, 2015). During the 1990s, California courts had but two occasions to consider the relationship between the statute's civil and criminal sections, and in both cases the court applied standards from the criminal sections to civil disputes, not the other way around. *See* Stadish v. Superior Court, 84 Cal. Rptr. 2d 350, 358 (Ct. App. 1999); State Farm Fire & Cas. Co. v. Superior Court, 62 Cal. Rptr. 2d 834, 851 (Ct. App. 1997).

cases."[260] In 1991, Rosenblatt published an article describing the issue of "how to protect confidential information from disclosure during a criminal prosecution without violating a defendant's Sixth Amendment right to a fair trial and the public's First Amendment right to view criminal justice proceedings."[261] While he noted early on that "the accused enjoys a panoply of constitutional rights,"[262] the article focused predominantly on defendants' public trial rights and the public's access rights.[263] Rosenblatt made no mention of the newly minted privilege as a limit on discovery or subpoena power.

There is a smattering of criminal cases considering trade secret disclosures during the 1970s and 1980s, but they primarily concern issues of sealing and excluding the public from trials. In 1970, the Second Circuit held that a trial court had erred in denying the defense a copy of a computer program that the government's witness had relied on to generate "figures" used during testimony.[264] Four years later the Second Circuit ordered a third party's trade secret to be disclosed in a criminal contempt proceeding but suggested that the district court close the proceeding to the public, limit attendees, or put attendees under an oath of confidentiality with regard to the trade secret.[265] The district court in that case had also ordered disclosure but refused even to close the courtroom, citing Sixth Amendment concerns.[266]

[260] *See* Kenneth Rosenblatt, *Criminal Law and the Information Age: Protecting Trade Secrets from Disclosure in Criminal Cases*, COMPUTER LAW., Jan. 1991, at 15, 15 n.*, 16.

[261] *Id.* at 15.

[262] *Id.*

[263] *See id.* at 16-17 (discussing the statutory procedures established by sections 1061, 1062, and 1063 of the California Evidence Code and specifically analyzing defendants' and the public's rights to object to protective orders, court closures, or sealing of documents).

[264] *See* United States v. Dioguardi, 428 F.2d 1033, 1037-38 (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.").

[265] *See* Stamicarbon, N.V. v. Am. Cyanamid Co., 506 F.2d 532, 534-35, 539-41 (2d Cir. 1974) (ordering disclosure of a third party's trade secrets and suggesting that if the owner "was likely to suffer irreparable injury, and [if] protection of its secrets could be achieved with minimal disruption of the criminal proceedings," the district court should close the proceedings to the public, "selectively exclude" the owner's competitors, or place attendees under an oath of confidentiality). I have found one district court decision from 1964 denying a criminal defendant discovery of a third party's trade secrets that had been seized by the government. *See* United States v. Aluminum Co. of Am., 232 F. Supp. 664, 665-66 (E.D. Pa. 1964) (discussing the trade secret privilege and a heightened burden of showing necessity in order to obtain discovery but ultimately denying discovery for failure to show relevance).

[266] *See Stamicarbon*, 506 F.2d at 536. The Second Circuit mentioned similar concerns about the public trial right. *See id.* at 542 ("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.").

Trade secret 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 data,[267] statistical standards,[268] and "primer sequences."[269] At least one conviction was reversed because a private laboratory had refused to disclose its statistical standards for determining a DNA "match."[270] A Vermont court selectively excluded DNA evidence tested with certain systems as a result of the manufacturers' nondisclosures and the absence of independent validation.[271] Early commentators called for the use of only public laboratories "so that the laboratories cannot hide behind 'trade secrets' to withhold information from defendants."[272] In 1992, the National Research Council's Committee on DNA Technology in Forensic Science 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."[273]

But most courts eventually found the DNA evidence admissible despite the trade secret methodologies used to analyze it.[274] By 2007, a general consensus

[267] *See, e.g.*, People v. Cavin, No. 00-4395-FY, 2000 WL 35721883, slip op. at 41 (Mich. Cir. Ct. Lake Cty. Oct. 18, 2000).

[268] *See, e.g.*, State v. Schwartz, 447 N.W.2d 422, 427 (Minn. 1989).

[269] *See, e.g.*, State v. Lynch, No. CR 98-11390, 1999 WL 34966936, slip op. at 4 (Ariz. Super. Ct. Maricopa Cty. Aug. 20, 1999).

[270] *See* People v. Davis, 601 N.Y.S.2d 174, 175 (App. Div. 1993) (per curiam); *see also* California v. Bokin, No. 168461, slip op. at 8 & n.6 (Cal. Super. Ct. City & Cty. S.F. May 6, 1999) (stating that the court "advised the government" that it could not rely on developmental validation reports where discovery of "proprietary information" had been withheld from the defense).

[271] *See* State v. Pfenning, No. 57-4-96, 2000 WL 35721887, slip op. at 49, 52-54, 68 (Vt. Super. Ct. Grand Isle Cty. Apr. 6, 2000) (finding the results of some DNA test systems inadmissible both because their proprietary primer sequences were undisclosed and because they lacked independent validation but admitting the results of other DNA test systems despite undisclosed primer sequences because of rigorous independent validation testing and peer review).

[272] *See, e.g.*, George J. Annas, *DNA Fingerprinting in the Twilight Zone*, HASTINGS CTR. REP., Mar./Apr. 1990, at 35, 37.

[273] NAT'L RESEARCH COUNCIL, DNA TECHNOLOGY IN FORENSIC SCIENCE 162 (1992); *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 tension between asserting that a scientific methodology is "sufficiently known and proven to be regarded as generally accepted by the scientific community" while at the same time arguing that the details of that methodology are "sufficiently unique and innovative to constitute trade secrets").

[274] *See, e.g.*, People v. Hill, 107 Cal. Rptr. 2d 110, 116, 118-19 (Ct. App. 2001) (holding the results of a DNA test system admissible even though the manufacturer "had not . . . publicly released" the validation data, claiming that the data were proprietary); State v. Bailey, 677 N.W.2d 380, 398-401 (Minn. 2004) (declining to exclude DNA evidence, and

footnote continued on next page

had formed; the American Bar Association (ABA) proposed its own trade secret privilege standard specifically for DNA evidence in criminal cases.[275] The ABA adopted the language of proposed federal rule 508 nearly verbatim,[276] quoting the Advisory Committee's 1970 note that the privilege had found "ample recognition, and indeed, a denial of it would be difficult to defend."[277]

A second wave of criminal cases challenging trade secret evidence began around the mid-2000s, when a series of defendants charged with driving under the influence tried to access the source code in breath test devices. They wanted to see for themselves how the devices worked, not take the manufacturers at their word or be limited to black-box validation studies in presenting a defense.[278] A few courts ordered the source code disclosed to defense experts,[279] leading to the discovery of some bugs but otherwise to the affirmation of the tools.[280] Others found that the code was not in the government's possession

remanding for a further admissibility hearing, even though the test system's proprietary primer sequences were undisclosed); State v. Traylor, 656 N.W.2d 885, 898-99 (Minn. 2003) (holding DNA evidence admissible despite an assertion that the methodology used to produce the evidence was a protected trade secret but also asserting that protective orders should be pursued when defendants seek to discover proprietary information). These cases concerned defense efforts under evidence law or due process standards to exclude expert evidence that was based on trade secret methodologies. They did not address defense efforts to subpoena trade secrets in order to cross-examine the admitted evidence and challenge its weight. *See, e.g.*, *Traylor*, 656 N.W.2d at 898-99. Perhaps for that reason, these opinions do not directly consider the trade secret evidentiary privilege.

[275] AM. BAR ASS'N, ABA STANDARDS FOR CRIMINAL JUSTICE: DNA EVIDENCE standard 16-5.2 & cmt., at 102-04 (3d ed. 2007).

[276] *Compare id.* standard 16-5.2, at 102, *with* Proposed Fed. R. Evid. 508, 56 F.R.D. 183, 249-50 (1972).

[277] AM. BAR ASS'N, *supra* note 275, standard 16-5.2 cmt., at 103 n.285 (quoting Proposed Fed. R. Evid. 508 advisory committee's note, 56 F.R.D. at 250).

[278] *See* Aurora J. Wilson, *Discovery of Breathalyzer Source Code in DUI Prosecutions*, 7 WASH. J.L. TECH. & ARTS 121, 124-25 (2011); *see also* Chessman, *supra* note 20, at 195-96.

[279] *See, e.g.*, Krugman v. CMI, Inc., 437 S.W.3d 167, 169 (Ky. Ct. App. 2014) (stating that the trial court had ordered trade secret source code disclosed but had "granted a protective order"); *In re* Source Code Evidentiary Hearings in Implied Consent Matters, 816 N.W.2d 525, 529 & n.5 (Minn. 2012); Underdahl v. Comm'r of Pub. Safety (*In re* Comm'r of Pub. Safety), 735 N.W.2d 706, 709-10, 712-13 (Minn. 2007); State v. Chun, 923 A.2d 226, 226-27 (N.J. 2007) (per curiam).

[280] *See In re Source Code Evidentiary Hearings*, 816 N.W.2d at 543 (holding as a result of a review of source code that when a certain breath test instrument reports a "deficient sample" while running a particular version of the software, the results are unreliable and inadmissible unless verified through other means, but otherwise finding no problems with the device (quoting the district court's opinion)); State v. Chun, 943 A.2d 114, 120, 171-73 (N.J. 2008) (holding that the results of a breath test were admissible but requiring the manufacturer to make modifications and correct errors discovered in the code).

and thus not the prosecutor's to hand over.[281] The rest held that defendants had not sufficiently shown that the source code was relevant or material.[282] Judges in the last group sometimes measured defense arguments against a higher burden than would have applied to evidence not protected by trade secret law, for example by requiring a strict showing of the necessity of the source code rather than mere relevance or materiality.[283] But none ruled explicitly that they were, or were not, "privileging" trade secret evidence.[284]

[281] *See, e.g.*, Moe v. State, 944 So. 2d 1096, 1097 (Fla. Dist. Ct. App. 2006); Smith v. State, 750 S.E.2d 758, 763 (Ga. Ct. App. 2013) (rejecting the argument that the state had "constructive possession" of the source code); State v. Kuhl, 741 N.W.2d 701, 708-10 (Neb. Ct. App. 2007) (holding that source code was not discoverable from the state because the state did not possess the code and "did not have a legal obligation to produce evidence not in its possession"), *aff'd*, 755 N.W.2d 389 (Neb. 2008).

[282] *See, e.g.*, State v. Bernini, 218 P.3d 1064, 1067-69 (Ariz. Ct. App. 2009) (finding that the defendants had failed to demonstrate "substantial need" for proprietary software); State v. Bastos, 985 So. 2d 37, 42-43 (Fla. Dist. Ct. App. 2008) (finding that breath test source code was not sufficiently "material" to compel an out-of-state manufacturer to produce it (quoting FLA. STAT. § 942.03)); Commonwealth v. House, 295 S.W.3d 825, 829 (Ky. 2009) (declaring a subpoena of source code to be "nothing but a classic fishing expedition"); State v. Underdahl, 767 N.W.2d 677, 685-86 (Minn. 2009) (holding that the defendant had failed to demonstrate that requested source code "may relate to his guilt or innocence"); People v. Cialino, 831 N.Y.S.2d 680, 680-82 (Crim. Ct. 2007) (faulting the defendant for failure to provide a reasonable basis for concluding that "any software changes and upgrades had caused the [software] used in this case to be unreliable").

[283] For instance, a 2008 opinion from a Florida appeals court denied discovery of trade secret source code absent a "particularized showing" of necessity, a higher threshold for materiality than the court required for discovery of nonproprietary documents related to testimony in the same case. *See Bastos*, 985 So. 2d at 40, 43. Similarly, a criminal court in New York City asserted that it was "incumbent on the defendant" to provide a "reasonable basis" for the court to believe that a software change had altered the reliability of the breath test machine in order to succeed in a discovery motion for the machine's source code. *See Cialino*, 831 N.Y.S.2d at 682. Yet in the same case, the court approved discovery requests for nonproprietary evidence, including "reports concerning the [state's] operation and maintenance of the machine," without imposing this "reasonable basis" test. *See id.* at 680-82. In contrast, other courts expressly refused to alter the burden for discovery. The Georgia Supreme Court, for example, vacated a denial of discovery because the lower court had erred in applying an overly stringent burden of materiality. *See* Davenport v. State, 711 S.E.2d 699, 700, 702-03 (Ga. 2011).

[284] Although dicta in some opinions mention trade secrets or proprietary interests, no court cited or even expressly discussed a trade secret evidentiary privilege, much less based its holding on one. *See, e.g.*, State v. Burnell, No. MV06479034S, 2007 WL 241230, at *2 (Conn. Super. Ct. Jan. 18, 2007) (mentioning trade secrets but not an evidentiary privilege); *Moe*, 944 So. 2d at 1097 (noting that the manufacturer had "invoked its statutory and common law privileges protecting the code from disclosure" to the state without identifying what process, if any, the state had used to seek access to the code, and basing its holding on other grounds); *In re Comm'r of Pub. Safety*, 735 N.W.2d at 710-13 (making no reference to an evidentiary trade secret privilege); *Kuhl*, 741 N.W.2d at 708-10 (mentioning trade secrets but no assertions of an evidentiary privilege and basing its holding on other grounds); *Chun*, 943 A.2d at 122-23 (making no reference to an evidentiary trade secret privilege); *Cialino*, 831 N.Y.S.2d at 680-82 (mentioning trade

footnote continued on next page

The *Chubbs* opinion changed all of this in 2015 by applying an explicit evidentiary privilege for trade secret evidence in a criminal case.[285] It was likely the first appeals court to do so in the nation's history.[286] The introduction of privileged trade secret evidence in criminal cases is thus a relatively recent development. Whether, and to what extent, the privilege should entitle trade secret holders to a total withholding remedy is an open legal question.

III. Law and Consequences of the Trade Secret Privilege

This Part describes the rules that currently govern the trade secret privilege and examines them in relation to criminal procedure, substantive trade secret law, and broader privilege law. I begin by arguing that the privilege is particularly injurious in criminal proceedings. A wholesale application of the current civil rules to criminal proceedings will almost certainly lead to systemic overclaiming and wrongful exclusion of relevant evidence; impose an unreasonable burden on defendants' discovery and subpoena rights; and undermine the legitimacy of criminal proceedings by implying that the government values intellectual property owners more than other groups affected by criminal proceedings. Further, these harms are entirely unjustified because the privilege is unnecessary in criminal cases. Narrow criminal discovery and subpoena powers already bar defendants from accessing irrelevant or immaterial trade secret information. And when trade secret evidence is relevant to a case, protective orders, sealing, and limited courtroom closures provide sufficient safeguards. This Part then contends that the privilege overprotects intellectual property and fails to serve the purposes of either trade secret law or of privilege law.

secrets but not a trade secret evidentiary privilege). Other cases made no mention of trade secrecy or proprietary interests at all. *See, e.g.*, State v. Walters, No. DBDMV050340997S, 2006 WL 785393, at *1 (Conn. Super. Ct. Feb. 15, 2006); *Bastos*, 985 So. 2d at 42-43.

[285] *See* People v. Superior Court (*Chubbs*), No. B258569, 2015 WL 139069, at *6, *9 (Cal. Ct. App. Jan. 9, 2015).

[286] *See supra* notes 250-54 and accompanying text. A search of criminal appellate cases linked to Westlaw's key number 311Hk402—which captures trade secrets and commercial information under the banner of privileged communications and confidentiality—yields no cases, though it also misses *Chubbs* because (as an unpublished decision) *Chubbs* was not assigned key numbers. A review of all cases in Westlaw's Citing References tool for the state trade secret statutes enacted by Florida, Kansas, New Jersey, and Texas, *see* FLA. STAT. § 90.506 (2017); KAN. STAT. ANN. § 60-432 (2017); N.J. STAT. ANN. § 2A:84A-26 (West 2018); TEX. R. EVID. 507, yields no criminal appellate cases that recognize a trade secret privilege before *Chubbs* did in 2015. Two pre-2015 criminal appellate cases in Florida cited the state trade secret privilege in passing. *See supra* note 254 (discussing those two cases).

A. The Trade Secret Privilege Is Harmful in Criminal Cases

Courts considering the privilege apply a three-step test. First, they consider whether the alleged trade secret is valid and whether ordering its disclosure would cause harm.[287] Next, they assess whether the information is relevant and necessary to the case.[288] Finally, they weigh the risk of harm from disclosure against the need for the information.[289]

1. Overclaiming

To invoke the privilege, one must first establish that a valid trade secret exists.[290] That is, the claimant must show that the purported trade secret satisfies a particular jurisdiction's definitional requirements, including that the claimant has taken sufficient safeguards to keep the information confidential.[291] In civil suits, this process can be difficult and risky; whether sensitive information qualifies as a trade secret is a frequent focus of litigation in civil misappropriation lawsuits.[292] And the showing may be especially difficult for privilege claimants because courts have not settled on precisely what definition of a trade secret applies to invocations of the privilege.[293] Then there is the risk that the opposing party will disprove the validity of a purported trade secret and eviscerate its value.[294] Combined, the difficulty and risk are likely to deter borderline and fraudulent claims to the privilege where there is no legitimate trade secret to protect.

[287] *See, e.g.*, *Chubbs*, 2015 WL 139069, at *5-6.

[288] *See, e.g.*, Bridgestone/Firestone, Inc. v. Superior Court, 9 Cal. Rptr. 2d 709, 713 (Ct. App. 1992).

[289] *See id.* at 713-14 (developing the standard for asserting a trade secret in civil cases); *see also Chubbs*, 2015 WL 139069, at *5-7 (adopting the *Bridgestone* standard in a criminal case).

[290] *See, e.g.*, Ferolito v. Ariz. Beverages USA, LLC, 990 N.Y.S.2d 218, 220 (App. Div. 2014) (finding that Morgan Stanley had met its burden of establishing that documents its counterparty had sought in discovery "contained one or more trade secrets").

[291] *See, e.g.*, *Protecting Trade Secrets During Discovery*, LAW. BRIEF, Feb. 13, 2009, at 1, 3.

[292] *See, e.g.*, William M. Corrigan, Jr. & Jeffrey L. Schultz, *Trade Secret Litigation—An Overview*, 63 J. MO. B. 234, 235-37 (2007) (collecting trade secret misappropriation cases that turned on whether the information at issue qualified as a trade secret).

[293] *See* 26 WRIGHT & GRAHAM, *supra* note 40, § 5644, at 331-32 (describing the criticism that establishing the validity of a trade secret in the context of a privilege claim is "open-ended and fact intensive" (quoting Peter C. Quittmeyer, *Trade Secrets and Confidential Information Under Georgia Law*, 19 GA. L. REV. 623, 635 (1985))).

[294] *Cf., e.g.*, Procter & Gamble Co. v. Nabisco Brands, Inc., 111 F.R.D. 326, 329-31 (D. Del. 1986) (holding that documents sought in discovery did not qualify for a protective order because they were not trade secrets).

Yet these constraints are missing in most criminal cases; it is easier and safer to assert the privilege in criminal cases because fewer defendants are equipped with the resources to challenge the validity of an alleged trade secret.[295] Potential privilege claimants can reasonably anticipate that their assertions of privilege will go unchallenged, so they will be more likely to overclaim protections where no trade secret exists.

At least one example of likely overclaiming already exists. New York City's Office of Chief Medical Examiner (OCME) 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. In one case, the OCME asserted that the code "is a copyrighted and proprietary asset belonging exclusively to the City of New York."[296] In another, it withheld the code in order to preserve the City's "ownership interest."[297] New York state courts ruled repeatedly for the OCME, without ever considering whether the code qualified as a trade secret under New York's relatively narrow substantive trade secret law.[298] For instance, one court

[295] *Cf.* Paul C. Giannelli, *The Right to Defense Experts*, CRIM. JUST., Summer 2003, at 15, 15-16 (documenting resource disparities that impede indigent defendants' access to expert services). The exception to this rule is criminal trade secret misappropriation, where defendants are more likely to be well-resourced industry competitors of the alleged victim. *See, e.g.*, People v. Gopal, 217 Cal. Rptr. 487, 493 (Ct. App. 1985) (featuring a criminal defendant "arguing that none of the information claimed to be a trade secret is in fact or law a trade secret"). Moreover, in criminal misappropriation prosecutions, a privilege to entirely withhold trade secret evidence is often unavailable anyway because due process requires the government to inform defendants what it is they are accused of stealing. As a result, the standard protection for trade secrets in such cases is already a protective order, not a withholding entitlement. *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, 464 (2015) (explaining that prosecutors use protective orders to "zealously guard a victim's trade secret information").

[296] Affirmation of Rebecca L. Johannesen in Support of Motion to Quash ¶ 9, People v. Johnson, No. 502/2014 (N.Y. Sup. Ct. Feb. 10, 2016); *see also id.* ¶ 12 ("Moreover, no [nondisclosure agreement] can adequately protect OCME's interest in its proprietary source code once it is disclosed . . . .").

[297] *Johnson* Subpoena Letter, *supra* note 80, at 2 ("Were OCME to hand over the source code, Legal Aid would have everything they need to cure defects in their own program . . . .").

[298] *See, e.g.*, People v. Carter, No. 2573/14, 2016 WL 239708, at *7 (N.Y. Sup. Ct. Jan. 12, 2016) (denying a defendant's discovery motion for source code in part because "the source code is proprietary" but failing to consider whether the "proprietary" interest rose to the level of a trade secret).

New York follows the relatively narrow Restatement definition of a trade secret. *See* Ashland Mgmt. Inc. v. Janien, 624 N.E.2d 1007, 1008, 1013 (N.Y. 1993) (relying on the Restatement (First) of Torts to hold that "a computerized mathematical stock selection model" that used mathematical formulas to evaluate financial criteria did not qualify as

footnote continued on next page

granted the OCME's motion in part because

> where the materials sought are privileged or confidential, as they are here, given New York City's copyright and proprietary interest in the Forensic Statistical Tool (FST) software, the defense must make a showing that the materials are not just relevant and material, but are reasonably likely to contain information that is exculpatory.[299]

The court never considered whether New York City's "proprietary interest" amounted to a trade secret.

Eventually, a defendant challenged the software in federal court,[300] and Judge Valerie Caproni of the Southern District of New York ordered the code's disclosure to the defense under a protective order.[301] A defense expert then reviewed the code and found an undisclosed function that caused the software program to discard data from certain calculations without notice to the user.[302] The expert opined that "[s]uch departures from the published descriptions of FST's behavior during its actual operation raise the question if additional undocumented behaviors, either intended or actual, affect casework samples."[303] Beyond even this serious concern, the incident exposes how trade secret barriers to criminal discovery can exacerbate gaps in regulatory enforcement; the OCME added the undisclosed function after the software program was validated and approved by New York's Commission on Forensic Science, but failed either to revalidate the program or to notify the Commission and seek its approval for the alteration.[304] Conversely, the

"secret"—and thus did not qualify as a trade secret—where the formulas were secret but the criteria had been publicly disclosed (citing 4 RESTATEMENT (FIRST) OF TORTS § 757 (AM. LAW INST. 1939))).

Note that most jurisdictions permit government entities to assert trade secret claims. *See* Levine, *supra* note 31, at 163-64 (observing that a minority of states refuse to recognize government trade secrets); *cf.* David S. Levine, *The People's Trade Secrets?*, 18 MICH. TELECOMM. & TECH. L. REV. 61, 107-10 (2011) (arguing against the validity of government trade secrets).

[299] *See* People v. Johnson, No. 00502-2014, slip op. at 2-3 (N.Y. Sup. Ct. Apr. 21, 2016).

[300] The agency again asserted that its code was "a proprietary and copyrighted statistical tool owned by the City of New York." Letter Regarding Voluntary Disclosure of FST Source Code at 1, United States v. Johnson, No. 1:15-cr-00565-VEC (S.D.N.Y. May 3, 2016).

[301] United States v. Johnson, No. 1:15-cr-00565-VEC, slip op. at 1 (S.D.N.Y. July 6, 2016) (stating that while the court was prepared to enter a protective order, it "question[ed] why a public laboratory would need a protective order in this context").

[302] Declaration of Nathaniel Adams at 20, *Johnson*, No. 1:15-cr-00565-VEC (S.D.N.Y Oct. 17, 2017).

[303] *Id.*

[304] *See* Letter from Julie Frye, Staff Attorney, The Legal Aid Soc'y, et al., to Catherine Leahy-Scott, N.Y. State Inspector Gen. 2-5 (Sept. 1, 2017) (on file with author). The Commission on Forensic Science is the regulatory authority charged with overseeing the OCME's DNA analysis methodologies. *See* N.Y. EXEC. LAW § 995-b (McKinney 2018).

incident also illustrates how removing trade secret barriers to criminal discovery can enhance the efficacy and credibility of regulatory oversight; when a defendant's expert witness exposed the alteration, defense attorneys alerted the state inspector general and sought an audit of the OCME.[305]

Returning to the privilege, the OCME's behavior shows that the rules governing the trade secret privilege in civil cases are inadequate to protect against borderline or even knowingly false assertions of the privilege in criminal proceedings. Notably, even after the undisclosed function was exposed, and after the OCME had replaced its in-house software program with an alternative program, the agency still refused to publicly disclose the code for the original program.[306] Not until journalists filed a motion to unseal based on the First Amendment did the agency finally publish the code and agree to a court order unsealing the expert's affidavits.[307] This type of behavior is especially troubling given that in practice, the privilege has been applied in criminal cases without any showing of trade secret validity. Overclaiming and abuse can surely be expected if courts and legislatures recognize a criminal trade secret privilege.

2. Raising the burden

To challenge the privilege, a party must show that the information is both relevant and *necessary* to its case.[308] The relevance and necessity analyses are distinct. Some courts treat the showing of relevance as a duplicate of the liberal discovery standards from civil procedure.[309] Others apply a more stringent

[305] *See* Letter from Julie Frye to Catherine Leahy-Scott, *supra* note 304, at 2, 12.

[306] *See* Lauren Kirchner, *Traces of Crime: How New York's DNA Techniques Became Tainted*, N.Y. TIMES (Sept. 4, 2017), https://perma.cc/V53S-CPL3; Barbara Sampson, *Setting the Record Straight on DNA Science*, MEDIUM (Sept. 6, 2017), https://perma.cc/64R4-ZTHB (describing the OCME's transition from FST to STRmix).

[307] *See* Memorandum in Support of Application by ProPublica for Leave to Intervene, Lift the Protective Order and Unseal Judicial Records at 20-22, United States v. Johnson, No. 1:15-cr-00565-VEC (S.D.N.Y. Sept. 25, 2017). "[A]fter long and careful consideration," the OCME decided not to object to the lifting of the protective order. *See* Letter Regarding ProPublica's Motion for Leave to Intervene at 1, *Johnson*, No. 1:15-cr-00565-VEC (S.D.N.Y. Oct. 10, 2017); *see also* Order at 1-2, *Johnson*, No. 1:15-cr-00565-VEC (S.D.N.Y. Oct. 16, 2017) (unsealing order).

[308] *See, e.g.*, People v. Superior Court (*Chubbs*), No. B258569, 2015 WL 139069, at *5 (Cal. Ct. App. Jan. 9, 2015) (citing Bridgestone/Firestone, Inc. v. Superior Court, 9 Cal. Rptr. 2d 709, 713 (Ct. App. 1992)).

[309] *See, e.g.*, Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co., 107 F.R.D. 288, 293 (D. Del. 1985) ("When disclosure of trade secrets is sought during discovery, the governing relevance standard that the movant must satisfy is the broad relevance standard applicable to pre-trial discovery . . . ."); Rohm & Haas Co. v. Lin, 992 A.2d 132, 143 (Pa. Super. Ct. 2010) ("Generally, discovery is liberally allowed to any matter, not privileged, which is relevant to the cause being tried. Discovery in trade secret

footnote continued on next page

test. For instance, the Texas Supreme Court has required a "heightened burden for obtaining trade secret information," asserting that "because relevance is the standard for discovery in general," requiring only the usual relevance showing "would render [the statutory privilege] meaningless."[310] The test for necessity in turn requires showing that the information is needed to prove or rebut a theory at trial;[311] that denial would cause a specific injury;[312] and that the information cannot be obtained from any alternative source.[313]

One problem with importing these rules wholesale into criminal proceedings is that the procedural backdrop against which they operate differs dramatically from civil disputes. Criminal discovery and subpoena regimes are miserly compared to their civil counterparts.[314] For example, parties have fewer obligations to disclose the facts, data, and full reports that form the bases of expert opinion testimony in criminal as compared to civil proceedings.[315] Criminal defendants already face a more challenging burden to obtain information. It is therefore more onerous for them to make the showing required to defeat the privilege. Even a criminal defendant's constitutional rights to discover particular types of evidence do not guarantee that the privilege will be defeated.[316] Imposing an unreasonably high burden on

litigation is permissible so long as the information sought to be obtained is reasonably related to the underlying cause of action and the need for this information outweighs any harm that may occur as a result of its release." (citation omitted)).

[310] *In re* Cont'l Gen. Tire, Inc., 979 S.W.2d 609, 613-14 (Tex. 1998).

[311] *See, e.g.*, *Coca-Cola Bottling*, 107 F.R.D. at 293.

[312] 1 MELVIN F. JAGER, TRADE SECRETS LAW § 5:33, at 5-167 (2017). Statutes codifying the privilege also generally include exceptions to ensure that "allowance of the privilege will not tend to conceal fraud or otherwise work injustice." *E.g.*, CAL. EVID. CODE § 1060 (West 2018); N.H. R. EVID. 507.

[313] *See, e.g.*, *In re Cont'l Gen. Tire*, 979 S.W.2d at 615; 1 JAGER, *supra* note 312, § 5:33, at 5-166 to -167; *id.* at 5-167 n.9 (collecting sources).

[314] *See infra* notes 343-65 and accompanying text.

[315] *See, e.g.*, United States v. Mehta, 236 F. Supp. 2d 150, 155 (D. Mass. 2002) (noting the "much broader" requirements and allowances under civil as opposed to criminal discovery rules for expert testimony).

[316] *See* EDWARD J. IMWINKELRIED & NORMAN M. GARLAND, EXCULPATORY EVIDENCE: THE ACCUSED'S CONSTITUTIONAL RIGHT TO INTRODUCE FAVORABLE EVIDENCE § 10-5, at 496 (4th ed. 2015) (explaining that in most cases, courts have rejected arguments that a defendant's constitutional right to present a defense should pierce an evidentiary privilege). *But see* Pennsylvania v. Ritchie, 480 U.S. 39, 57-61 (1987) (holding that the defendant was entitled to have privileged records reviewed by the judge in camera). In any event, the circumstances in which current doctrine and practice afford defendants constitutional rights to discovery are narrow. *See* Gray v. Netherland, 518 U.S. 152, 168 (1996) (confirming that the Constitution does not afford a general right to criminal discovery and that apart from *Brady v. Maryland*, 373 U.S. 83 (1963), it says little about the amount of discovery); Brandon L. Garrett, *Constitutional Regulation of Forensic Evidence*, 73 WASH. & LEE L. REV. 1147, 1179-80 (2016) (explaining that *Brady* obligations are "underdeveloped in the context of forensic evidence").

criminal defendants in turn exacerbates the risk of wrongfully excluding evidence and threatens the integrity of the truth-seeking process.[317]

3. Balancing procedural justice

Finally, courts weigh the seeking party's need for the information against the likely harm from disclosure.[318] Properly applied, the test considers disclosure not to the public, but rather to the opposing party under the terms of any protective order issued by the court.[319] Courts generally presume the risk of harm to be higher if the parties are business competitors and lower in other circumstances.[320] Courts may also consider the availability of alternative intellectual property protections, such as copyrights or patents, that can mitigate the risks from disclosure.[321] In most civil cases, courts grant discovery of trade secrets subject to a protective order.[322] In criminal cases, the opposite is true; courts frequently deny discovery altogether.[323]

Overvaluing trade secret claims in criminal cases is inconsistent with principles of procedural justice. Allan Lind and Tom Tyler have developed a "group value model" under which the legitimacy of the criminal justice system depends on the signals a legal process sends about how government authorities

[317] *Cf.* Welsh S. White, *Evidentiary Privileges and the Defendant's Constitutional Right to Introduce Evidence*, 80 J. CRIM. L. & CRIMINOLOGY 377, 378 (1989) ("When relevant defense evidence is excluded for some purpose other than enhancing the accuracy of fact-finding, the danger of convicting an innocent defendant increases."); Chessman, *supra* note 20, at 188-89, 222-23 (illustrating the gravity of source code errors for criminal defendants and arguing that broad discovery "enhances the fairness of the adversary system" by increasing the amount of evidence in the hands of both parties (quoting Taylor v. Illinois, 484 U.S. 400, 411 n.16 (1988))).

[318] *See* 1 JAGER, *supra* note 312, § 5:33, at 5-170.

[319] *See* Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co., 107 F.R.D. 288, 293 (D. Del. 1985).

[320] *Cf.* United States v. United Fruit Co., 410 F.2d 553, 556 (5th Cir. 1969) (noting the rule that courts should exercise discretion to avoid unnecessary disclosure of trade secrets, and all the more so when the case involves potential business competitors); Pincheira v. Allstate Ins. Co., 190 P.3d 322, 330 (N.M. 2008) (stating that "[d]etailed privilege logs or in camera hearings are unnecessary" when parties in a trade secret case are not competitors).

[321] *See* 3 JAGER, *supra* note 312, § 27:13, at 27-22 (2017).

[322] *See, e.g.*, Fed. Open Mkt. Comm. of the Fed. Reserve Sys. v. Merrill, 443 U.S. 340, 362 n.24 (1979) (stating that a trial court in a civil case will more commonly enter a protective order than forbid any disclosure of trade secrets). *But see* Bridgestone/Firestone, Inc. v. Superior Court, 9 Cal. Rptr. 2d 709, 713, 716 (Ct. App. 1992) (applying the privilege to reverse a trial court's discovery order in a products liability case).

[323] *See* Imwinkelried, *supra* note 20, at 99-101.

value particular social groups.[324] According to this model, the trade secret privilege's balancing test is suspect because it appears to place pure financial interests on par with life and liberty. More specifically, the test signals that courts value intellectual property holders more than two other social groups. The first group thus denigrated comprises anyone who is affected by a criminal justice outcome and for whom greater transparency could provide assurance that the outcome was proper. At a minimum, this group includes defendants, victims, and their families and communities.

The second denigrated group comprises persons whose duty to testify conflicts with their interests in confidentiality or property—but whose interests are not defined as trade secrets—and who are forced to testify nonetheless under existing law. Criminal courts frequently balance compelled disclosure against an array of counterweights, such as murder victims' privacy rights in their personal writings[325] or parents' resistance to testifying against their children.[326] Yet such competing interests are often unshielded by privilege.[327] So too, financial interests do not generally excuse compliance with criminal subpoenas.[328] In rare cases, a court might consider "genuine financial oppression" as one factor in determining the reasonableness of a subpoena.[329] But such consideration is nothing like a categorical privilege because it is evaluated on a case-by-case basis and could theoretically apply to anyone. In comparison, the trade secret privilege is a complete outlier that singles out the owners of a particular type of property for categorical, special treatment.

[324] *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, 412-13 (2002) (citing E. ALLAN LIND & TOM R. TYLER, THE SOCIAL PSYCHOLOGY OF PROCEDURAL JUSTICE 228-40 (1998)).

[325] *See* Marijo A. Ford & Paul A. Nembach, Note, *The Victim's Right to Privacy: Imperfect Protection from the Criminal Justice System*, 8 ST. JOHN'S J. LEGAL COMMENT. 205, 212-15 (1992).

[326] Note, *Parent-Child Loyalty and Testimonial Privilege*, 100 HARV. L. REV. 910, 910 (1987).

[327] *See, e.g.*, *Open Issue: Whether to Recognize a Parent-Child Privilege?*, FED. EVIDENCE REV. (June 18, 2014), https://perma.cc/7D8D-7PRB.

[328] *See* Hurtado v. United States, 410 U.S. 578, 589 (1973) (asserting the general rule that one has a "public obligation to provide evidence . . . no matter how financially burdensome it may be").

[329] *See In re* Grand Jury Subpoena Duces Tecum Issued to the First Nat'l Bank of Md., 436 F. Supp. 46, 49 (D. Md. 1977) (declining to order reimbursement for the financial costs of complying with a grand jury subpoena because "the obligation to provide evidence persists in the face of all but genuine financial oppression").

B. The Trade Secret Privilege Is Unnecessary in Criminal Cases

This Subpart contends that options other than an evidentiary privilege suffice to protect 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 motions and subpoenas without resort to privilege. And in extreme cases in which disclosing relevant information in response to nonfrivolous defense requests creates well-founded concerns of harm, limited protective orders are available to safeguard the interests of trade secret holders to the full extent reasonable. Robert Cary and colleagues have written a thorough overview of federal criminal discovery and subpoena rules and practice.[330] I draw on their analysis to show precisely how high the threshold already is for defendants to access trade secret evidence, without a privilege raising that bar higher still. The following discussion focuses on federal criminal procedure, but similar issues arise in analogous state statutes.[331]

1. Discovery

The first avenue for protecting trade secrets without relying on a blanket privilege involves reasonable restrictions on criminal discovery. Criminal discovery was virtually nonexistent until the mid-twentieth century.[332] One classic justification for its absence was that providing discovery would exacerbate constitutional inequalities that already skewed in favor of the defense,[333] such as the prosecution's burden of proof[334] or Fifth Amendment limits on the government's power to demand inculpatory evidence from the

[330] ROBERT M. CARY ET AL., FEDERAL CRIMINAL DISCOVERY (2011).

[331] *See* 5 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 20.2(b) (4th ed. 2015) (comparing, generally, the structure of federal and state criminal discovery provisions); *id.* § 20.3(*l*) (describing federal and state provisions for the issuance of protective orders); *see also, e.g.,* John Schoeffel, The Legal Aid Soc'y, Criminal Discovery Reform in New York: A Proposal to Repeal C.P.L. Article 240 and to Enact a New C.P.L. Article 245, at 2-3 (2009) (on file with author) (describing various state criminal discovery provisions and recent reforms).

[332] *See* 5 LAFAVE ET AL., *supra* note 331, § 20.1(a); 2 WRIGHT & GRAHAM, *supra* note 40, § 251 (4th ed. 2009).

[333] *See, e.g.,* CARY ET AL., *supra* note 330, at 4 (discussing Chief Justice Vanderbilt of the New Jersey Supreme Court and his argument against providing criminal discovery to defendants, as well as Justice Brennan's response in favor of such discovery).

[334] *Cf.* Richard A. Posner, *An Economic Approach to the Law of Evidence*, 51 STAN. L. REV. 1477, 1504-07 (1999) (arguing that prosecutors' higher burden of proof partially balances defendants' comparatively limited investigative resources).

accused.[335] If discovery were granted, the argument went, the government would open its files to the defense but receive nothing comparable in return.[336]

Critics of this anti-discovery perspective observed the numerous other procedural and material powers that skew in favor of the government,[337] such as a prosecutor's power to effectively depose witnesses by convening a grand jury investigation.[338] Paul Giannelli has argued that limited criminal discovery has particularly perverse effects for the adversarial review of expert evidence.[339] Reflecting these types of critiques, the classic understanding of criminal discovery began to shift by 1946 with the adoption of Rule 16 of the Federal Rules of Criminal Procedure, which provided the defense some minimal rights of access to information about the government's case.[340]

[335] *See* 2 WRIGHT & GRAHAM, *supra* note 40, § 251, at 57-58 (4th ed. 2009); *see also, e.g.*, United States v. Garsson, 291 F. 646, 649 (S.D.N.Y. 1923) (L. Hand, J.) ("Under our criminal procedure the accused has every advantage. . . . He is immune from question or comment on his silence . . . . Why in addition he should in advance have the whole evidence against him to pick over at his leisure, and make his defense, fairly or foully, I have never been able to see.").

[336] *See, e.g.*, *Garsson*, 291 F. at 649 ("While the prosecution is held rigidly to the charge, [the accused] need not disclose the barest outline of his defense.").

[337] *See, e.g.*, William J. Brennan, Jr., *The Criminal Prosecution: Sporting Event or Quest for Truth?*, 1963 WASH. U. L.Q. 279, 285-87 (1963) (arguing that the limited financial resources of many criminal defendants and the late stage at which defense attorneys are usually appointed militate in favor of expanding defendants' discovery rights); Abraham S. Goldstein, *The State and the Accused: Balance of Advantage in Criminal Procedure*, 69 YALE L.J. 1149, 1152 (1960) (arguing that criminal procedure "gives overwhelming advantage to the prosecution").

[338] *See* Andrew D. Leipold, *Why Grand Juries Do Not (and Cannot) Protect the Accused*, 80 CORNELL L. REV. 260, 314-17 (1995); David A. Sklansky & Stephen C. Yeazell, *Comparative Law Without Leaving Home: What Civil Procedure Can Teach Criminal Procedure, and Vice Versa*, 94 GEO. L.J. 683, 714 (2006).

[339] *See* Paul C. Giannelli, *Pretrial Discovery of Expert Testimony*, 44 CRIM. L. BULL. 943, 943-45 (2008); *see also* Murphy, *supra* note 25, at 751-52 (arguing that the government's exclusive access to its forensic databases "inevitably inhibits or outright prevents defense attorneys and independent researchers from challenging the validity of the government's conclusions").

[340] *See* FED. R. CRIM. P. 16 advisory committee's note (noting that the rule gives courts discretion to grant defendants access to materials seized by the state); CARY ET AL., *supra* note 330, at 2 (identifying the enactment of Rule 16 as a turning point for criminal discovery).

Subsequent reforms slowly increased the scope of criminal discovery[341] and imposed some reciprocal disclosure requirements on the defense.[342]

But despite a gradual expansion, criminal discovery today remains sufficiently restrictive to adequately protect trade secrets from wrongful disclosure without resort to a privilege. It imposes three main limits on disclosure, which I refer to as *materiality*, *summarization*, and *good cause* restrictions. First, unlike civil parties that may discover broad swaths of merely tangentially relevant documents and then sift through them to determine what to use in a case, criminal defendants generally cannot obtain immaterial information in discovery.[343] Criminal defendants must establish materiality via a prima facie showing that information has "more than . . . some abstract logical relationship to the issues in the case" and would allow them "significantly to alter the quantum of proof in [their] favor."[344] While some courts have described this showing as "not a heavy burden,"[345] it does require specificity that can be difficult to achieve.[346] As a result, while a civil trade secret privilege could conceivably be necessary to prevent bulk disclosures of trade secrets that are barely related to a case, a criminal trade secret privilege

[341] The Jencks Act of 1957 required the government to disclose prosecution witnesses' prior statements. *See* Pub. L. No. 85-269, 71 Stat. 595 (codified as amended at 18 U.S.C. § 3500 (2016)). In 1963, the U.S. Supreme Court held in *Brady v. Maryland* that the government has a constitutional obligation to disclose exculpatory or material information to the defense. *See* 373 U.S. 83, 87 (1963).

[342] *See* 5 LAFAVE ET AL., *supra* note 331, § 20.1(d), at 424-25. In general, these "prosecution discovery provisions" are "much narrower in scope than [the] defense-discovery provisions." *Id.* at 425.

[343] *Compare* FED R. CIV. P. 26(b)(1) (providing for "discovery regarding any nonprivileged matter that is *relevant* to any party's claim or defense and proportional to the needs of the case" (emphasis added)), *with* FED. R. CRIM. P. 16(a)(1)(E) (providing that "the government must permit the defendant to inspect . . . [documents or objects if] the item is *material* to preparing the defense" (emphasis added)).

[344] *See, e.g.*, United States v. Ross, 511 F.2d 757, 762-63 (5th Cir. 1975); *see also* 5 LAFAVE ET AL., *supra* note 331, § 20.3(g), at 486 & n.128 (citing *Ross* for the proposition that showing materiality is a higher burden than showing relevancy); *id.* at 486 n.126 (describing some variation in materiality requirements between states).

[345] *E.g.*, United States v. George, 786 F. Supp. 56, 58 (D.D.C. 1992).

[346] *See, e.g.*, United States v. Mayes, 917 F.2d 457, 461 (10th Cir. 1990) (rejecting a constitutional challenge to Rule 16's exceptions to the government's disclosure obligations); 9A BARBARA J. VAN ARSDALE ET AL., FEDERAL PROCEDURE: LAWYERS EDITION § 22:1208 (2015) (describing precedent from seven federal courts of appeals requiring criminal defendants to make discovery requests with some specificity); *see also* FED. R. CRIM. P. 16 advisory committee's note to 1974 amendment ("It may be difficult for a defendant to make [the materiality] showing if he does not know what the evidence is."); *cf.* United States v. Burr, 25 F. Cas. 187, 191 (C.C.D. Va. 1807) (No. 14,694) (Marshall, C.J.) ("Now if a paper be in possession of the opposite party, what statement of its contents or applicability can be expected from the person who claims its production, he not precisely knowing its contents?").

cannot be so justified because criminal discovery's materiality restrictions already serve that function.

Second, Rule 16 also includes summarization restrictions: discovery obligations that the government can fulfill by mere summary, rather than disclosure, of original documents. For instance, Rule 16(a)(1)(G) obliges the government upon request to disclose a summary of any expert opinion testimony it intends to introduce.[347] In theory, the disclosure must suffice to allow the defense to prepare for cross-examination.[348] In practice, the required disclosure of an expert's methodology can be satisfied by a general description.[349] Critics have argued that such descriptions are inadequate. For instance, the National Commission on Forensic Science, a joint commission of the Department of Justice and the Department of Commerce's National Institute of Standards and Technology, recently recommended expanding pretrial criminal discovery in order to help defense attorneys prepare to challenge potentially invalid or unreliable forensic evidence.[350] In the commission's

[347] FED. R. CRIM. P. 16(a)(1)(G) (requiring the government to provide "a written summary" that "must *describe*" an expert witness's opinions, bases and reasons for those opinions, and qualifications (emphasis added)). *Compare id.*, *with* FED. R. CIV. P. 26(a)(2)(B) (requiring expert witnesses to author and sign written reports that "must *contain* . . . a complete statement of all opinions," bases and reasons for those opinions, qualifications, facts or data they considered, a history of prior testimony, and their compensation (emphasis added)).

[348] *See* FED. R. CRIM. P. 16 advisory committee's note to 1993 amendment; *see also* CARY ET AL., *supra* note 330, at 125. The advisory committee note to Rule 705 of the Federal Rules of Evidence, one of the rules governing expert testimony, cites Rule 26 of the Federal Rules of Civil Procedure as reassurance that "the cross-examiner [will have] the advance knowledge which is essential for effective cross-examination." FED. R. EVID. 705 advisory committee's note. But no parallel to Rule 26 exists in criminal cases.

[349] *See, e.g.*, United States v. Mehta, 236 F. Supp. 2d 150, 156 (D. Mass. 2002) ("The government properly has provided summary charts . . . and has described generally the methodology used in creating those charts. . . . Nothing more is required."); CARY ET AL., *supra* note 330, at 123 ("Certainly the rule does not require the level of detail expected of a Civil Rule 26 report."); Giannelli, *supra* note 339, at 947 (observing that laboratories have been criticized for "preparation of reports containing minimal information in order not to give the 'other side' ammunition for cross-examination" (quoting Douglas M. Lucas, *The Ethical Responsibilities of the Forensic Scientist: Exploring the Limits*, 34 J. FORENSIC SCI. 719, 724 (1989))); NAT'L COMM'N ON FORENSIC SCI., PRETRIAL DISCOVERY IN FORENSIC EVIDENCE CASES 6, 11-13 (n.d.), https://perma.cc/5TL5-YB9X (arguing that expert discovery requirements are inadequate in federal criminal cases); *see also* NAT'L RESEARCH COUNCIL, NAT'L ACADS. OF SCIS., STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 21 (2009) (noting that many forensic laboratory reports contain insufficient methodological detail); Paul C. Giannelli, *Criminal Discovery, Scientific Evidence, and DNA*, 44 VAND. L. REV. 791, 803-04 (1991) (same).

[350] *See* Nat'l Comm'n on Forensic Sci., Views of the Commission: Pretrial Discovery of Forensic Materials 1-3 (2015), https://perma.cc/AH5L-6KKE; *see also* NAT'L COMM'N ON FORENSIC SCI., *supra* note 349, at 1-2. Judge Rakoff of the Southern District of New York resigned from the commission in protest when it appeared that pretrial discovery reforms might be overlooked. *See Full Text: Judge's Protest Resignation Letter*, WASH. POST

footnote continued on next page

appraisal, Rule 16(a)(1)(G) disclosures have been insufficient to prevent the introduction of faulty forensics into trials.[351] Whether or not one agrees with the critics' view, one thing is clear: Summarization restrictions make the trade secret privilege redundant because they limit defense access to in-depth, unfiltered information regardless of its trade secret status.

Third, trial courts also have broad discretion to prevent abusive, frivolous, or harassing discovery requests.[352] Rule 16(d)(1) grants a district court discretion "for good cause [to] deny, restrict, or defer discovery or inspection, or grant other appropriate relief," including nondisclosure orders.[353] This additional guarantee applies explicitly to protect "business enterprises from economic reprisals."[354] A court may find "good cause" on its own, without any required showing by the parties, and subject only to abuse of discretion review.[355] Alternatively, a moving party may make an ex parte submission to the court requesting a "good cause" limit on its disclosure obligations.[356] These procedural constraints are sufficient to protect against abusive discovery demands without resort to a categorical privilege.

2. Subpoenas

Baked-in procedural limits on criminal subpoenas are even more restrictive than their discovery counterparts. To obtain a criminal subpoena, the moving party must make a preliminary showing of relevancy, admissibility, and specificity for the information sought.[357] The relevancy showing is

(Jan. 29, 2015), https://perma.cc/QZC3-PGVG. Judge Rakoff returned to the commission after the Justice Department revised its position. *See* Spencer S. Hsu, *Judge Rakoff Returns to Forensic Panel After Justice Department Backs Off Decision*, WASH. POST (Jan. 30, 2015), https://perma.cc/7H4C-A6QS.

[351] *See* NAT'L COMM'N ON FORENSIC SCI., *supra* note 349, at 11-13; *see also* Nat'l Comm'n on Forensic Sci., *supra* note 350, at 1-2. Note that Rule 16(a)(1)(G) disclosures may be narrower than those required for a *Daubert* challenge. *See* Margaret A. Berger, *Procedural Paradigms for Applying the* Daubert *Test*, 78 MINN. L. REV. 1345, 1360 (1994).

[352] *See* FED. R. CRIM. P. 16 advisory committee's note to 1966 amendment (noting that Rule 16 "provisions [were] made to guard against possible abuses").

[353] FED. R. CRIM. P. 16(d)(1); *see also* Taylor v. Illinois, 484 U.S. 400, 415 n.20 (1988) ("Under the Federal Rules of Criminal Procedure and under the rules adopted by most States, a party may request a protective order if he or she has just cause for objecting to a discovery request."); Alderman v. United States, 394 U.S. 165, 185 (1969).

[354] *See* FED. R. CRIM. P. 16 advisory committee's note to 1966 amendment; *see also id.* 16 advisory committee's note to 1974 amendment (indicating that good cause includes "economic harm").

[355] *See* 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).

[356] *See* FED. R. CRIM. P. 16(d)(1).

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

lenient: It tracks Rule 401 of the Federal Rules of Evidence,[358] which defines relevance in part as having "any tendency to make a fact more or less probable than it would be without the evidence."[359] But to satisfy the admissibility requirement, the moving party must show that the subpoenaed information itself is likely to be evidentiary. That is, mere likelihood that the information will point to the discovery of other admissible evidence is not enough.[360]

Meeting such a high standard can be particularly difficult before trial, when a defendant's theory of the case has not fully developed. To help assuage that difficulty, some courts have interpreted the specificity requirement leniently, finding it to be coterminous with a showing of relevance and admissibility.[361] Other courts have taken a more stringent view, requiring an additional showing of what the materials are likely to contain.[362] Regardless, the subpoena must be made "in good faith"; it cannot be a "fishing expedition."[363] And parties moving for pretrial subpoenas must satisfy yet another burden: They must show that it is necessary to access the documents before trial begins.[364] Finally, as with the "good cause" restrictions on criminal discovery, courts have discretion to "quash or modify [a] subpoena if compliance would be unreasonable or oppressive."[365]

In sum, trade secret information that is not sufficiently likely to produce relevant and admissible evidence is not subject to subpoena, with or without a privilege. And even admissible evidence will not be subject to subpoena,

[358] *See* CARY ET AL., *supra* note 330, at 226 ("Courts following *Nixon* have defined the 'relevancy' hurdle by reference to Evidence Rule 401 . . . .").

[359] FED. R. EVID. 401(a). To be relevant, the fact made more or less probable must be "of consequence in determining the action." *Id.* 401(b).

[360] *See Nixon*, 418 U.S. at 698 (observing that subpoenas are "not intended to provide a means of discovery for criminal cases"); 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 also* CARY ET AL., *supra* note 330, at 227 (stating that civil but not criminal subpoenas can be used to lead to the discovery of other admissible evidence).

[361] *See, e.g.*, United States v. Libby, 432 F. Supp. 2d 26, 31 (D.D.C. 2006) (noting that specificity can be satisfied "if there is a 'sufficient likelihood' . . . that the documents being sought contain relevant and admissible evidence" (quoting *Nixon*, 418 U.S. at 700)). *But see* CARY ET AL., *supra* note 330, at 232 ("Specificity is also what sets the criminal subpoena most sharply apart from the civil.").

[362] *See, e.g.*, United States v. Hardy, 224 F.3d 752, 755 (8th Cir. 2000); CARY ET AL., *supra* note 330, at 228-29.

[363] *Nixon*, 418 U.S. at 699-700 (citing United States v. Iozia, 13 F.R.D. 335, 338 (S.D.N.Y. 1952)).

[364] *See id.* at 699 (requiring the party requesting a subpoena to show that it "cannot properly prepare for trial without such production and inspection in advance of trial").

[365] *See* FED. R. CRIM. P. 17(c)(2).

especially before trial, unless defendants clear a slew of other challenging hurdles.

Those limits can guard against inappropriate requests for trade secrets. As a case in point, some defendants might engage in a form of "graymail" by demanding disclosure of trade secrets with the intent to pressure the prosecution to drop the case, or at least to withdraw certain evidence.[366] A defendant could demand (1) the government's own trade secrets, (2) those of an expert witness, or (3) those of a third-party vendor. In the second and third scenarios, the prosecution might worry about damaging the government's relationship with experts or vendors and foreclosing opportunities to work with them in future cases. But graymail tactics can be adequately addressed using normal discovery and subpoena standards; trial courts are tasked with distinguishing between abusive discovery or subpoena motions and their legitimate counterparts, and courts are given the discretion to act accordingly.

Consider a recent case before the D.C. Circuit in which a convicted defendant sought access to the mapping software the Drug Enforcement Administration (DEA) uses to analyze GPS location-tracking data, the results of which had been introduced into evidence at his criminal trial.[367] While it is conceivable that accessing the software could have been useful to the defense—perhaps by enabling an expert to evaluate whether the program generated a misleading display of the defendant's location—a court could also plausibly find that the methodology for producing that display was entirely irrelevant to the case. Had the defendant sought to discover or subpoena the software during his criminal trial, the court could have denied the motions as not "material to preparing the defense"[368] or "unreasonable."[369]

3. Protective orders, sealing, and courtroom closures

For trade secret evidence that satisfies the criminal discovery or subpoena requirements, courts can mitigate any risk from disclosure by using protective

[366] *See* Rosenblatt, *supra* note 260, at 15. This issue arose in cases surrounding the child pornography website Playpen when parties sought source code of a cybercrime investigative software program, source code whose secrecy was arguably key to the efficacy of the tool. *See, e.g.*, United States v. Levin, 874 F.3d 316, 318, 320 (1st Cir. 2017) (describing the "network investigative technique" used to obtain IP addresses of visitors to the site); *see also* Farivar, *supra* note 93 (noting that federal prosecutors voluntarily dismissed their appeal "[r]ather than disclose the source code").

[367] *See* Aguiar v. DEA, 865 F.3d 730, 733 (D.C. Cir. 2017). The DEA denied the defendant's requests, claiming that the software was not an agency record within the meaning of 5 U.S.C. § 552 because it was licensed from a third-party vendor. *See Aguiar*, 865 F.3d at 733, 735-36.

[368] FED. R. CRIM. P. 16(a)(1)(E)(i).

[369] *Id.* 17(c)(2).

orders, sealing orders, and limited courtroom closures.[370] For example, protective orders may require the defense to keep the information confidential and to use it for no purpose other than the instant proceeding.[371] When necessary, judges can limit disclosure to opposing counsel and expert witnesses.[372]

In civil discovery, judges routinely order trade secrets disclosed to opposing parties under protective orders.[373] When documents are filed with the court, parties can move to seal them from public view.[374] And once a case reaches trial, courts impose an array of measures to safeguard trade secrets from public disclosure: They can order that trade secret evidence be displayed on screens visible to the jury but not the gallery; instruct counsel and witnesses to refer to information abstractly, such as by predetermined numbers corresponding to the screen displays; or temporarily close the courtroom if it becomes necessary to testify about the pure substance of a trade secret.[375] These types of safeguards are standard in civil suits for trade secret misappropriation, in which plaintiffs generally must reveal their secrets with "reasonable

[370] *See* UNIF. TRADE SECRETS ACT § 5 (UNIF. LAW COMM'N 1985) ("[A] court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include granting protective orders in connection with discovery proceedings, holding in-camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval.").

[371] *See, e.g.*, State v. Peters, 264 P.3d 1124, 1128 (Mont. 2011) (describing an order limiting access to trade secrets to counsel, expert witnesses, parties, and a few others).

[372] *See, e.g.*, United States v. Siegel, No. 96 Cr. 411 (ACS), 1997 WL 12804, at *4 (S.D.N.Y. Jan. 14, 1997) (ordering that a third party's trade secret bid formula "may be reviewed only by defendants' counsel and an expert retained by the defendants, solely for the purposes of preparing and presenting a defense to the pending criminal charges").

[373] *See, e.g.*, Fed. Open Mkt. Comm. of the Fed. Reserve Sys. v. Merrill, 443 U.S. 340, 362 n.24 (1979) ("[O]rders forbidding any disclosure of trade secrets . . . are rare. More commonly, the trial court will enter a protective order . . . ."); Dinler v. City of New York (*In re* City of New York), 607 F.3d 923, 935 (2d Cir. 2010) ("The disclosure of confidential information on an 'attorneys' eyes only' basis is a routine feature of civil litigation involving trade secrets."). Civil protective orders are generally available on a showing of "good cause." *See* FED. R. CIV. P. 26(c)(1). The Northern District of California has even published a model protective order for trade secrets in civil litigation that limits disclosure of "highly confidential" information to "attorneys' eyes only." *See* Model Protective Order for Litigation Involving Patents, Highly Sensitive Confidential Information and/or Trade Secrets (n.d.), https://perma.cc/NVQ7-8D9Z (archived Apr. 10, 2018).

[374] *See, e.g.*, Pintos v. Pac. Creditors Ass'n, 605 F.3d 665, 678 (9th Cir. 2010) (noting that motions to seal must show "compelling reasons" that outweigh the common law right of access to judicial documents (quoting Kamakana v. City & County of Honolulu, 447 F.3d 1172, 1178-79 (9th Cir. 2006))).

[375] *See, e.g.*, Order re Motion to Close Courtroom at 2-3, Waymo LLC v. Uber Techs., Inc., No. 3:17-cv-00939-WHA (N.D. Cal. Jan. 18, 2018). Thank you to Victoria Cundiff for suggesting this example.

particularity" as part of their prima facie claim.[376] The fact that trade secret owners routinely pursue civil misappropriation claims,[377] despite the likelihood that they will have to disclose some or all of their secrets during litigation, indicates that procedural safeguards work.

Similar procedures can be and are applied successfully in criminal cases, notwithstanding defendants' Sixth Amendment right to a public trial.[378] For instance, in criminal prosecutions for trade secret misappropriation, the government often must disclose the victim's confidential information.[379] As in civil litigation, courts mitigate risk to the trade secret owner via protective orders, sealing orders, and limited courtroom closures.[380]

Perhaps, then, trade secrets should always be disclosed under a protective order to criminal defendants who can meet the standard discovery or subpoena requirements. Developers have argued against this solution in part by voicing concern that a defendant's counsel or expert witnesses will themselves misappropriate the trade secret. For example, the OCME reported a belief that defense counsel was seeking source code to develop a competing software

[376] *See, e.g.*, CAL. CIV. PROC. CODE § 2019.210 (West 2018) ("In any action alleging the misappropriation of a trade secret . . . , the party alleging the misappropriation shall identify the trade secret with reasonable particularity subject to any [protective] orders that may be appropriate . . . ."); Nilssen v. Motorola, Inc., 963 F. Supp. 664, 671-73 (N.D. Ill. 1997) (requiring that the plaintiff "articulate protectable trade secrets with specificity or suffer dismissal of his claim").

[377] *See* David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 301, 302 tbl.1 (2009/2010) (documenting a dramatic rise in federal trade secret cases from 1990 to 2010).

[378] *See* U.S. CONST. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial . . . .").

[379] *See, e.g.*, United States v. Fei Ye, 436 F.3d 1117, 1119, 1121, 1124 (9th Cir. 2006) (observing that the government had "previously disclosed all of the trade secret materials pursuant to a protective order"). *But cf.* United States v. Hsu, 155 F.3d 189, 191-92, 197-204 (3d Cir. 1998) (denying discovery of trade secrets to a defendant charged with attempt or conspiracy to steal those secrets because the trade secrets' validity was not an element of those offenses); Levine & Flowers, *supra* note 295, at 476 (noting that prosecutors limit disclosure of trade secrets by bringing "charges that do not require the prosecution to prove the information taken by the defendant actually constituted a trade secret").

[380] *See* 18 U.S.C. § 1835 (2016) (providing protections to preserve confidentiality in federal trade secret cases); United States v. Aleynikov, No. 10 Cr. 96(DLC), 2010 WL 5158125, at *1 (S.D.N.Y. Dec. 14, 2010) (describing a decision to exclude the public from portions of a jury trial during which trade secrets would be disclosed); United States v. Roberts, No. 3:08-CR-175, 2010 WL 1010000, at *8-9 (E.D. Tenn. Mar. 17, 2010) (concluding that Sixth Amendment rights are not "adversely affected or infringed by placing reasonable and minimal restrictions on the public's, not defendants' or the jury's, right to have access to . . . information"); Levine & Flowers, *supra* note 295, at 466-67, 476 (observing that prosecutors rely on protective orders under Rule 16(d) of the Federal Rules of Criminal Procedure to limit disclosure of trade secrets).

program, one that "would then be made public as an exact facsimile of something belonging to the City of New York."[381]

The risk of leaks is discussed in Part III.C.2 below; here, I identify a related issue. A vigorous defense that is proper in every way could also in certain respects resemble a business competition. Defendants who successfully subpoena trade secret information will likely—and should—use the secrets to challenge the validity and reliability of criminal justice technologies, perhaps even by building alternative tools for independent testing. These challenges could have detrimental effects on the commercial value of the technology, for instance by identifying its flaws and vulnerabilities. But it would be a mistake to characterize vigorous defense representation as unfair business competition rather than core legal process. As long as defendants do not brandish legal process for the improper purpose of obtaining commercial advantages, their efforts should be clearly distinguished from misappropriation.

It is also true that overly stringent protective orders can be highly problematic. For instance, Jonathan Abel has documented the "devastating effect" of protective orders providing that information about police officer misconduct may be used only in a particular case.[382] The result has been that prosecutors and defense attorneys who are aware of officer misconduct covered by a protective order can neither inform their colleagues nor use the knowledge themselves in future cases featuring testimony by that officer, interfering with prosecutors' *Brady* obligation to disclose favorable material evidence within their constructive knowledge.[383] Similar problems could occur in the trade secret context if experts in one case identify serious flaws in a forensic system but are unable to share that information with future defendants.

A possible way to avert such scenarios would be to exempt an expert's conclusion from the protective order while maintaining confidentiality for the trade secret bases of that conclusion. If the expert finds no flaws in the system, then the null result would be disclosed, and the trade secrets could remain protected without causing concern. If the expert concludes that the system is seriously flawed, then that finding could be shared. Future defendants could use the expert's conclusion to support additional discovery and subpoena motions. In exceptional cases, members of the press or public could intervene and move to unseal the record by challenging whether good cause exists for continued confidentiality.[384]

[381] *See Johnson* Subpoena Letter, *supra* note 80, at 2.

[382] *See* Jonathan Abel, Brady*'s Blind Spot: Impeachment Evidence in Police Personnel Files and the Battle Splitting the Prosecution Team*, 67 STAN. L. REV. 743, 802 (2015).

[383] *See id.* at 802-03.

[384] *Cf.* Seattle Times Co. v. Rhinehart, 467 U.S. 20, 37 (1984) (holding that a protective order for pretrial discovery information does not offend the First Amendment if it is based on a showing of good cause); United States v. Simon (*In re* Application of Dow

footnote continued on next page

At some point, the defense community might also seek to override protective orders and share trade secret information with each other in an attempt to pool resources and thus better understand and rebut complex forensic evidence. Murphy has pointed out that due to resource constraints, the decentralized nature of criminal defense work, and strategic tradeoffs in individual cases, it is often not feasible for defense attorneys to challenge the underlying methodologies of technologically complex forensic science methods.[385] 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."[386] That board could grant limited access to appropriate researchers asking generalizable questions about a forensic methodology and make the research "available on a broad basis, to the benefit of defendants as a class."[387] That proposal was well developed, and hopefully we will accomplish it soon.[388] But defendants also need access to information about how technology was used in their individual cases, and this may require continued disclosure of sensitive information on an individual basis. Centralized review and adversarial scrutiny can exist symbiotically.

C. The Trade Secret Privilege Overprotects Intellectual Property

This Subpart shows why neither the law nor the theory of trade secrecy justifies recognizing a trade secret privilege in criminal cases. Not only do the theoretical rationales for trade secrecy fail to support the privilege, but they also actually encourage its opposite: disclosure of trade secret evidence to the accused, subject to a protective order.

1. Substantive trade secret law, compared

Trade secret law protects secret information from wrongful acquisition or use. The general requirements are as follows. Information qualifies for legal

Jones & Co.), 842 F.2d 603, 607 (2d Cir. 1988) (recognizing that the First Amendment protects the rights of "potential receivers of otherwise restrained speech" to intervene); Daniels v. City of New York, 200 F.R.D. 205, 207 (S.D.N.Y. 2001) (noting that "[w]hen a private party asserts a public interest in order to gain access to information" by modifying a protective order, the party seeking to maintain confidentiality has the burden to show "'good cause' for continued confidentiality").

[385] *See* Murphy, *supra* note 25, at 761-62.

[386] *See id.* at 778.

[387] *See id.* at 783-84.

[388] *Cf.* Barack Obama, Commentary, *The President's Role in Advancing Criminal Justice Reform*, 130 HARV. L. REV. 811, 860-62 (2017) (documenting recent efforts to strengthen forensic sciences generally, including a collaboration between the FBI, the Innocence Project, and the National Association of Criminal Defense Lawyers that could serve as a model for the board Murphy proposes).

protection if the owner "has taken reasonable measures to keep such information secret" and if "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information."[389] The law does not protect against *all* acquisitions or uses of trade secrets, but rather only *improper* ones, known as misappropriations.[390] Thus, while theft, deceit, and skullduggery count as misappropriation, independent discovery and reverse engineering do not.[391] If a hostile competitor dismantles a publicly available product and uncovers the secret, no cause of action will lie.[392]

Compared to substantive trade secret law, an evidentiary privilege to withhold information overprotects. This is because trade secrets that are subject to discovery or subpoena already enjoy standard legal protections as trade secrets. Should an opposing party submit an abusive discovery demand or violate a protective order, that party would be liable for misappropriation. The owner of those trade secrets could seek the usual remedies, from damages[393] to criminal penalties.[394] Layering on an evidentiary privilege to withhold the information in the first place thus creates stronger protections in evidence law than trade secrets enjoy elsewhere.

This calculation of comparative overprotection holds even if one analogizes the privilege to an injunction. Both restrain the use of information ex ante. But injunctions are significantly more burdensome to obtain under substantive trade secret law; they generally require a showing of "actual or threatened"

[389] *See* 18 U.S.C. § 1839(3) (2016).

[390] *See id.* § 1839(5) ("[T]he term 'misappropriation' means . . . acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or . . . disclosure or use of a trade secret of another without express or implied consent by a person who . . . used improper means to acquire knowledge of the trade secret [or] . . . knew or had reason to know that the knowledge of the trade secret was [acquired by improper means] . . . .").

[391] *See id.* § 1839(6) ("[T]he term 'improper means' . . . includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage . . . and . . . does not include reverse engineering, independent derivation, or any other lawful means of acquisition . . . .").

[392] *See id.*

[393] *See id.* § 1836(b)(1) ("An owner of a trade secret that is misappropriated may bring a civil action under this subsection . . . ."); *id.* § 1836(b)(3)(B) (providing for damages).

[394] *See, e.g.*, TEX. PENAL CODE ANN. § 31.05(b) (West 2017) ("A person commits an offense if, without the owner's effective consent, he knowingly . . . makes a copy of an article representing a trade secret . . . ."); *see also id.* § 31.05(c) ("An offense under this section is a felony of the third degree.").

misappropriation.[395] Mere speculative risk does not suffice.[396] With the privilege, in contrast, there does not have to be any actual or threatened misappropriation. To assert the privilege, one merely has to show that *if disclosure were to occur*, it would likely harm the trade secret holder more than benefit the opposing party.[397] Put another way, privilege law presumes the fact of future disclosure.

The precise type of disclosure—to opposing counsel, to business competitors, or to the public—should matter a great deal to this analysis. Of course, presuming that future disclosure will occur is logical if the disclosure in question is to opposing counsel via a discovery order that the court is about to issue. And in civil proceedings, some courts have clarified precisely this: The test to assert the privilege assesses the risk of harm from disclosure *to the opposing party*, in the controlled context of a judicial proceeding, and subject to any limits that the court may impose, such as a protective order or docket sealing.[398]

But counterintuitively, criminal courts have allowed parties asserting the privilege to claim a likely harm from disclosure *to business competitors* or to the public, even when defense counsel has agreed to a protective order that prohibits use of the information for purposes other than litigating the case.[399] These courts have not required any showing that defense counsel will inevitably, or even likely, violate the protective order. Rather, courts are merely balancing the risk of harm *if* disclosure were to occur.[400] Put differently, courts applying the evidentiary privilege in criminal cases have

[395] *See, e.g.*, 18 U.S.C. § 1836(b)(3)(A)(i).

[396] *See, e.g.*, Flir Sys., Inc. v. Parrish, 95 Cal. Rptr. 3d 307, 312 (Ct. App. 2009) (rejecting a trade secret claim where the "action was premised on the theory that respondents could not mass produce [a product] without [inevitably] misappropriating trade secrets").

[397] *Cf.* Elizabeth A. Rowe, *Striking a Balance: When Should Trade-Secret Law Shield Disclosures to the Government?*, 96 IOWA L. REV. 791, 819-21 (2011) ("The courts will often balance the requesting party's need for the information against the injury that might result *if* disclosure is permitted." (emphasis added)).

[398] *See, e.g.*, Bridgestone/Firestone, Inc. v. Superior Court, 9 Cal. Rptr. 2d 709, 713 (Ct. App. 1992) ("[I]n the balancing process the court must necessarily consider the protection afforded the holder of the privilege *by a protective order* . . . ." (emphasis added)); 1 JAGER, *supra* note 312, § 5:33, at 5-170 ("The relevant inquiry with respect to injury is not with respect to the harm caused by a public disclosure. Rather, the injury must be measured with respect to the disclosure under an appropriate protective order.").

[399] *See, e.g.*, Transcript of Record, *supra* note 49, at 4096, 4111.

[400] *See, e.g.*, People v. Superior Court (*Chubbs*), No. B258569, 2015 WL 139069, at *7 (Cal. Ct. App. 2015) (noting the developer's claim "that disclosure of the source code would enable its competitors to copy the product, causing the company irreparable harm"); Commonwealth v. Foley, 38 A.3d 882, 889 (Pa. Super. Ct. 2012) ("[I]t would not be possible to market TrueAllele if it were available for free.").

presumed that any disclosure—even to opposing counsel—will inevitably result in disclosure to business competitors or to the public at large.

Perhaps, then, the privilege as it has been applied in criminal proceedings is most akin to the "inevitable disclosure" doctrine of substantive trade secret law. The inevitable disclosure doctrine permits injunctions based on circumstantial evidence rather than on direct evidence of actual or threated misappropriation.[401] For example, a company may claim that a departing employee will inevitably rely on its trade secrets while working for a new employer, despite the employee's disavowing any such intent.[402]

Yet even analogized to an inevitable disclosure injunction, the privilege still overprotects because it remains less burdensome to obtain than an injunction. To start, some jurisdictions have been hesitant to recognize the inevitable disclosure doctrine;[403] others have rejected it entirely.[404] And language in the DTSA suggests that the doctrine may not be available under a federal cause of action.[405] Courts that do grant these injunctions still require the trade secret holder to establish that the circumstances of that *particular case* will inevitably lead to misappropriation.[406] In contrast, criminal courts have

[401] *See* PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1269-70 (7th Cir. 1995) (reasoning that the general manager of a PepsiCo subsidiary, who had "extensive and intimate knowledge about [PepsiCo's] strategic goals for 1995 in sports drinks and new age drinks," and who had covertly negotiated a new C-level position for Gatorade, "would necessarily be making decisions about Gatorade . . . by relying on his knowledge of [PepsiCo's] trade secrets").

[402] *See, e.g.*, *id.*

[403] *See, e.g.*, ArchiText, Inc. v. Kikuchi, No. 0500600, 2005 WL 2864244, at *3 (Mass. Super. Ct. May 19, 2005).

[404] *See, e.g.*, Whyte v. Schlage Lock Co., 125 Cal. Rptr. 2d 277, 293 (Ct. App. 2002); LeJeune v. Coin Acceptors, Inc., 849 A.2d 451, 471 (Md. 2004).

[405] *See* 18 U.S.C. § 1836(b)(3)(A)(i) (2016) (restricting courts' power to issue injunctions that "prevent a person from entering into an employment relationship" and requiring that any restrictions on employment "shall be based on evidence of threatened misappropriation and not merely on the information the person knows"). *But see* Molon Motor & Coil Corp. v. Nidec Motor Corp., No. 16 C 03545, 2017 WL 1954531, at *5-6 (N.D. Ill. May 11, 2017) (denying the defendant's motion to dismiss even though the plaintiff had pleaded circumstantial facts supporting an inference of inevitable disclosure, but no more, in a misappropriation claim brought under both Illinois state law and the DTSA).

[406] Inevitable disclosure claims are highly fact-specific and often involve some additional wrongful act by the defendant. In *PepsiCo*, for instance, the defendant's "lack of forthrightness on some occasions, and out and out lies on others, in the period between the time he accepted the position with [Gatorade] and when he informed plaintiff that he had accepted that position" contributed to the court's conclusion that he could not be trusted not to rely on PepsiCo's trade secrets in his new position. *See* 54 F.3d at 1270-71 (quoting the district court's opinion).

upheld the evidentiary privilege without any showing that a particular defense attorney is especially incapable of complying with a protective order.[407]

One might argue that comparing the privilege to substantive trade secret law is misguided because the privilege is itself a branch of the substantive law.[408] After all, trade secret law's numerous common law and statutory sources leave its precise boundaries diffuse. But even from an internal perspective, the privilege goes beyond the furthest reaches of alternative branches of trade secret law, affording greater protection than even the inevitable disclosure doctrine. External or internal, the privilege grants trade secrets "protection plus."

2. The purposes of trade secret law

Trade secret law has several purposes, which may be described broadly as "[t]he maintenance of standards of commercial ethics and the encouragement of invention."[409] The law exists somewhere between a regime of total secrecy and one of no secrecy. Despite its name, one stated objective of trade secret law is to facilitate controlled information sharing.[410] After all, truly secret information needs no legal protection but can be costly to keep secret.[411] Trade secret law alleviates overinvestment in alternative forms of secrecy protections. It also enables innovators to offer ideas for sale, or to share information with employees, without destroying the value of that information in the process.[412] Since its common law origins, trade secret law has also protected information

[407] *See, e.g.*, Transcript of Record, *supra* note 49, at 4096, 4111; *cf.* Brown Bag Software v. Symantec Corp., 960 F.2d 1465, 1469, 1471 (9th Cir. 1992) (largely limiting an "attorneys' eyes only" disclosure of trade secrets to an outside consultant because keeping the information confidential would conflict with in-house counsel's other duties for the competitor-employer).

[408] Thank you to Tejas Narechania for articulating this counterargument.

[409] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481 (1974).

[410] *See, e.g.*, *id.* at 486 (predicting that without legal protection for trade secrets, developers would invest in expensive self-help measures to protect valuable information, causing research to fragment and licensing markets to shrivel); Lemley, *supra* note 201, at 332-37 (arguing that "[p]aradoxically, . . . trade secret law actually encourages broader disclosure and use of information" because it substitutes for physical secrecy that would otherwise restrict the flow of information within innovation teams and because it facilitates disclosures in precontractual negotiations).

[411] For example, without the trade secret legal protection afforded in *E.I. duPont deNemours & Co. v. Christopher*, 431 F.2d 1012 (5th Cir. 1970), DuPont would have had to build a physical roof over an unfinished facility to protect its secrets from aerial surveillance by competitors. *See id.* at 1016. Similarly, the Seventh Circuit in *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.* noted that excess secrecy protections can inhibit workflow within a firm. *See* 925 F.2d 174, 180 (7th Cir. 1991) ("[P]erfect security is not optimum security.").

[412] *See, e.g.*, Lemley, *supra* note 201, at 334-36.

that is disclosed to government officials,[413] whether the disclosure is compelled[414] or undertaken voluntarily—for example, to obtain regulatory approval.[415] As the D.C. Circuit put it, legal protection for trade secrets helps to ensure the "continued reliability" of disclosures compelled by the government and the "continued availability" of those that are volunteered.[416]

The fact that trade secret law aims, at least in part, to facilitate information sharing for purposes of negotiation, employment, and regulation suggests that the law should also perform this function in criminal proceedings. Revealing trade secrets under duties of confidentiality in business or regulatory contexts is arguably analogous to revealing them under a protective order in a criminal proceeding.[417] And because entrance to any market is conditioned on regulatory disclosures,[418] entrance to the criminal justice market could be deemed a waiver of the privilege to completely withhold trade secret evidence from judicial proceedings.[419]

[413] *See, e.g.*, Cincinnati Bell Foundry Co. v. Dodds, 10 Ohio Dec. Reprint 154, 157 (Super. Ct. Cincinnati 1887) ("A secret of trade or manufacture does not lose its character . . . even if . . . the process is liable to be inspected by the assessor of internal revenue or other public officer."). Government officials who leak trade secrets are subject to fines and criminal penalties. *See, e.g.*, 18 U.S.C. § 1905 (2016).

[414] *See* Rowe, *supra* note 397, at 802-03 (noting that absent a statutory guarantee of confidentiality, trade secret holders might seek protective orders when responding to administrative subpoenas).

[415] *Compare* 7 U.S.C. § 136a(a), (c) (2016) (requiring disclosure of the formula for pesticides as a condition of lawful distribution), *with* 5 U.S.C. § 552(b)(4) (2016) (exempting trade secrets from Freedom of Information Act requests).

[416] *See* Critical Mass Energy Project v. Nuclear Regulatory Comm'n, 975 F.2d 871, 878 (D.C. Cir. 1992) (en banc).

[417] For instance, at a high level of abstraction, trade secret disclosures that facilitate business or regulation and those that facilitate cross-examination share similar goals of advancing knowledge. *Compare* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 493 (1974) (explaining that a goal of trade secret law is "technological and scientific advancement"), *with* Lilly v. Virginia, 527 U.S. 116, 124 (1999) (plurality opinion) (describing cross-examination as the "greatest legal engine ever invented for the discovery of truth" (quoting California v. Green, 399 U.S. 149, 158 (1970))). Granted, this is not a perfect analogy: Industry negotiations involve voluntary disclosures that risk theft by competitors, whereas criminal subpoenas facilitate involuntary adversarial scrutiny that risks leaks by noncompetitors and are thus perhaps more directly analogous to administrative subpoenas.

[418] For a snapshot of the types of regulatory agencies that compel disclosures of trade secrets, see *FOIA Guide, 2004 Edition: Exemption 4*, U.S. DEP'T JUST., https://perma.cc/89NL-Q7EA (last updated July 23, 2014) (listing cases litigating public records requests to those agencies).

[419] *Cf., e.g.*, Amicus Curiae Brief of Electronic Frontier Foundation in Support of Defendant and Appellant Billy Ray Johnson at 19, People v. Johnson, No. F071640 (Cal. Ct. App. Sept. 13, 2017) (making a similar argument).

Of course, there is a risk of leaks.[420] A defendant's expert witness might be or become a business competitor of the trade secret holder.[421] And noncompetitors could be uniquely disposed to destroy trade secrets by releasing them to the public.[422] But those risks are hardly anathema to trade secret policy. Compared to patents, which offer limited-duration monopolies for the quid pro quo of public disclosure, trade secret law is designed to leak.[423] The relative weakness of trade secret law—that it offers no protection against *proper* use or acquisition—helps to balance rights to exclude with competing interests in knowledge dissemination that aids downstream innovators.[424] The U.S. Supreme Court has even recognized that the "substantial risk" of undetectable *theft* of trade secrets may be socially useful in that it encourages innovators to seek patents, which require disclosure.[425]

Routine disclosures under protective orders in the controlled context of criminal proceedings would arguably pose a lesser risk of leaks than occurs in standard trade secrets cases. Granted, the quantity of disclosures in criminal proceedings would be higher; this seems likely to increase the probability of leaks. Nonetheless, that same quantity of disclosures could also make trade secret theft easier to detect and thus deter, as repeat players could identify stolen information in subsequent cases; while it might be difficult to pinpoint

[420] In civil cases, protective orders for source code have been violated. *See, e.g.*, Bradford Techs., Inc. v. NCV Software.com, No. C 11-04621 EDL, 2013 WL 75772, at *3 (N.D. Cal. Jan. 4, 2013) (involving counsel who provided disclosed source code to his client, in violation of the terms of the protective order); MobileMedia Ideas LLC v. Apple Inc., No. 10-258-SLR/MPT, 2012 WL 5379056, at *2 (D. Del. Oct. 31, 2012) (involving a nontestifying consultant who printed copies of disclosed source code), *recommendation adopted by* 2013 WL 5314709 (D. Del. Sept. 16, 2013).

[421] For instance, in a murder trial in New York, two competitor developers of forensic DNA analysis software both analyzed the defendant's DNA sample. *See* PCAST Report Addendum, *supra* note 148, at 8.

[422] *See, e.g.*, Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1368 (E.D. Va. 1995) (holding that documents that had been posted to the internet had become part of the public domain and were no longer trade secrets); *see also* Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 782 (2007) ("Revealing secrets to the public would not only thwart the misappropriator's intent to free-ride on the secret; it would also facilitate detection . . . ."); *cf.* DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 195 (Ct. App. 2004) ("[A] competitor who has misappropriated the plaintiff's business secret for profit . . . has as much interest as the plaintiff has in keeping the secret . . . .").

[423] *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 490 (1974) ("Where patent law acts as a barrier, trade secret law functions relatively as a sieve."). It is this leakiness that saves trade secret law from preemption by the federal "patent policy of disclosure." *See id.* at 489-92.

[424] *See, e.g.*, David D. Friedman et al., *Some Economics of Trade Secret Law*, 5 J. ECON. PERSP. 61, 67, 70 (1991) (arguing that the lack of legal protection against reverse engineering and accidental loss may lead to follow-on innovation).

[425] *See Kewanee Oil*, 416 U.S. at 490.

the precise source of a leak, repeat expert witnesses could catch subsequent uses of a stolen trade secret when evaluating the misappropriator's product.[426] Breach of a protective order would also be subject not merely to standard liability for misappropriation but also to criminal contempt of court.[427] Perhaps for that reason, trade secrets have existed comfortably alongside protective orders for years in high-risk civil litigation, such as in patent lawsuits where disclosures are made to direct competitors who have already allegedly infringed intellectual property rights.[428]

Further, trade secret law has room for public policy exceptions.[429] For instance, in 2016 Congress chose to immunize whistleblowers who divulge trade secrets "in confidence to a . . . government official . . . or to an attorney . . . solely for the purpose of reporting or investigating a suspected violation of law."[430] While the clear legislative intent of that provision of the DTSA was to promote law enforcement investigations of corporate fraud,[431] there is a plausible textual argument that the law actually authorizes the disclosure of trade secrets to criminal defense attorneys to assist their investigations into the alleged crimes their clients are charged with committing. The statutory text imposes no constraints on the type of attorney to whom a trade secret may be disclosed, and it makes no distinction between corporate fraud and any other "suspected violation of law" or between investigations conducted by the government and those conducted by the defense.

More broadly, the DTSA exception shows that trade secret protections may be relaxed to benefit the criminal justice system. Trade secret law has produced mechanisms to facilitate limited information disclosures. If industry and regulators may enjoy trade secret-enhanced information sharing, then those defending life or liberty should too. Put differently, trade secret policy

[426] Thank you to Mark Lemley for sharing this argument.

[427] *See, e.g.*, 18 U.S.C. § 401 (2016) (giving a federal court the "power to punish by fine or imprisonment, or both, . . . [d]isobedience or resistance to its lawful . . . order").

[428] *See supra* notes 373-77 and accompanying text.

[429] *See, e.g.*, Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 CALIF. L. REV. 1, 30-31, 54-55 (2017) (observing that judicially created public policy exceptions to trade secret protections are present but "murky" and proposing a safe harbor for whistleblowers who disclose trade secrets to trusted intermediaries for law enforcement purposes); Samuelson, *supra* note 422, at 787-88 (describing public policy limits on trade secret protections, including where information "is relevant to public health or safety" (quoting RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c, at 457 (AM. LAW INST. 1995))). As discussed below, Menell's proposal to offer safe harbor for whistleblowers was passed into federal trade secret law.

[430] *See* Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, § 7(a)(3), 130 Stat. 376, 384 (codified at 18 U.S.C. § 1833(b)).

[431] *See* Peter S. Menell, *Misconstruing Whistleblower Immunity Under the Defend Trade Secrets Act*, 1 NEV. L.J.F. 92, 96 (2017).

not only fails to justify withholding information from the accused; it actually encourages its disclosure.

3. Innovation concerns

Recent case law reflects a concern that developers will not make or sell technologies for criminal justice use unless they are assured that their trade secrets will receive privilege protections. One developer has submitted affidavits in criminal courts across the country stating that complying with defendants' subpoenas for trade secret source code could "cause irreparable harm to the company, as other companies would be able to copy the code and potentially put him out of business."[432] Prosecutors have claimed that compelled disclosures would "threaten[] the very existence of the software and the company."[433] One judge refused to grant a defense subpoena out of concern that a developer might "decline to act as a [state] expert."[434] Another worried that "it would not be possible to market [the proprietary software] if it were available for free."[435]

Those are troubling predictions. We need accurate, reliable, neutral tools to protect the safety of our communities, identify the true perpetrators of crimes, exonerate the wrongly accused, and achieve just outcomes for guilty defendants.[436] The need for innovation is particularly urgent in the forensic sciences. Unvalidated and unreliable forensic evidence is undermining criminal trials.[437] In 2009, a National Academy of Sciences report identified a "notable 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.[438] More recent

[432] *See, e.g.*, Commonwealth v. Robinson, No. CC 201307777, slip op. at 2 (Pa. Ct. C.P. Allegheny Cty. Feb. 4, 2016) (describing the declaration); *see also* Affidavit of Mark W. Perlin ¶ 11, State v. Shaw, No. CR-13-575691 (Ohio Ct. C.P. Cuyahoga Cty. June 19, 2014) ("Such disclosure is . . . financially devastating."); Declaration of Mark W. Perlin, *supra* note 142, ¶ 74 ("Disclosure of the TrueAllele source code trade secret would cause irreparable harm to the company, enabling competitors to easily copy the company's proprietary products and services."); Second Declaration of Mark W. Perlin in Response to Defense Motion to Compel ¶ 91, State v. Fair, No. 10-1-09274-5 SEA (Wash. Super. Ct. King Cty. Apr. 3, 2016) ("[R]eview of source code would enable the reverse engineering of the TrueAllele technology, allowing others to learn the trade secrets that keep Cybergenetics solvent.").

[433] *See, e.g.*, *Shaw* Motion to Quash, *supra* note 80, at 9.

[434] *See Robinson*, No. CC 201307777, slip op. at 2-3.

[435] *See* Commonwealth v. Foley, 38 A.3d 882, 889 (Pa. Super. Ct. 2012).

[436] *Cf.* Obama, *supra* note 388, at 812 (asserting that "[h]ow we treat citizens who make mistakes (even serious mistakes)" characterizes who we are as a society).

[437] *See, e.g.*, PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 8, at x.

[438] *See* NAT'L RESEARCH COUNCIL, *supra* note 349, at 8, 142, 154, 163.

studies have questioned the scientific foundations of bite mark, arson, hair and fiber, ballistic, blood spatter, shaken baby syndrome, and even DNA and fingerprint analysis.[439] In September 2016, the Obama Administration's President's Council of Advisors on Science and Technology published a report finding a "need to evaluate specific forensic methods to determine whether they have been scientifically established to be valid and reliable."[440]

Indeed, as this Article has shown, secrecy around forensic methods is the status quo[441]—and may well have contributed to the current state of affairs. There is no evidence that requiring limited trade secret disclosures under protective orders in criminal proceedings or parole hearings would in fact deter innovation. Such disclosures might do the opposite by encouraging the development of better-quality tools and methods that can withstand adversarial scrutiny and by enabling rigorous cross-examination to serve as a check on government procurement decisions in the criminal justice market.

What is more, trade secret law is not the only way to encourage innovation in criminal justice technologies. In fact, the current market includes companies with relatively transparent business strategies. ESR, which claims a 54% U.S. market share in probabilistic DNA analysis tools,[442] has a voluntary policy to disclose trade secret source code to criminal defendants subject to several requirements, including that defendants sign a confidentiality agreement.[443] Predictive policing companies CivicScape and Azavea have embraced public transparency, relying on open-source algorithms, publishing their source code and input variables, and sharing information about their data and models with independent auditors.[444] As Ram has argued in depth,

[439] *See, e.g.,* Alex Kozinski, Preface, *Criminal Law 2.0*, 44 GEO. L.J. ANN. REV. CRIM. PROC., at iii, iii-v (2015); Radley Balko, Opinion, *Seventh Circuit Grants Immunity to Bite Mark "Experts" Who Put Innocent Man in Prison for 23 Years*, WASH. POST (Sept. 8, 2015), https://perma.cc/9JY2-ZDVL; Debbie Cenziper, *Prosecutors Build Murder Cases on Disputed Shaken Baby Syndrome Diagnosis*, WASH. POST (Mar. 20, 2015), https://perma.cc/96GF-MQSQ.

[440] PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., *supra* note 8, at x.

[441] *See supra* notes 267-77 and accompanying text.

[442] *See* Wexler, *supra* note 12. ESR, one of New Zealand's Crown Research Institutes, owns STRmix. *See STRmix*, ESR, https://perma.cc/KHU4-KJVV (archived Apr. 11, 2018).

[443] *See* ESR, Access to STRmix Software by Defence Legal Teams 1-2 (2016), https://perma.cc/FA45-LY6U.

[444] On April 3, 2017, predictive policing company CivicScape published its source code on GitHub with the explanation: "By making our code and data open-source, we are inviting feedback and conversation about CivicScape in the belief that many eyes make our tools better for all." CivicScape, *Preventing and Diagnosing Bias in CivicScape*, GITHUB (Apr. 3, 2017), https://perma.cc/2WBK-CZN9; *see also Resources*, HUNCHLAB, https://perma.cc/YN3A-VLXN (archived Apr. 11, 2018) ("We consistently share HunchLab's inner-workings with police departments, journalists, and activists."). *footnote continued on next page*

alternative policies could promote innovation of new criminal justice technologies without reliance on trade secrecy.[445] Options could include patents for innovations that qualify as patentable subject matter;[446] prize competitions;[447] government grants;[448] regulatory exclusivities, in which transparency could be a condition of a "sole source contract" with a government procurement office;[449] and potential disclosure-facilitating amendments to tax incentives.[450] While each model has its limits, the models could be combined to provide a robust array of rewards for innovation in criminal justice technology.[451]

Compelled disclosure subject to a protective order is thus hardly guaranteed to produce the adverse results for innovation some developers have claimed. Ambiguous evidence about the effects on innovation is an unconvincing rationale for denying criminal defendants access to relevant evidence, particularly in light of the protections that trade secret holders still enjoy when disclosures are made under a protective order.

In sum, as compared to substantive trade secret doctrine, the trade secret evidentiary privilege overprotects intellectual property and contradicts the disclosure-prompting purpose of trade secret law, and even the broader goal of encouraging innovation fails to justify a total withholding remedy under the privilege.

HunchLab is owned by Azavea. *See* HunchLab: Under the Hood, at i (2015), https://perma.cc/7546-33UQ.

[445] *See* Ram, *supra* note 25, at 701 ("[A] court's decision to require disclosure sufficient to enable vigorous inspection, testing, and validation need not leave innovators without sufficient rewards for their work.").

[446] *See, e.g.*, *id.* at 701-04.

[447] *See, e.g.*, *id.* at 704-07; *see also* Camilla A. Hrdy, *Commercialization Awards*, 2015 WIS. L. REV. 13, 72-81 (comparing the commercialization incentives of patent models against those of government awards).

[448] *See, e.g.*, Ram, *supra* note 25, at 707-10.

[449] *See, e.g.*, *id.* at 710-12 (citing Letter from Mark W. Perlin, Chief Sci. & Exec. Officer, Cybergenetics, to Jerry D. Varnell, Contract Specialist, U.S. Dep't of Justice 1 (Apr. 1, 2015), https://perma.cc/7ML3-EJMQ).

[450] *See, e.g.*, *id.* at 712-13.

[451] *See id.* at 715-17 (advocating for innovation incentives that promote early and broad public disclosures for criminal justice technologies and noting that various innovation incentives may be combined). Ram also notes that the developer of TrueAllele has benefited from multiple government grants. *See id.* at 716. Cybergenetics, which owns TrueAllele, also has multiple patents. *See Patents*, CYBERGENETICS, https://perma.cc/8GF7-GFEA (archived Apr. 11, 2018).

D. The Scope and Purpose of Privilege Law

Of course, concluding that the privilege overprotects intellectual property, or contradicts the theoretical goals of trade secret protection, does not necessarily mean that it is unlawful, even in criminal cases. This Subpart therefore examines whether courts lack the power to recognize a criminal trade secret privilege. It first notes the absence of binding authority requiring courts to recognize a privilege in criminal cases or to provide privilege claimants with a total withholding entitlement. That absence, combined with the requirement that courts construe privileges narrowly, may prohibit judges from extending the privilege into criminal proceedings. And even if courts are not barred from recognizing a criminal trade secret privilege, doing so would fail to serve the purpose of privilege law: to balance truth-seeking in adjudication against competing societal interests that are extrinsic to the courts.

1. Judicial authority and a criminal trade secret privilege

The vast majority of courts today retain discretion to cabin the trade secret privilege to civil proceedings alone. I have found no appellate rulings either upholding or striking down the privilege in a criminal proceeding, with an unpublished decision of a California appeals court as the sole exception.[452] In jurisdictions where the privilege remains a creature of common law, such as New York,[453] and with respect to federal claims,[454] no binding authority currently requires courts to recognize a trade secret privilege in criminal cases. Even in statutory jurisdictions it is often unclear whether and to what extent the privilege must apply in criminal proceedings. The texts of trade secret privilege statutes generally include an escape hatch stating that the privilege may apply only if its allowance "will not tend to conceal fraud or otherwise

[452] *See* People v. Superior Court (*Chubbs*), No. B258569, 2015 WL 139069, at *5-9 (Cal. Ct. App. 2015). *Chubbs* is unpublished and thus technically nonbinding, *see supra* note 71, although trial courts throughout California are likely to follow its ruling because decisions of California's Courts of Appeal generally carry great force in trial courts across the state, *see* Auto Equity Sales, Inc. v. Superior Court, 369 P.2d 937, 940 (Cal. 1962). For a description of my search technique for criminal appellate rulings on a trade secret evidentiary privilege, see note 286 above.

[453] *See, e.g.*, 5 ROBERT A. BARKER & VINCENT C. ALEXANDER, EVIDENCE IN NEW YORK STATE AND FEDERAL COURTS § 5:57, at 431 & n.1 (2d ed. 2011). *But see* N.Y. STATE BAR ASS'N, EVIDENTIARY PRIVILEGES: GRAND JURY, CRIMINAL AND CIVIL TRIALS, at vii-xii (6th ed. 2015) (omitting any mention of a trade secret privilege).

[454] *See* FED. R. EVID. 501 ("The common law . . . governs a claim of privilege unless . . . the United States Constitution[,] a federal statute[,] or rules prescribed by the Supreme Court [provide otherwise].").

work injustice."[455] Courts could conceivably construe a phrase like "otherwise work injustice" to prohibit recognition of the privilege in criminal proceedings. In the alternative, that phrase could be construed to limit the privilege to affording the trade secret holder remedies like protective orders, sealing orders, or exclusion of the public from certain proceedings—not a total withholding entitlement.[456]

Because most courts are not currently required to extend the privilege wholesale from civil to criminal cases, they may also be barred from doing so. The U.S. Supreme Court has repeatedly asserted that "evidentiary privileges must be construed narrowly because privileges impede the search for the truth."[457] At least one state has codified this rule in terms of statutory construction: California's Law Revision Commission has explained that "privileges are not recognized in the absence of statute" and that privilege statutes "preclude[] the courts from elaborating upon the statutory scheme."[458] The push in several jurisdictions to narrow construction of evidentiary privileges, combined with the dearth of binding authority requiring a criminal trade secret privilege, supports a credible claim that today's courts lack the authority to recognize the privilege in criminal proceedings.

[455] *See, e.g.*, ALASKA R. EVID. 508; CAL. EVID. CODE § 1060 (West 2018); N.J. STAT. ANN. § 2A:84A-26 (West 2018); *see also* FLA. STAT. § 90.506 (2017) (similar language); TEX. R. EVID. 507(a) (similar language).

[456] For instance, this type of limit is arguably what the 1990 amendments to California's statutory privilege sought to accomplish. California's original statutory privilege from 1965 had granted a withholding entitlement and had not mentioned criminal proceedings. *See* Act of May 18, 1965, ch. 299, 1965 Cal. Stat. 1297, 1335 (codified at CAL. EVID. CODE § 1060). The 1990 amendments added specific procedures for asserting the privilege in criminal proceedings. *See* Act of Sept. 10, 1990, ch. 714, 1990 Cal. Stat. 3316, 3319-20 (codified as amended at CAL. EVID. CODE §§ 1061-1063); Act of June 18, 1990, ch. 149, 1990 Cal. Stat. 1215 (codified as amended at CAL. EVID. CODE §§ 1061-1062). Those procedures entitle trade secret holders to protective orders limiting the scope of disclosure, such as to counsel alone, *see* CAL. EVID. CODE § 1061(b)(4)(A); to restrictions on filing the trade secret information in the public court record, *see id.* § 1061(b)(4)(D); and to exclusion of the public from a portion of the proceedings, *see id.* § 1062(a). The amendments do not include a complete withholding remedy, and thus the legislature arguably did not intend that remedy to apply to assertions of the privilege in criminal cases. *Cf. Chubbs*, 2015 WL 139069, at *4 (noting that the trial court held that a total withholding entitlement does "work injustice" (quoting CAL. EVID. CODE § 1060)). For a description of *Chubbs*'s statutory argument, see notes 65-66 and accompanying text above.

[457] *See* Pierce County v. Guillen *ex rel.* Guillen, 537 U.S. 129, 144 (2003); *see also* United States v. Nixon, 418 U.S. 683, 710 (1974) ("Whatever their origins, these exceptions to the demand for every man's evidence are not lightly created nor expansively construed, for they are in derogation of the search for truth.").

[458] *See* CAL. EVID. CODE § 911 law revision commission's comments. Note, however, that the comment also asserts that "courts to a limited extent are permitted to develop the details of declared principles" and cites California's trade secrets provision as an example. *See id.*

2. Sensitive information inside and outside the courts

Even if courts are not barred from extending a trade secret privilege into criminal proceedings, the question remains whether doing so would serve the purpose of privilege law. Evidentiary privileges pit truth-seeking against competing values.[459] Whenever they apply, privileges can exclude relevant evidence.[460] Parties denied access to privileged information may not realize that anything relevant is missing, much less know precisely what was denied.[461] Privilege law trades off these harms in the name of certain intimate relationships, such as those with spouses, psychotherapists, attorneys, or spiritual counselors.[462] Utilitarians justify the tradeoff by arguing that evidentiary privileges, over time if not in individual cases, cause merely a de minimis loss of relevant evidence because, presumably, without the guarantee of privilege protections people would not disclose the information at issue in the first place.[463] Humanists, in contrast, presume that evidentiary privileges do cause significant exclusions of relevant evidence but find those losses justified by competing values such as limiting judicial intrusion into significant relationships of trust and intimacy.[464]

[459] *See, e.g.*, Eileen A. Scallen, *Relational and Informational Privileges and the Case of the Mysterious Mediation Privilege*, 38 LOY. L.A. L. REV. 537, 538 (2004) (noting that privileges are "mixed blessings" created to protect socially important interests and relationships that also exclude "potentially relevant, reliable, and credible evidence").

[460] *See, e.g.*, *Developments in the Law—Privileged Communications*, 98 HARV. L. REV. 1450, 1473 (1985) (noting that the "traditional justification" for privilege law "ignores specific injury to those actually before the court . . . by weighing the benefit of their encouragement of communications within the relevant *class* of relation against the cost of their obstruction to truth-seeking" (footnote omitted)).

[461] Some theorists resist classifying privileges as evidentiary rules because they are designed to serve purposes other than factfinding. *See* Alex Stein, *The New Doctrinalism: Implications for Evidence Theory*, 163 U. PA. L. REV. 2085, 2094 n.47 (2015).

[462] *See, e.g.*, Jaffee v. Redmond, 518 U.S. 1, 9-10 (1996) (recognizing a privilege "protecting confidential communications between a psychotherapist and her patient"); Upjohn Co. v. United States, 449 U.S. 383, 389-90 (1981) (discussing the attorney-client privilege); United States v. Brock, 724 F.3d 817, 820-23 (7th Cir. 2013) (discussing two distinct marital privileges recognized under federal law); Mullen v. United States, 263 F.2d 275, 277-80 (D.C. Cir. 1959) (recognizing a "confessor-confessant" privilege).

[463] *See, e.g.*, Edward J. Imwinkelried, Essay, *The New Wigmore: An Essay on Rethinking the Foundation of Evidentiary Privileges*, 83 B.U. L. REV. 315, 317-18 (2003); *see also* Ronald J. Allen et al., *A Positive Theory of the Attorney-Client Privilege and the Work Product Doctrine*, 19 J. LEGAL STUD. 359, 364 (1990) (arguing that the attorney-client privilege enhances truth-seeking, even while raising costs for opposing parties to discover relevant evidence, because it incentivizes clients to tell their attorneys unfavorable information that is relevant to an honest "contingent" legal claim).

[464] *See* Imwinkelried, *supra* note 463, at 325-40 (discussing privacy and autonomy as bases for a "humanistic theory for communications privileges").

Given the goal of balancing truth-seeking with competing societal values, it does not make sense to grant trade secrets *more* protection within privilege law than they enjoy outside of it. My earlier conclusion that a trade secret evidentiary privilege overprotects intellectual property, then, also suggests that it fails to serve the purpose of privilege law.

To be sure, the trade secret privilege may at first appear as more of an equalizer than an overprotector. After all, trade secret disclosures outside of court are often voluntary, whereas responding to a subpoena or discovery demand is not. This reasoning that privileges simply maintain an existing equilibrium of voluntary information sharing may well apply to a variety of evidentiary privileges. For instance, Eileen Scallen proposes that some privileges for special relationships—such as attorney-client, doctor-patient, or psychotherapist-patient—are simply extensions of fiduciary duties that already exist.[465] Accordingly, these privileges replicate fiduciaries' existing duties not to reveal the information entrusted to them, thereby granting identical protection to sensitive information inside and outside the courts.

Yet the trade secret privilege is distinguishable from Scallen's fiduciary extension theory. While trade secret disclosures outside the judicial context are often voluntary, society also encourages and compels involuntary disclosures and appropriations of trade secrets, such as regulatory disclosures and reverse engineering.[466] Therefore, granting a privilege to entirely withhold trade secret evidence affords the information more protection within privilege law than society grants it elsewhere. The trade secret privilege does not serve privilege law's purpose of balancing truth-seeking in adjudication against competing societal values extrinsic to courts.

3. Differential incentives

Differences in the government's and criminal defendants' incentives to scrutinize the methodologies behind criminal justice technologies further strengthen the policy argument against a criminal trade secret privilege. The issue may be explained by reference to Amar's structural theory of criminal procedure and Murphy's institutional analysis of scientific evidence. Amar proposes a theory of "compulsion parity," under which evidentiary privileges are permissible as long as they are symmetrical—that is, as long as they require the government and criminal defendants both to relinquish access to relevant

[465] *See* Scallen, *supra* note 459, at 571-72 ("These privileges merely minimize some of the consequences of breach of fiduciary duty by refusing to allow the disloyal fiduciary to compound the betrayal by testifying in court. . . . Seeing the fiduciary quality of relational interests helps to explain why only one party holds certain privileges instead of both parties.").

[466] *See supra* notes 413-16, 424-25 and accompanying text.

evidence.[467] According to this theory, the government's "self-denial" in recognizing a privilege will help to ensure that the privilege is truly justified by a "'compelling interest' against compulsion."[468] Amar's model of government self-restraint works beautifully if, over time, privileges impose balanced handicaps on government and defense investigations.[469] But the model will falter if the government's incentives to seek out certain types of information are systematically lower than those of criminal defendants. If, for instance, a particular category of evidence is likely to weaken the government's case, then privileging that type of information is hardly self-denial.

Murphy's writing shows that investigative and forensic tools and methods embody precisely such a differential incentives scenario.[470] An agency that implements these tools and methods has already deemed them valid and reliable according to whatever procurement standards apply and will have weak incentives to identify information that could prove otherwise.[471] In sharp contrast, individuals who become the targets of these tools and methods will have had no prior opportunity to evaluate them and will be highly motivated to scrutinize them for any fault.[472] Symmetrical constraints on prosecutors' and defendants' access to information about investigative and forensic technologies will therefore systematically aid the government and harm the accused.

Reading Amar's and Murphy's works together, then, gives rise to a "differential incentives" theory of privileges for criminal cases. When the government's interests in scrutinizing certain categories of information are either greater than or equal to those of the accused, privileges are more likely to be justified. But when the government's interests in accessing a particular kind of information are systematically lesser than those of criminal defendants,

[467] *See* Akhil Reed Amar, Foreword, *Sixth Amendment First Principles*, 84 GEO. L.J. 641, 699 (1996).

[468] *See id.*

[469] This may well be the case for what Amar calls the "true privacy privileges," meaning privileges for intimate relationships such as those between spouses. *See id.* at 704. For example, a defendant might want to provide evidence that a third party is guilty of the crime and seek to compel the third party's spouse to testify against him. The government might at other times seek to compel a defendant's spouse to testify.

[470] *See* Murphy, *supra* note 25, at 747-48 (observing that "there is generally no centralized market to drive the development of institutional 'defense-side' forensic testing or research facilities" and that "[f]orensic scientists often feel the pressure to produce results that will please their central and even sole client, the government, and to shield their processes from the defense or even the public domain").

[471] *See id.* at 746 (noting that as long as police and prosecutors are satisfied with the results of forensic methods, "laboratories need not engage in any new development or self-criticism").

[472] For examples of individual defendants who proved highly motivated to challenge—and effective at challenging—criminal justice technologies, consider the cases of Daniel Rigmaiden and Glenn Rodríguez, both discussed in Wexler, *supra* note 12.

privileges are more likely to be unjustified. Trade secrets in criminal justice technologies fit within the latter scenario.

Conclusion

This Article has made the case against recognizing a trade secret privilege in criminal cases. The application of the privilege in criminal contexts is a relatively recent development and is not generally required by controlling authority. In addition to being discretionary, extending the privilege wholesale from civil to criminal proceedings is both harmful and unnecessary.

A criminal trade secret privilege would almost certainly lead to overclaiming, abuse, and the exclusion of highly probative evidence; it would also project a message that the government values intellectual property holders more than those whose life or liberty is at stake. These harms are unnecessary because narrow criminal discovery and subpoena powers combined with protective orders should suffice to safeguard the interests of trade secret owners to the full extent reasonable. Illustrating the sufficiency of those safeguards, after a draft of this Article was posted to SSRN in February 2017, the developer of the software program at issue in *Chubbs* began voluntarily offering limited access to the program's source code, under protective orders, to criminal defendants' expert witnesses.[473]

What is more, compared to substantive trade secret law, the privilege overprotects intellectual property and fails to serve the purposes of either trade secret law or of privilege law. Withholding information from the accused because it is a trade secret mischaracterizes defense advocacy as a business competition.

More broadly, this Article raises the issue of how evidence rules function differently in civil and criminal cases. At common law, some commentators considered criminal evidence to be a distinct area of law.[474] 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.[475] Yet vast procedural differences—as in the scope of civil and criminal discovery—mean that information inputs for each type of case diverge. When the underlying rules of procedure vary, applying formally consistent evidence rules will produce disparate results. To achieve consistent results across civil and criminal law, the rules of evidence must be tailored according to the procedural backdrop.

[473] Email from Mark W. Perlin to author (Mar. 7, 2018) (on file with author) (asserting that as of July 2017, "Cybergenetics provides defense access to source code under confidentiality agreement[s]").

[474] *See* JOHN H. LANGBEIN, THE ORIGINS OF ADVERSARY CRIMINAL TRIAL 178 (2003); *see also* Sklansky & Yeazell, *supra* note 338, at 728 n.176, 729 (describing debates in the late nineteenth and early twentieth centuries as to whether "criminal evidence" was a distinct body of law).

[475] *See* Sklansky & Yeazell, *supra* note 338, at 729.