Printed in U.S.A.
Vol. 112, No. 4

INNOVATING CRIMINAL JUSTICE

Natalie Ram

ABSTRACT—From secret stingray devices that can pinpoint a suspect's location, to advanced forensic DNA-analysis tools, to recidivism risk statistic software—the use of privately developed criminal justice technologies is growing. So too is a concomitant pattern of trade secret assertion surrounding these technologies. This Article charts the role of private law secrecy in shielding criminal justice activities, demonstrating that such secrecy is pervasive, problematic, and ultimately unnecessary for the production of well-designed criminal justice tools.

This Article makes three contributions to the existing literature. First, the Article establishes that trade secrecy now permeates American criminal justice, shielding privately developed criminal justice technologies from vigorous cross-examination and review. Second, the Article argues that private law secrecy surrounding the inner workings—or even the existence—of these criminal justice technologies imposes potentially unconstitutional harms on individual defendants and significant practical harms on both the criminal justice system and the development of well-designed criminal justice technology. Third, the Article brings the extensive literature on innovation policy to bear on the production of privately developed criminal justice technologies, demonstrating that trade secrecy is not essential to either the existence or operation of those technologies. The Article proposes alternative innovation policies that the government, as both a funder of research and the primary purchaser of criminal justice technologies, is uniquely well-positioned to implement.

AUTHOR—Assistant Professor, University of Baltimore School of Law; J.D., Yale Law School; A.B., Princeton University. Many thanks to Stephanie Bair, Jack Balkin, Teneille Brown, Jenny E. Carroll, Alta Charo, Glenn Cohen, Robert Cook Deegan, Gregory Dolin, Michele Gilman, Hank Greely, Yaniv Heled, William Hubbard, David Jaros, Max Mehlman, Lisa Ouellette, W. Nicholson Price II, Sonja Ralston, Richard Re, John A. Robertson, Rachel Sachs, Jake Sherkow, and Chris Slobogin for their helpful comments on this project. This work also benefitted from feedback at the BioLaw Conference at Stanford Law School, the Health Law Professors' Conference at Georgia State University, the Wiet Life Science Law Scholars Conference at Loyola University Chicago School of Law,

and the Junior Faculty Workshop at the University of Maryland. Finally, thank you to the editors of the *Northwestern University Law Review* for their excellent work. All errors are my own.

INTRODUCTION

In 2015, Billy Ray Johnson was sentenced to life imprisonment without parole for a series of sexual assaults and burglaries that he says he did not commit.[1] The primary evidence in the case consisted of traces of DNA found on items from three crime scenes, including a phone, clothing, and a zip tie investigators believed had been used to bind one of the victims.[2] In order to link Johnson to the crime-scene DNA, investigators relied on TrueAllele, a privately developed and privately owned software

[1] *See* Rebecca Wexler, *When a Computer Program Keeps You in Jail*, N.Y. TIMES (June 13, 2017), https://www.nytimes.com/2017/06/13/opinion/how-computers-are-harming-criminal-justice.html [https://perma.cc/AL5T-3G6D]. There are at least two significant cases involving probabilistic genotyping software in which the defendant's last name is Johnson. Accordingly, this Article will refer to the case involving Billy Ray Johnson as the "*Billy Ray Johnson* case" for clarity.

[2] *See* CYBERGENETICS, PEOPLE OF CALIFORNIA V BILLY RAY JOHNSON, https://www.cybgen.com/news/cases/California-v-Billy-Ray-Johnson.shtml [https://perma.cc/NS4N-L4CJ] (last visited Oct. 25, 2017) (describing the Billy Ray Johnson case and TrueAllele's role in it).

program for analyzing DNA mixtures that typical DNA analysis cannot resolve.[3] Yet when an expert witness for Johnson sought to examine TrueAllele's source code, she was rebuffed.[4] TrueAllele's source code, its creator Mark Perlin steadfastly maintained, is a trade secret.[5] Perlin refused to make that code available for review even when Johnson's attorney offered to sign a protective order.[6] The judge in the case, meanwhile, refused to order that the source code be disclosed—but did admit the DNA analysis that TrueAllele generated into evidence.[7] None of the investigators, prosecutors, defense attorneys, or even the judge in Johnson's case were permitted access to the source code of the crucial software. Indeed, to date, no one outside of Cybergenetics—Perlin's company—has seen or examined that source code.[8] Yet, largely based on the DNA analysis that TrueAllele generated, Johnson was convicted.[9]

Billy Ray Johnson's case is not the only recent example of the criminal justice system relying on privately developed tools shielded by assertions of trade secret protection.[10] The use of trade secrets to inhibit

---

[3] Wexler, *supra* note 1; CYBERGENETICS, *supra* note 2 (observing that "[d]ue to the complexity of these low-level 3 and 4 person mixtures, human review of the data was largely inconclusive," but that TrueAllele "yielded match statistics from 33 mixture items. 8 of these items linked Johnson to the 3 crimes").

[4] Wexler, *supra* note 1.

[5] *Id.*

[6] *Id.*

[7] *See* Respondent's Brief at 73, People v. Johnson, No. F071640 (Cal. Ct. App. Aug. 7, 2017) (quoting the trial court's motion to review TrueAllele's source code and explaining that "[t]he source code is a trade secret. I don't think adequate showing has been made to justify the breech [sic] of that privilege"); *id.* at 74 (recounting that the trial court admitted TrueAllele's analysis at trial over defense objections).

[8] *See* ERIN E. MURPHY, INSIDE THE CELL: THE DARK SIDE OF FORENSIC DNA 101 (2015); Robert Gavin, *Cybergenetics True Allele Casework DNA Study is Winner in Cold Case Murder Conviction*, TIMES UNION (Mar. 31, 2015), http://www.timesunion.com/tuplus-local/article/Cybergenetics-True-Allele-Casework-DNA-study-is-6171690.php [https://perma.cc/XU89-YQUL] ("Only [Perlin] and one of his colleagues know the 'source code' behind [TrueAllele]."). Access to a machine on which a particular software program is installed is not access to that software's source code. The code that is installed and runs on a particular machine is object code—a series of 1s and 0s that even few programmers can read and translate. *See* Edward J. Imwinkelried, *Computer Source Code: A Source of the Growing Controversy Over the Reliability of Automated Forensic Techniques*, 66 DEPAUL L. REV. 97, 104 (2016). Source code, by contrast, is programming written in a language that other programmers familiar with that programming language can read, write, and understand. *Id.* at 103–04. Once complete, source code is "compiled"—translated—into object code. *Id.* at 104.

[9] *See* Wexler, *supra* note 1; ABC News, *East Bakersfield Residents React to the Conviction of Billy Ray Johnson*, YOUTUBE.COM (Apr. 22, 2015), https://www.youtube.com/watch?v=xoA_yUaPgvU (including a Deputy District Attorney stating, "It was the DNA that enabled us to know who raped these women").

[10] *See, e.g.*, Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. (forthcoming 2018) (observing the rise of trade secret assertion in criminal cases).

disclosure of technical information pervades the criminal justice process—from investigation, to trial, to sentencing. For instance, CMI, Inc., the manufacturer of the Intoxilyzer (a common breath test device for intoxication), has repeatedly fought efforts to compel disclosure of its devices' source code in criminal cases, arguing that the source code is a valuable trade secret.[11] Harris Corp., the private company that manufactures and sells the bulk of stingray devices—which effectively turn a cell phone into a real-time tracking device of startling precision—has gone even further.[12] It secured the cooperation of the federal government in preventing disclosure of even the existence of these devices, not only to defense counsel but even to courts themselves, based in part on the device's "valuable proprietary information"—their value as a trade secret.[13] At sentencing, meanwhile, many courts now rely on recidivism risk scores generated by privately developed software whose formula for weighting input factors is, once again, not disclosed on trade secret grounds.[14] Even the Solicitor General of the United States has acknowledged that "[s]ome uses of an undisclosed risk-assessment algorithm" may raise significant constitutional concerns.[15]

---

[11] *See, e.g.*, Charles Short, Note, *Guilt by Machine: The Problem of Source Code Discovery in Florida DUI Prosecutions*, 61 FLA. L. REV. 177, 182 (2009); Associated Press, *Drunk Driving Cases Turn on Source Code*, NBCNEWS.COM (Mar. 12, 2006), http://www.nbcnews.com/id/11752290/ns/technology_and_science-tech_and_gadgets/t/drunk-driving-cases-turn-source-code [https://perma.cc/ZN5N-NKCK] (in a drunken driving case, "[t]he company that makes the Intoxilyzer refused to reveal the computer source code for its machine because it was a trade secret"); *see also* Andrea Roth, *Trial by Machine*, 104 GEO. L.J. 1245, 1272 (2016) (observing that "[t]o date, only one group of litigants has successfully gained access to a breath machine's source code, and even then, only upon court order after the state initially refused to disclose it").

[12] *See* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 101, 104 (2017), http://www.nyulawreview.org/sites/default/files/Joh-FINAL_0.pdf [https://perma.cc/2QJT-SPWG].

[13] *See* Letter from Tania W. Hanna, Dir., Gov't Relations, Harris Corp. & Evan S. Morris, Legal Analyst, Gov't Relations, Harris Corp. to Marlene H. Dortch, Secretary, Fed. Commc'n Comm'n (Oct. 12, 2010) [hereinafter Harris Letter], https://d3gn0r3afghep.cloudfront.net/foia_files/10-8-14_MR13549_RES_ID2014-668.pdf [https://perma.cc/Q9J7-JEC3] (revised request for confidentiality of Harris Corporation); *see also* Joh, *supra* note 12, at 106.

[14] *See, e.g.*, State v. Loomis, 2016 WI 68, ¶¶ 96–122, 371 Wis. 2d 235, 881 N.W.2d 749 (approving the use of COMPAS, a recidivism risk scoring tool, despite nondisclosure of the underlying source code), *cert. denied*, 137 S. Ct. 2290 (2017); *id.* ¶ 51 ("Northpointe, Inc., the developer of COMPAS, considers COMPAS a proprietary instrument and a trade secret."); *see also* Adam Liptak, *Sent to Prison by a Software Program's Secret Algorithms*, N.Y. TIMES (May 1, 2017), https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html [https://perma.cc/6WZY-MSZB] ("Compas and other products with similar algorithms play a role in many states' criminal justice systems.").

[15] Brief for the United States as Amicus Curiae at 18, Loomis v. Wisconsin, 137 S. Ct. 1240 (2017) (No. 16-6387), 2017 WL 2333897, at *18 [hereinafter U.S. *Loomis* Brief]. To be sure, the Acting Solicitor General recommended that the Supreme Court deny certiorari in *Loomis*. *Id.* at *1. The Acting Solicitor General explained that, in his view, "the Wisconsin Supreme Court correctly declined to find a

At each step in the criminal justice process, defendants, their attorneys, and sometimes even the judges in whose courtrooms innocence, guilt, or imprisonment is determined operate at an informational disadvantage due to claims of corporate secrecy. These technologies pit private law assertions of secrecy against criminal justice due process norms.

This Article makes three contributions to the existing literature. It demonstrates that, from investigation to sentencing, the role of private law mechanisms in shielding criminal justice activities is growing. It explains how these mechanisms are problematic for practical and potentially constitutional reasons. And it argues that the secrecy surrounding criminal justice technologies is not essential to their existence or operation. This Article thus offers a way through the growing thicket of trade secrecy assertion that now permeates criminal justice.

First, Part I establishes a common thread of private secrecy tools—trade secrets foremost among them—at work in American criminal justice. Technologies developed by private firms, subject to assertions of private law protection, are now embedded in multiple stages of the criminal justice process. As described above, police, prosecutors, and courts already make use of such technologies. Although scholars previously have shed light on some of these technologies, most have treated these technologies as though they operate in separate silos and have not fully appreciated the role of trade secret assertion throughout the criminal justice system.[16] This Article provides a deeper and broader assessment.

Second, Part II argues that the use of trade secrecy to shield criminal justice technologies from disclosure threatens to stall the development of effective (and appropriate) technology and puts new pressure on traditional criminal defense protections. Well-designed and well-tested algorithms can advance the cause of criminal justice, making the impenetrable

due process violation" in Loomis' case. *Id.* at *18. Nonetheless, the Acting Solicitor General's concession that use of risk-assessment algorithms may raise constitutional concerns is itself significant.

[16] *See, e.g.*, Joh, *supra* note 12 (discussing private secrecy tools in the Fourth Amendment context); Roth, *supra* note 11 at 1274 (discussing the proliferation of algorithms throughout criminal adjudication, but only briefly describing the issue and costs of trade secret assertion surrounding those algorithms); Christian Chessman, Note, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CAL. L. REV. 179, 209–13 (2017); Short, *supra* note 11 (discussing source code discovery difficulties regarding Florida DUI cases only); *cf.* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014) (discussing the rise of "Big Data" algorithms in consumer transactions, and focusing on credit scoring); W. Nicholson Price II, *Black-Box Medicine*, 28 HARV. J.L. & TECH. 419 (2015) (describing the promise and difficulties of highly complex predictive algorithms for personalized medicine). This is only now beginning to change. *See* Wexler, *supra* note 10 (identifying trade secret assertion at multiple points in the criminal justice process).

interpretable or shifting aspects of decisionmaking from more to (hopefully) less biased data sources.[17] But a lack of transparency—and accordingly an inability for defense counsel and others to verify and validate these data sources—makes even the best designed algorithm problematic. Access to source code and other similar information is often essential for defendants to fully interrogate the algorithms that have led to their arrest, conviction, or sentence. Private law protection surrounding the inner workings or even the existence of new technology thus threatens to undermine the ability of judges and defense counsel to ensure that criminal justice respects constitutionally significant privacy interests, condemns only the guilty, and punishes the guilty fairly.

Third, Parts III and IV offer a way forward, bringing the extensive literature on innovation policy to bear on the production of privately developed criminal justice algorithms. Existing literature, where it exists at all, addresses these technologies within the confines of criminal law or the law of evidence.[18] A broader perspective, bridging the fields of intellectual property and criminal justice, yields significant insights.

Contrary to the claims of developers, trade secret protection is not essential for the production of useful algorithms. Innovation policy is more than simply intellectual property rights like trade secrets and patents.[19] Rather, mechanisms for encouraging innovation can fund companies doing research—for example, through grants—or reward companies for the successful products of that research—for example, through prizes or regulatory exclusivities. Tax policy can reward both innovation-focused research and its products.

Unlike trade secrecy, most of these mechanisms can be coupled with a requirement to disclose source code or other relevant information beyond the confines of a protective order or nondisclosure agreement. Part III describes this multitude of policy mechanisms available for incentivizing innovation in the field of criminal justice algorithms, of which trade

---

[17] *See, e.g.*, EXECUTIVE OFFICE OF THE PRESIDENT, FORENSIC SCIENCE IN CRIMINAL COURTS 79 (2016) [hereinafter PCAST REPORT], https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf [https://perma.cc/V3A7-A23P] (concluding that software programs like TrueAllele "clearly represent a major improvement over purely subjective interpretation"); MODEL PENAL CODE § 6.03 cmt. f (Tentative Draft No. 3, 2014) (explaining that algorithmic tools in sentencing may "offer better predictions of future behavior than the clinical judgments of treatment professionals such as psychiatrists and psychologists, or the intuitions of criminal-justice professionals such as judges and probation officers").

[18] *See, e.g.*, Joh, *supra* note 12 (criminal law lens); Roth, *supra* note 11 (same); Wexler, *supra* note 10 (evidence law lens).

[19] *See, e.g.*, Daniel J. Hemel & Lisa Larrimore Ouellette, *Beyond the Patents–Prizes Debate*, 92 TEX. L. REV. 303 (2013) (summarizing the literature on patents versus prizes versus grants and adding tax incentives to the range of innovation policy levers).

secrecy is merely one. Identifying the uses, advantages, and potential costs of various innovation levers makes plain that deference to assertions of trade secret protection in the criminal justice arena is neither necessary nor inevitable. When circumstances demand greater transparency about how criminal justice technologies work, many tools of innovation policy are readily available to deliver the innovation incentive previously provided by secrecy.

Part IV accordingly proposes how innovation policies might be adapted should trade secrecy give way in the face of constitutional and other concerns. In this context, where there is good reason to require disclosure surrounding court proceedings, developers are likely to respond efficiently to mechanisms other than secrecy if secrecy is no longer available. Moreover, achieving an alternate solution should be well within reach. One key actor in innovation policy—the government, through its law enforcement mission—is already inherently enmeshed in encouraging and compensating innovation in this field as the sole (or at least primary) purchaser of the fruits of that innovation. A key actor for enforcing disclosure is also already enmeshed in the tension between trade secret assertion and criminal justice norms—the courts. Courts should be empowered by the existence of alternative innovation policy levers to order trade secret disclosure without fear that useful algorithms will be lost. Indeed, if courts begin to order trade secret disclosure frequently or broadly, other government entities are well situated to institute complementary innovation policies through procurement and other policies, should additional compensation for innovation be necessary. Thus, courts need not wait for legislatures to act.

I. A PROLIFERATION OF SECRET TECHNOLOGY

Privately-developed algorithms have come to occupy a key role in criminal justice processes,[20] and along with them, assertions of trade secret protection. Crucially, it is not merely the fact that algorithms are in use in criminal investigations and proceedings that makes this pattern of technological innovation worthy of note;[21] nor is the fact that these algorithms are developed by private companies, rather than by the state itself, that makes their use so problematic.[22] Rather, it is the concomitant

[20] *See* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 1975 (2017) ("While scientific instruments and cameras have been a mainstay in courtrooms for well over a century, the past century has witnessed a noteworthy rise in the silent testimony of instruments." (internal quotation marks omitted)).

[21] Though this use is certainly noteworthy. *See, e.g.*, Roth, *supra* note 11.

[22] Though this, too, is noteworthy. *See, e.g.*, Joh, *supra* note 12.

pattern of trade secret assertion that cripples courts and defense counsel—and sometimes prosecutors, as well—from ensuring accuracy in criminal justice.

Broadly defined, a trade secret is information that is "subject to reasonable efforts to maintain secrecy and derives independent economic value from its secrecy."[23] So long as the information at issue remains secret, the legal protections of trade secret law will attach indefinitely.[24] Of greatest relevance here, so long as trade secret status remains intact, a trade secret holder may assert that status in litigation to attempt to bar or limit discovery of its protected information.

This Part surveys the conflict between private commercial interests and criminal defense claims from criminal investigation, to trial, to sentencing.

A. Secrecy in Policing

In March 2016, *State v. Andrews* became the first judicial decision to hold that police cannot, without a warrant, make use of a stingray device.[25] A stingray device is a cell site simulator, which allows police to track a cell phone with near pinpoint accuracy in real time.[26] It operates by mimicking a cellphone tower, forcing "all nearby phones within its range to provide it with identifying information."[27] And a stingray is a relatively small

---

[23] W. Nicholson Price II, *Regulating Secrecy*, 91 WASH. L. REV. 1769, 1776 (2016).

[24] *Id.* at 1777.

[25] *See* State v. Andrews, 134 A.3d 324, 327 (Md. Ct. Spec. App. 2016); Spencer S. Hsu, *A Maryland Court is the First to Require a Warrant for Covert Cellphone Tracking*, WASH. POST (Mar. 31, 2016), https://www.washingtonpost.com/world/national-security/a-maryland-court-is-the-first-to-require-a-warrant-for-covert-cellphone-tracking/2016/03/31/472d9b0a-f74d-11e5-8b23-538270a1ca31 [https://perma.cc/95GJ-ENEJ].

[26] Joh, *supra* note 12, at 104. Stingrays are also known as "IMSI catchers." *Stingray Tracking Devices*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices [https://perma.cc/UDU7-MMSY]. "IMSI," in turn, stands for "international mobile subscriber identity," which is "a unique number, usually fifteen digits," that identifies a particular cellphone subscriber. Andrew Hemmer, Note, *Duty of Candor in the Digital Age: The Need for Heightened Judicial Supervision of Stingray Searches*, 91 CHI.-KENT L. REV. 295, 299 n.32 (2016).

The term "stingray" comes from the name of a particular model of cell site simulator. *See* Devin Coldewey, *Who Catches the IMSI Catchers? Researchers Demonstrate Stingray Detection Kit*, TECHCRUNCH (June 2, 2017), https://techcrunch.com/2017/06/02/who-catches-the-imsi-catchers-researchers-demonstrate-stingray-detection-kit [https://perma.cc/4XPH-YHHP]. The company that manufactures the Stingray, Harris Corporation, also manufactures several other similar models, including the KingFish, the TriggerFish, and the Hailstorm devices. Joh, *supra* note 12, at 1044 n.105. Nonetheless, colloquially, the term "stingray" has stuck. *See* Coldewey, *supra*.

[27] Joh, *supra* note 12, at 104; *see also* Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 142–43, 145–47 (2013).

device—roughly the size of a suitcase.[28] It can be "carried by hand, installed in a vehicle, or even mounted on a drone."[29]

A stingray device can be deployed in at least two ways. First, where police know the hardware number of a suspect's cell phone, investigators can use a stingray to pinpoint that phone's location in real time.[30] This is what occurred in *Andrews*. Baltimore police used a stingray device called Hailstorm to track Kerron Andrews to a particular residence, where they arrested him on charges of attempted murder.[31] Indeed, stingray devices appear to be widely used to track cell phones in drug and other criminal investigations.[32]

Second, where police know a location of interest, investigators can use a stingray to identify all mobile devices in the vicinity of that location in real time.[33] Police might rely on this use where, for example, they know the physical location of a suspect in a criminal investigation, but they do not know what phone she is using—perhaps because she frequently changes devices by using "burner" phones.[34] By positioning a stingray device in the known vicinity of the suspect, investigators can collect the hardware number of that suspect's phone.

Importantly, in the course of either use, investigators will collect information about not only a target's cell phone but also all other cellular devices in that area. This is because a stingray operates by tricking all cellular devices in its vicinity to connect to it as they would to a real cell

---

[28] Joh, *supra* note 12, at 104.

[29] Pell & Soghoian, *supra* note 27, at 145.

[30] *See* Jennifer Valentino-DeVries, *How 'Stingray' Devices Work*, WALL ST. J. (Sept. 21, 2011), https://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work [https://perma.cc/A4PZ-CQTS].

[31] State v. Andrews, 134 A.3d 324, 329 (Md. Ct. Spec. App. 2016).

[32] Kim Zetter, *Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight*, WIRED (Apr. 9, 2013), https://www.wired.com/2013/04/verizon-rigmaiden-aircard [https://perma.cc/LHJ7-M2E7]; *see also* Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, BALT. SUN (Apr. 9, 2015), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html [https://perma.cc/94PE-5RNX] (reporting that Baltimore police have acknowledged using a stingray device "4,300 times since 2007," while "[t]he Florida Department of Law Enforcement says its officers have used the device about 1,800 times").

[33] Valentino-DeVries, *supra* note 30.

[34] *See* Pell & Soghoian, *supra* note 27, at 147. A "burner" phone is "a prepaid, inexpensive cell phone intended for temporary use to communicate criminal activities while evading police detection." Abigail Hoverman, Note, Riley *and Abandonment: Expanding Fourth Amendment Protection of Cell Phones*, 111 NW. U. L. REV. 517, 551 (2017).

phone tower.[35] Moreover, a stingray device may interrupt service to other devices in its vicinity.[36]

Beyond these basics, however, little is publicly known about stingray devices, including about how they work and how often they are used. The acquisition and use of stingray devices in individual cases is difficult to track. To date, the ACLU has identified "72 agencies in 24 states and the District of Columbia" as stingray owners.[37] At the same time, the ACLU asserts that that number "dramatically underrepresents the actual use of stingrays by law enforcement agencies nationwide" because "many agencies continue to shroud their purchase and use of stingrays in secrecy."[38] The secrecy surrounding law enforcement use of stingrays has also made it difficult to discover information about how exactly a stingray device works or can be used.[39]

That secrecy is not merely a product of investigative intransigence or "law enforcement privilege."[40] It is instead the deliberately sought outcome of the primary manufacturer of stingray devices—Harris Corporation.[41] For many years, Harris sold stingray devices to federal investigators.[42] When Harris sought to expand sales to local law enforcement departments, however, federal law required the Federal Communications Commission's (FCC) approval.[43] And when Harris filed for the necessary authorization, it requested that information about its devices "be treated as confidential and withheld from public inspection."[44] Harris offered two reasons for this request: that disclosure "could cause significant harm to federal, state, and

---

[35] Pell & Soghoian, *supra* note 27, at 147–48.

[36] Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders*, WIRED (Mar. 1, 2015), https://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders [https://perma.cc/6AZ7-CGA2].

[37] *Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them [https://perma.cc/9KU5-YZX9].

[38] *Id.*

[39] *See* Robert Patrick, *Controversial Secret Phone Tracker Figured in Dropped St. Louis Case*, ST. LOUIS POST-DISPATCH (Apr. 19, 2015), http://www.stltoday.com/news/local/crime-and-courts/controversial-secret-phone-tracker-figured-in-dropped-st-louis-case/article_fbb82630-aa7f-5200-b221-a7f90252b2d0.html [https://perma.cc/UVV3-3KQ7] ("The ability to track cellphones through their service providers' antenna network is commonly known and is openly discussed in court and on TV shows. But the full capabilities of the StingRay are not clear.").

[40] On the history of the law enforcement privilege, see Stephen Wm. Smith, *Policing Hoover's Ghost: The Privilege for Law Enforcement Techniques*, 54 AM. CRIM. L. REV. 233 (2017).

[41] *See* Joh, *supra* note 12, at 104.

[42] Patrick, *supra* note 39.

[43] *Id.*

[44] Harris Letter, *supra* note 13.

local law enforcement surveillance activities," and that disclosure might similarly "cause significant harm to . . . Harris' competitive interests."[45]

Despite identifying its competitive interests second, Harris devoted the bulk of its confidentiality request to this interest. Harris explained that public disclosure of information about stingrays "could compromise Harris' ability to sell and continue to develop the Stingray® product line" because such disclosure "would provide other companies the opportunity to reverse engineer the surveillance technology."[46] Emphasizing the "many competitors that provide surveillance equipment to law enforcement officials," Harris pressed that "any disclosure . . . regarding the Stingray® product would relinquish valuable proprietary information about how the technology was developed and the manufacturing process."[47] And Harris bluntly asserted that "[d]isclosure would result in substantial competitive harm to Harris" and "would reveal Harris trade secrets."[48]

Assuring the FCC that it had taken care to protect "proprietary aspects of its equipment design and manufacturing processes," Harris requested that information about stingray devices "be withheld from public disclosure until and unless Harris notifies the Commission that such information may be publicly released."[49] To facilitate its request for confidentiality, Harris proposed that it would market and sell its stingray devices to "federal/state/local public safety and law enforcement officials only" and that "[s]tate and local law enforcement agencies must advance coordinate with the FBI the acquisition and use of equipment authorized under this authorization."[50]

The FCC granted Harris's nondisclosure request, and the result has been a raft of rigid nondisclosure agreements between the FBI and local police departments.[51] For instance, in order to acquire the Hailstorm device at issue in *Andrews*, the Baltimore Police Department had to enter into a nondisclosure agreement with the FBI,[52] agreeing among other things not to disclose the use of the Hailstorm device—even to a court, and even if it

---

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *See* Joh, *supra* note 12, at 106.

[52] State v. Andrews, 134 A.3d 324, 337–38 (Md. Ct. Spec. App. 2016) (describing the nondisclosure agreement as a "condition of [Baltimore Police Department's] purchase of" the Hailstorm device).

meant dropping charges all together.[53] A similar nondisclosure agreement signed by the Tucson Police Department prohibits the City of Tucson from disclosing any information about its stingray use—even to "other governmental entit[ies]"—without Harris's prior written consent.[54] Allocating the power to determine disclosure to Harris, rather than to a law enforcement agency, reinforces the "competitive interest" rationale for secrecy, while attenuating any relationship between nondisclosure and legitimate law enforcement concerns. Similar nondisclosure agreements have been unearthed for several other police departments around the country.[55]

Pursuant to these nondisclosure obligations, police departments have gone to great lengths to obscure their possession and use of stingray devices. Prosecutors appear to have dropped charges rather than face questions about stingray use.[56] Investigators have also stymied court overview of stingray use by obfuscating their use of the devices in court documents. In *Andrews*, for instance, the court admonished the police department for intentionally concealing its use of a stingray device from a judge when seeking a court order to track the defendant.[57] Moreover, likely because of its nondisclosure agreement, "the State provided limited information regarding the function and use" of the stingray device in judicial hearings regarding the admissibility of information obtained through its use.[58]

---

[53] *Id.* at 338 (summarizing the nondisclosure agreement, including its instruction that "[i]f necessary 'the Office of the State's Attorney for Baltimore will, at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to provide, any information concerning the Harris Corporation wireless collection equipment/technology'" (quoting Non-Disclosure Agreement Between Ernest Reith, Acting Assistant Dir., Operational Tech. Div., Fed. Bureau of Investigation, and Frederick H. Bealefeld, III, Police Comm'r, Balt. Police Dept. & Gregg L. Bernstein, Esq., State's Attorney, Office of the State's Attorney for Balt. City ¶ 5 (Aug. 11, 2011), http://s3.documentcloud.org/documents/1808819/baltimore-police-stingray-non-disclosure-agreement.pdf [https://perma.cc/6PFZ-CFE3])).

[54] Kim Zetter, *Police Contract with Spy Tool Maker Prohibits Talking About Device's Use*, WIRED (Mar. 4, 2014), https://www.wired.com/2014/03/harris-stingray-nda [https://perma.cc/SCB4-C62B] (quoting the nondisclosure agreement entered into by the City of Tucson, Arizona).

[55] Joh, *supra* note 12, at 106–08 (discussing nondisclosure agreements with the police departments of Baltimore, Maryland; Tucson, Arizona; and St. Louis, Missouri).

[56] *See* Patrick, *supra* note 39 ("Just one day before a city police officer was to face questions about a secret device used to locate suspects in a violent robbery spree, prosecutors dropped more than a dozen charges against the three defendants."). More broadly, Patrick reports, "[o]fficials across the U.S. have been willing to drop cases rather than subject the technology to scrutiny by judges and defense lawyers." *Id.*

[57] *Andrews*, 134 A.3d at 338–39.

[58] *Id.* at 340.

Private competitive concerns and assertions of trade secrecy thus have impeded both courts and defendants from knowing, examining, or effectively challenging how criminal cases are built or potential defendants identified and investigated. Significantly, as in *Andrews*, secrecy surrounding stingray use often shrouds investigative methods in mystery, even though prosecutors may not seek to rely at trial on data generated by the stingray device itself.[59] These devices accordingly implicate different criminal justice interests than tools designed to produce trial evidence directly.

B. Secrecy in Prosecuting

Just as trade secret assertion pervades aspects of criminal investigation, so too has it come to occupy a central role in the production and presentation of key evidence for criminal trials. Two technologies exemplify the growth, persistence, and effectiveness of trade secret assertion surrounding the production of evidence: alcohol breath test devices and probabilistic genotyping software. Together, these technologies represent two generations of cases grappling with private trade secret assertion in the context of criminal discovery.[60]

1. Alcohol Breath Test Devices

Among the most longstanding tools in this category are breath test devices for measuring intoxication in drivers suspected of driving under the influence. These devices connect a small tube to a portable computer.[61] When a suspect blows into the tube, that air flows "into a chamber with an infrared light and a sensor that's designed to detect alcohol vapor through a process called infrared spectrometry."[62] Breath test machines often sport names designed to convey "mechanical objectivity," like the "Breathalyzer," the "Drunk-O-Meter," or the "Intoxilyzer."[63]

---

[59] *Id.* In *Andrews*, for instance, police used a stingray device to track Andrews to a specific location, where a subsequent search (with a warrant) uncovered a gun nearby. *Id.* at 326. Andrews argued that the gun should be suppressed as evidence tainted by the warrantless use of the stingray device—as "fruit of the poisonous tree." *Id.* The location data generated by the stingray device directly was not at issue because prosecutors did not seek to rely on that data during a trial.

[60] *See* Imwinkelried, *supra* note 8, at 100.

[61] *See* Declan McCullagh, *Police Blotter: Court Won't Release Breathalyzer Source Code*, CNET NEWS (Feb. 3, 2009), https://www.cnet.com/news/police-blotter-court-wont-release-breathalyzer-source-code [https://perma.cc/G5XU-MFHC] (describing how breath test devices work).

[62] *Id.*; *see also In re* Source Code Evidentiary Hearings in Implied Consent Matters, 816 N.W.2d 525, 528 (Minn. 2012) (describing leading breath test device as "us[ing] infrared absorption spectroscopy to measure the breath alcohol concentration of subjects who provide breath samples").

[63] Roth, *supra* note 11, at 1269. Importantly, these alcohol breath test devices are not the handheld tools used by law enforcement officers to conduct field sobriety tests at the roadside. *See* Birchfield v. North Dakota, 136 S. Ct. 2160, 2191 (2016) (Sotomayor, J., dissenting) ("There is a common

Like Harris, manufacturers of breath test devices have strenuously resisted efforts to make information about their devices public or even accessible to criminal defense experts.[64] For instance, Draeger, which manufactures the Alcotest, one popular breath test device, has refused to sell its devices to non-law enforcement individuals for independent testing,[65] while asserting trade secrecy in its source code.[66] In criminal cases, CMI, Incorporated, the manufacturer of the Intoxilyzer, another common breath test device, has repeatedly refused to disclose the source code for its devices on trade secret grounds.[67] Source code is the "lifeblood" of a piece of software.[68] It "dictates which tasks a program performs, how the program performs the tasks, and the sequence in which the program performs the tasks."[69]

Most of the time, this assertion of trade secrecy has prevailed. Courts have repeatedly vindicated manufacturers' trade secret claims—directly or indirectly—by refusing to grant defendants access to the source code of breath test devices.[70] In some cases, courts have explicitly acceded to manufacturers' assertions of trade secret protection.[71] In others, courts have

misconception that breath tests are conducted roadside, immediately after a driver is arrested. While some preliminary testing is conducted roadside, reliability concerns with roadside tests confine their use in most circumstances to establishing probable cause for an arrest. The standard evidentiary breath test is conducted after a motorist is arrested and transported to a police station, governmental building, or mobile testing facility where officers can access reliable, evidence-grade breath testing machinery." (citations omitted)).

[64] Defendants have also faced significant difficulty in assessing whether the data indicating their intoxication is valid due to the paucity of data that many breath test devices actually produce for inspection. The Intoxilyzer 8000, for instance, produces only a "printout card" reporting blood alcohol concentration—it does not preserve any material that could be retested. *See* Roth, *supra* note 11, at 1271.

[65] *See* MARK DENBEAUX ET AL., THE UNTESTABLE DRUNK DRIVING TEST (2009). According to Denbeaux and colleagues, Draeger has also prohibited the State of New Jersey, with which Draeger holds an exclusive contract to supply alcohol breath test devices, from making any Draeger device available for outside, independent testing.

[66] State v. Chun, 943 A.2d 114 (N.J. 2008) (describing Draeger's efforts to resist source code disclosure).

[67] *See, e.g.*, Associated Press, *supra* note 11; McCullagh, *supra* note 61.

[68] Imwinkelried, *supra* note 8, at 99 (internal quotation marks omitted).

[69] *Id.*

[70] *See id.* at 100 ("With few exceptions, the clear majority of courts rejected defendants' requests that a defense expert be granted access to the program's source code." (footnotes omitted)); *see, e.g.*, State v. Burnell, No. MV06479034S, 2007 WL 241230, at *2 (Conn. Super. Ct. Jan. 18, 2007); Moe v. State, 944 So. 2d 1096, 1097 (Fla. Dist. Ct. App. 2006); People v. Cialino, 831 N.Y.S.2d 680, 681–82 (Crim. Ct. 2007). *But see, e.g.*, State v. Underdahl, 767 N.W.2d 677, 683–84 (Minn. 2009); State v. Chun, 923 A.2d 226, 226–27 (N.J. 2007).

[71] *See* Imwinkelried, *supra* note 8, at 110 (identifying courts in Connecticut, Florida, and New York as denying access to source code on these bases); Chessman, *supra* note 16, at 205 (identifying

denied defense discovery requests for the source code of a breath test device on grounds that the state is not in possession of the relevant code and so cannot disclose it.[72]

In *Moe v. State*, the Florida Court of Appeals cited both of these rationales—and demonstrated their relatedness—in denying a defendant access to the source code for Intoxilyzer 5000:

> It is without dispute that the State does not have possession of the source code because it is the property of CMI, Inc. It is also without dispute that the code is a trade secret of CMI, Inc. and that CMI, Inc. has invoked its statutory and common law privileges protecting the code from disclosure. Therefore, the State cannot obtain possession of the code.[73]

The State of Florida appears to have deliberately persisted in its non-possession of the relevant source code.[74]

Moreover, in some cases, CMI has refused to cooperate even where courts have granted defense requests to examine the relevant source code. In one group of Florida cases, CMI refused any disclosure until the courts, whose orders CMI had flouted, levied fines against it totaling more than $500,000.[75] Similarly, CMI has refused to disclose its source code even when that nondisclosure has prompted judges to dismiss charges.[76]

In the few cases where the disclosure of source code has successfully been compelled, that disclosure has come only after much wrangling. In Minnesota, for instance, the Department of Public Safety had to sue CMI itself to gain access to the source code underlying the Intoxilyzer devices in

---

three primary bases for denying defendants access to source code, including that "the source code is a trade secret").

[72] *See* Imwinkelried, *supra* note 8, at 110 (identifying a court in New York that denied access to source code on this basis); Chessman, *supra* note 16, at 205 (identifying "the state does not possess the source code" among the primary bases for denying defendants access to source code).

[73] 944 So. 2d at 1097; *see also* People v. Robinson, 860 N.Y.S.2d 159, 167 (App. Div. 2008) (explaining that "[t]he Intoxilyzer source code was not the property of the State, since it was owned and copyrighted by its manufacturer, CMI, Inc., a Kentucky corporation, and is a trade secret of CMI, Inc." and discussing similar cases); *Cialino*, 831 N.Y.S.2d at 681 (denying discovery because the source code was "the property of a corporation that invoked statutory and common law privileges protecting the code from disclosure, thereby making it unobtainable").

[74] *See* Chessman, *supra* note 16, at 214; Short, *supra* note 11, at 195 ("Florida, however, has made no effort to obtain the source code itself so that it can ensure the reliability of the Intoxilyzer's source code. Indeed, when the state had the opportunity to write some form of source code access into its contract with the manufacturer CMI, Inc., it declined to do so." (footnotes omitted)).

[75] *See* Short, *supra* note 11, at 183; Todd Ruger, *Fines Rise in DUI Software Fight*, SARASOTA HERALD-TRIBUNE (Mar. 9, 2008), http://www.heraldtribune.com/news/20080309/fines-rise-in-dui-software-fight [https://perma.cc/2K85-443Y]. In light of those fines, CMI sought to arrange a "controlled viewing" of its source code, coupled with a protective order and a nondisclosure agreement. Ruger, *supra*.

[76] *See, e.g.*, Associated Press, *supra* note 11.

use throughout the state.[77] CMI resisted that lawsuit as well, asserting once again that "the source code itself contained proprietary trade secrets which it would not disclose under any circumstances."[78]

There is good reason for defendants to seek to examine the breath test devices whose results are used to investigate, charge, and convict them. For one thing, human programmers are the ones who encode breath test devices with judgments about when and how to measure alcohol vapor and how to convert that into a number signifying intoxication.[79] Sometimes, those judgments are wrong. For instance, one court observed that the Intoxilyzer model at issue could give false positive results—indicating intoxication where there is none—for individuals who suffer from diabetes, are on the Adkins diet, or experience occupational exposure to certain paint thinners.[80] These false positives are due not to inadvertent errors in programming but rather to intentional judgments about how to measure alcohol in the breath.[81] A certain number of false positive results are the foreseeable consequence of an imperfect methodology that measures compounds in the breath without accounting for alternative (non-alcoholic) compounds that may yield similar test results.[82] Commentators have also observed that breath test devices may give incorrect results if an individual either blows insufficient air or blows for too long into the device.[83] In this Goldilocks scenario, an error may result from blowing too much or too little.

Sometimes, even if its science is sound, a machine may malfunction for other reasons entirely. As developers identify bugs, patch them, and

---

[77] *See* David Hanners, *State Sues Breath-Test Machine Manufacturer*, TWIN CITIES PIONEER PRESS (Mar. 3, 2008), http://www.twincities.com/2008/03/03/state-sues-breath-test-machine-manufacturer [https://perma.cc/CR6G-XFC9].

[78] *Id.* (quoting Minnesota's complaint (citation omitted)). Minnesota did not seek CMI's source code eagerly. It initiated litigation against CMI only after the Minnesota Supreme Court concluded, in separate litigation, that the state was entitled to access the source code and that defendants were entitled to examine it. *See In re* Comm'r of Pub. Safety, 735 N.W.2d 706, 713 (Minn. 2007).

[79] *See* Roth, *supra* note 11, at 1270–71.

[80] State v. Bastos, 985 So. 2d 37, 41–42 (Fla. Dist. Ct. App. 2008); Short, *supra* note 11, at 178.

[81] *See Bastos*, 985 So. 2d at 41–42 ("[T]he machine is designed to examine only a portion of the infrared spectrum. For that reason, it is unable to produce a 'fingerprint' identification of ethanol to the exclusion of all other compounds. Instead, the machine is known to produce false positives. Examples of this would be compounds produced by the body as a result of the Adkins diet or diabetes. Exposure (usually occupational exposure) to certain paint thinners, lacquer, varnishes, and industrial cleaning solvents can also produce false positives.").

[82] *See id.*

[83] *See* Roth, *supra* note 11, at 1272 (observing that the Intoxilyzer 5000 could give "erroneous 'deficient sample' readings based on an artificially high breath-volume requirement"); Short, *supra* note 11, at 179–80 ("the longer an individual blows into the breath testing machine the higher the breath test results can be" (footnote omitted)).

perform other updates, they may introduce unintended errors.[84] One group of litigants discovered that the Intoxilyzer 8000 "was not properly programmed to differentiate between residual alcohol in the mouth and alcohol found in deep lung air, thus potentially leading to false positives."[85] In another case, independent analysis of the Draeger Alcotest 7110 found that catastrophic error detection was disabled, "meaning that the Alcotest software could appear to run correctly while executing wild branches or invalid code for a period of time."[86] The analysts further concluded, "the Alcotest software would not pass U.S. industry standards for software development and testing."[87] In light of results like these, at least two states have rejected use of the Intoxilyzer 8000, while other courts have, on occasion, refused to admit its results at trial.[88]

2. Probabilistic Genotyping Software

Alcohol breath test devices are not the only tool prosecutors rely on that inject private trade secret assertion into public criminal proceedings. A newer entrant in this domain is probabilistic genotyping software, typified by TrueAllele.[89] TrueAllele was the first (and remains among the most popular) of at least ten distinct software programs designed to "marshal[] complex statistics" to complete DNA analysis that traditional methods cannot.[90] While some of these programs are open-source, meaning that their

---

[84] *See* Ken Strutin, *An Examination of Source Code Evidence*, N.Y. L.J. (Nov. 13, 2007), http://www.newyorklawjournal.com/id=900005495696/An-Examination-of-Source-Code-Evidence [https://perma.cc/Q6V8-UN7A]; *see also* Chessman, *supra* note 16, at 186–92 (identifying "structural sources of error" that may unintentionally cause software to be unreliable or faulty, including "accidental errors," "software updates to legacy code," and "software rot").

[85] Roth, *supra* note 11, at 1271.

[86] Lawrence Taylor, *Secret Breathalyzer Software Finally Revealed*, DUI BLOG (Sept. 4, 2007), http://www.duiblog.com/2007/09/04/secret-breathalyzer-software-finally-revealed [https://perma.cc/5FXC-GZKC]; *see also* State v. Chun, 943 A.2d 114, 159 (N.J. 2008) (noting that the Alcotest's catastrophic error detection had been disabled in the firmware version 3.11, and that "if utilized, it would ensure that the device would shut down if it encountered such an error"); Short, *supra* note 11, at 185 (discussing *Chun* and the source code errors that independent analysis uncovered in the Draeger Alcotest).

[87] Taylor, *supra* note 86 (capitalization omitted).

[88] *See* Roth, *supra* note 11, at 1272 nn.150–51 (observing that Alaska and Tennessee have declined to certify the Intoxilyzer 8000, while at least one Ohio state court has refused to admit its results).

[89] *See* Imwinkelried, *supra* note 8, at 100 (noting the similarity of issues surrounding alcohol breath test devices and advanced DNA-analysis tools like TrueAllele).

[90] MURPHY, *supra* note 8, at 97; *see also* Roth, *supra* note 11, at 1262–63 (describing TrueAllele as a "coup de grâce" for computerized genetic interpretation and observing that "several other companies now have competing but similar software").

source code is freely available to the public, both TrueAllele and its primary competitor, STRmix, are not.[91]

Traditionally, human analysts have "manually and visually interpret[ed] DNA markers."[92] Where those methods of analysis fall short—often with the most complex mixtures or degraded fragments of DNA—probabilistic genotyping seeks to deliver answers. Probabilistic genotyping software employs a "mathematical model[] that aim[s] to predict when and why erratic observed results are nonetheless explainable."[93] In so doing, such software "endeavor[s] to account for the unpredictable behavior of DNA samples with low template or too many contributors."[94]

Mark Perlin, who created TrueAllele and sells it through his company Cybergenetics, boasts that TrueAllele "can be applied to any DNA mixture, always giving an answer."[95] Indeed, Perlin markets TrueAllele as a tool for analyzing precisely those DNA samples that are most likely to yield inconclusive results: samples containing DNA from multiple individuals

---

[91] *See* Roth, *supra* note 20, at 2019 ("Some developers have opened their source code to the public; others, such as Cybergenetics's 'TrueAllele' program and New Zealand DNA expert John Buckleton's 'STRmix,' have not." (citations omitted)); Lauren Kirchner, *Where Traditional DNA Testing Fails, Algorithms Take Over*, PROPUBLICA (Nov. 4, 2016), https://www.propublica.org/article/where-traditional-dna-testing-fails-algorithms-take-over [https://perma.cc/7CTW-BPPD] [hereinafter Kirchner, *Algorithms Take Over*]; *see also* PCAST REPORT, *supra* note 17, at 78–79 ("As of March 2014, at least 8 probabilistic genotyping software programs had been developed (called LRmix, Lab Retriever, likeLTD, FST, Armed Xpert, TrueAllele, STRmix, and DNA View Mixture Solution), with some being open source software and some being commercial products."). Despite the fact that FST was developed by the New York Office of the Chief Medical Officer (OCME), that office has repeatedly resisted efforts to examine FST's source code in criminal cases. *See* Lauren Kirchner, *Traces of Crime: How New York's DNA Techniques Became Tainted*, N.Y. TIMES (Sept. 4, 2017), https://www.nytimes.com/2017/09/04/nyregion/dna-analysis-evidence-new-york-disputed-techniques.html [https://perma.cc/DRN4-NLP3] [hereinafter Kirchner, *Traces of Crime*] (explaining that, in response to defense counsel requests to examine FST's source code, "the government refused to hand it over on the grounds that it was a 'proprietary and copyrighted' statistical tool owned by the City of New York").

[92] Kirchner, *Algorithms Take Over*, *supra* note 91.

[93] MURPHY, *supra* note 8, at 97.

[94] *Id.*

[95] Letter from Mark W. Perlin, Chief Sci. & Exec. Officer, Cybergenetics, to Jerry D. Varnell, Fed. Bureau of Investigation (Apr. 1, 2015), https://www.cybgen.com/information/newsroom/2015/may/Letter_to_FBI.pdf [https://perma.cc/7W7D-EBNZ] [hereinafter Perlin Letter].

("mixture" samples)[96] and samples containing very few cells ("low copy number" samples).[97] Perlin asserts that TrueAllele is "entirely objective."[98]

Yet, as with claims about the function and accuracy of stingray and alcohol breath test devices, Perlin's claims about TrueAllele's accuracy are difficult to verify because Perlin has invoked the shroud of trade secrecy. As in the *Billy Ray Johnson* case, Perlin has steadfastly refused to disclose TrueAllele's source code, even under protective order.[99] Perlin explicitly ties his nondisclosure to trade secrecy, writing that such secrecy is "needed by companies to innovate essential technology in a competitive world."[100] And while Perlin and his colleagues have published a handful of validation studies in peer-reviewed journals, even those did not make the underlying data available for independent reviewers to assess.[101] As set forth above, no one outside of Perlin's company has seen or examined TrueAllele's source code.[102]

Despite this lack of vigorous outside review, courts in at least ten states have admitted TrueAllele's results in criminal trials, while none have ordered disclosure of TrueAllele's source code.[103] In many cases, courts have relied on Perlin's assertion of trade secret protection in declining to

---

[96] *See* Perlin Letter, *supra* note 95, at 2 (describing TrueAllele as "a computerized solution to the DNA mixture problem"); CYBERGENETICS, https://www.cybgen.com/welcome.shtml [https://perma.cc/SX5C-346A] (asserting, on Cybergenetics' homepage, that TrueAllele "quickly and reliably solves DNA mixtures").

[97] CYBERGENETICS, TRUEALLELE® CASEWORK SERVICES (2013), https://www.cybgen.com/services/service_e-brochure.pdf [https://perma.cc/YR9N-WHF6] (brochure advertising TrueAllele and asserting, under frequently asked questions, that "TrueAllele Casework technology work[s] with Low Copy Number DNA"). In low copy number samples, the small number of available cells in a crime scene sample typically provides too little DNA for accurate analysis.

[98] Perlin Letter, *supra* note 95, at 3.

[99] Roth, *supra* note 11, at 1274; Wexler, *supra* note 1.

[100] *See* Mark Perlin, *Computers Are Helping Justice*, CYBERGENETICS (June 16, 2017), https://www.cybgen.com/information/newsroom/2017/jun/Cybergenetics-to-New-York-Times-Computers-are-helping-justice.shtml [https://perma.cc/PQ89-M5SN]. Perlin also declares that "privileged information," like that protected by trade secret law, "benefits society." *Id.*

[101] Roth, *supra* note 11, at 1274.

[102] *See* MURPHY, *supra* note 8, at 101 ("Perlin admitted that no other scientists had seen his code or reviewed it directly, and he stood by his refusal to make it available, defending it as a 'trade secret.'"); Robert Gavin, *Cybergenetics True Allele Casework DNA Study is Winner in Cold Case Murder Conviction*, TIMES UNION (Mar. 31, 2015), http://www.timesunion.com/tuplus-local/article/Cybergenetics-True-Allele-Casework-DNA-study-is-6171690.php [https://perma.cc/XU89-YQUL] ("Only [Perlin] and one of his colleagues know the 'source code' behind [TrueAllele].").

[103] *See TrueAllele Admissibility*, CYBERGENETICS, https://www.cybgen.com/information/admissibility/page.shtml [https://perma.cc/DJW2-69CA] (identifying cases admitting TrueAllele into evidence in California, Indiana, Louisiana, Massachusetts, New York, Ohio, Pennsylvania, South Carolina, Virginia, and Washington State).

order source code disclosure.[104] In the *Billy Ray Johnson* case, for instance, the trial court concluded, "[t]he source code is a trade secret. I don't think adequate showing has been made to justify the breech [sic] of that privilege."[105] In another case denying disclosure, the judge simply stated, "[t]his source code is the intellectual property of Cybergenetics."[106] Ordering disclosure "would not be reasonable," that court explained, because it "would cause irreparable harm to the company, as other companies would be able to copy the code and potentially put him out of business."[107]

To date, only one American court has compelled production of the source code for probabilistic genotyping software in a criminal case. In July 2016, a federal district court ordered New York City's crime laboratory to turn the source code of the lab's in-house Forensic Statistical Tool ("FST," a probabilistic genotyping tool) over to a defense expert for analysis.[108] That expert concluded, "the correctness of the behavior of the FST software should be seriously questioned."[109] Shortly thereafter, the U.S. attorney's office withdrew the FST-based DNA evidence in the case.[110] The crime lab later announced that it was discontinuing use of FST altogether.[111] Tellingly, however, the source code at issue in this case was not privately developed. Rather, it was developed by the crime lab itself, in the New York Office of the Chief Medical Officer (OCME).[112] As such, the

---

[104] *See* Wexler, *supra* note 10, at 12 n.48 (collecting cases in which courts have denied defendants access to source codes for probabilistic DNA-analysis software programs because the codes were alleged to be trade secrets).

[105] Respondent's Brief at 73, People v. Johnson, No. F071640 (Cal. Ct. App. Aug. 7, 2017) (quoting the trial court's decision (citation omitted)).

[106] Memorandum Order at 1, Commonwealth v. Robinson, No. CC 201307777 (Pa. C.P. Feb. 4, 2016).

[107] *Id.* at 2

[108] Order, United States v. Johnson, No. 1:15-CR-00565 (S.D.N.Y. July 6, 2016) (order denying crime lab's motion to quash source code subpoena); Memorandum in Support of Application by ProPublica for Leave to Intervene, Lift the Protective Order and Unseal Judicial Records at 7, United States v. Johnson, No. 1:15-CR-00565 (S.D.N.Y. Sept. 25, 2017) [hereinafter ProPublica Memorandum].

[109] Kirchner, *Traces of Crime*, *supra* note 91.

[110] *Id.*

[111] *Id.* The laboratory announced that, in place of FST, it would use the privately developed and proprietary STRmix. *Id.*

[112] Lauren Kirchner, *ProPublica Seeks Source Code for New York City's Disputed DNA Software*, PROPUBLICA (Sept. 25, 2017), https://www.propublica.org/article/propublica-seeks-source-code-for-new-york-city-disputed-dna-software [https://perma.cc/MR26-SS26].

software was not subject to the same kind of assertions of trade secrecy as TrueAllele.[113]

As the FST case makes clear, like breath test and other devices, the secrecy surrounding the details of how probabilistic genotyping software works is cause for concern. At the most basic level, DNA analysis is not the "crystal ball" it so often appears to be.[114] While forensic genetic analysis rests on a scientifically sound basis,[115] its use in practice has been riddled with errors.[116] There are dozens of known scandals involving mistaken, sloppy, or fraudulent casework.[117] Even if every crime scene investigator and lab analyst performs their work flawlessly, the resulting analysis may be inconclusive, unhelpful, or incorrect. This is because crime scene DNA is typically not a pristine sample. Instead, "[c]rime scene testing . . . is like seeking results from [a] dirty Band-Aid—after it has been in the trash for two weeks."[118] Such samples "may have been exposed to light, heat, moisture, or chemicals that can compromise the ability to get results."[119]

For its part, TrueAllele claims to mitigate these pitfalls by automating the DNA "interpretation process to give accurate and reliable answers,"[120]

---

[113] Of course, the OCME nonetheless repeatedly resisted efforts to examine FST's source code in criminal cases. *See* Kirchner, *Traces of Crime*, *supra* note 91. Disclosure of FST's source code was originally subject to a protective order. *See* ProPublica Memorandum, *supra* note 108, at 7 (recounting the procedural history of this case). That protective order was subsequently vacated. Order, United States v. Johnson, No. 1:15-cr-00565 (S.D.N.Y. Oct. 16, 2017) (order unsealing most records previously sealed or redacted); *see also* Lauren Kirchner, *Federal Judge Unseals New York Crime Lab's Software for Analyzing DNA Evidence*, PROPUBLICA (Oct. 20, 2017), https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence [https://perma.cc/NES4-Y82W].

[114] Natalie Ram, Book Review, 3 J.L. & BIOSCIS. 426, 427 (2016) (reviewing MURPHY, *supra* note 8); *see* MURPHY, *supra* note 8, at 311 (concluding that "DNA testing is neither savior nor cure-all; it is just another form of proof deserving of careful attention").

[115] *See* NAT'L RES. COUNCIL, COMM. ON IDENTIFYING THE NEED OF THE FORENSIC SCI. CMTY, STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 133 (2009) [hereinafter NAS REPORT] (providing multiple reasons why DNA testing is scientifically sound).

[116] *See generally* MURPHY, *supra* note 8 (documenting how DNA is collected, analyzed, disclosed, and used in criminal investigations and trials, and exposing its repeated documented scandals and errors).

[117] Ram, *supra* note 114, at 429; *see* MURPHY, *supra* note 8, at 53–73 (describing insufficient internal audit procedures, proficiency testing, oversight by forensic laboratory accreditation organizations, and quality assurance protocols, as well as inadequate laboratory resources, training, and even qualified supervisory personnel at numerous forensics laboratories throughout the United States). For instance, Murphy reports that deceptive behavior by lab analysts—"suggesting work was performed that actually was not—has occurred so many times that there is a word for it: *dry-labbing*." MURPHY, *supra* note 8, at 68.

[118] MURPHY, *supra* note 8, at 19.

[119] *Id.*

[120] Perlin Letter, *supra* note 95, at 3.

but that is not a complete response. For one thing, TrueAllele is marketed for use in the types of cases most likely to suffer from laboratory errors, even under the best of circumstances—those involving mixtures and low copy number samples.[121] As Professor Erin Murphy has explained, "when low quantities of DNA are tested, the potential for contamination runs high."[122] An imperfectly cleaned workspace or an analyst's accidental sneeze at the wrong moment may introduce foreign cells into an already-complex mixture or low copy number sample, confounding accurate analysis of the number of contributors and their distinct genetic profiles in the original sample.[123] More broadly, the factors giving rise to mistaken, sloppy, or fraudulent lab work are likely to be as significant, if not worse, where complex mixtures or low copy number samples are involved.

Moreover, while Perlin claims that TrueAllele is equally capable of "resolv[ing] DNA mixtures without any limitation on the number of contributing individuals,"[124] the President's Council of Advisors on Science and Technology disagrees.[125] In a recent report, that Council concluded that TrueAllele is reliable only "within a certain range, based on the available evidence and the inherent difficulty of the problem."[126] Specifically, TrueAllele was determined to be reliable for, at best, "three-person mixtures in which the minor contributor constitutes at least 20 percent of the intact DNA in the mixture" and in two-person mixtures where the minor contributor accounts for at least 10 percent of the available DNA.[127] Unfortunately, these thresholds may be unknown in many cases, particularly those involving degraded DNA evidence not susceptible to traditional analysis. Indeed, based on TrueAllele's marketing for and use in cases involving complex samples, one member of a forensic committee that

---

[121] *See supra* notes 96–97 and accompanying text.

[122] MURPHY, *supra* note 8, at 76. (describing difficulties with low copy number samples).

[123] *Id.* at 77.

[124] Perlin Letter, *supra* note 95, at 4.

[125] *See* PCAST REPORT, *supra* note 17, at 80 n.215 (noting that "the interpretation of DNA mixtures becomes increasingly challenging as the number of contributors increases").

[126] *Id.* at 80. The Report issued the same findings for STRmix. *Id.*

[127] *Id.* at 80 & n.216. In these cases, the Council observed that the mixtures involve "similar proportions" of DNA, which "are more straightforward to interpret owing to the limited number of alleles and relatively similar peak height." *Id.* at 80 n.216. Where a crime scene sample contains a mixture of DNA from multiple individuals, a "minor" contributor is an individual whose DNA is present as a small proportion of the total available DNA in the sample. *See* KEITH INMAN & NORAH RUDIN, AN INTRODUCTION TO FORENSIC DNA ANALYSIS 113 (2d ed. 2001) (explaining difficulties encountered in PCR when samples contain DNA from two or more people). If the disparity between major and minor DNA contributors becomes too great, this can make it difficult to assess the presence of the minor contributor and impossible to accurately identify the minor contributor's DNA profile. *Id.* Cases with a smaller number of contributors and larger proportions of minor contributor DNA are less likely to suffer from these defects. PCAST REPORT, *supra* note 17, at 80 n.216.

approved TrueAllele for use in New York in 2011 subsequently retracted that support.[128]

Even beyond the difficulties of working with complex samples, automating forensic interpretation does not render it free of human error and subjectivity. For instance, Perlin has altered TrueAllele's source code more than twenty-five times.[129] Yet, Perlin has given no explanation about what has been altered or why,[130] and it is impossible to know whether those changes corrected undisclosed errors or inadvertently introduced new ones.[131] Moreover, as with alcohol breath test devices, TrueAllele and other probabilistic genotyping software are the product of human judgments about how to interpret complex data inputs.[132] As set forth above, probabilistic genotyping software rely on mathematical models to attempt "to account for the unpredictable behavior of DNA samples with low template or too many contributors."[133] But each such software package, in attempting to do the same thing, uses a somewhat different mathematical model or codes for that model differently.[134] The consequence is that these

---

[128] Order at 16, Ohio v. Shaw, No. CR-13-575691 (Ohio Ct. Com. Pl. Oct. 10, 2014) (describing testimony by expert Dr. Ranjit Chakraborty that TrueAllele no longer had wide acceptance in his field and that he believed its applications for cases with closed sources and unknown application of variables still needed to be worked out). Chakraborty served as a member of the Scientific Working Group on DNA Analysis Methods (SWGDAM), which establishes national guidelines for forensic laboratories in the United States. Katherine L. Moss, Note, *The Admissibility of TrueAllele: A Computerized Interpretation System*, 72 WASH. & LEE L. REV. 1033, 1069 (2015). Chakraborty explained that the New York approval of which he had been a part "only extended to TrueAllele testing a higher quantity of DNA from a single source." *Id.* Moreover, Chakraborty asserted that "an independent party could not recreate or validate TrueAllele results without the source code." *Id.* at 1070.

[129] Roth, *supra* note 11, at 1273.

[130] *Id.*

[131] *See supra* text accompanying note 84.

[132] *See* MURPHY, *supra* note 8, at 97–98 (explaining that this type of software reflects how scientists and statisticians understand complex samples to behave, and that different software packages give weight to different factors and consequently may produce different results).

[133] *Id.* at 97.

[134] *See* PCAST REPORT, *supra* note 17, at 79 n. 211 ("Some programs use discrete (semi-continuous) methods, which use only allele information in conjunction with probabilities of allelic dropout and dropin, while other programs use continuous methods, which also incorporate information about peak height and other information. Within these two classes, the programs differ with respect to how they use the information. Some of the methods involve making assumptions about the number of individuals contributing to the DNA profile, and use this information to clean up noise (such as 'stutter' in DNA profiles)."); *see also* MURPHY, *supra* note 8, at 97 (software packages rely on mathematical models that "differ in their details, and as a result the predictions they make as regard the same piece of evidence may differ as well"); Roth, *supra* note 20, at 1996 ("Even if a programmer is not 'biased' in the sense of making choices to further a preconceived goal, her analytically controversial choices can affect the accuracy of the machine's scores and estimates. For example, in the DNA context, programmers have the power to set thresholds for what to count as a true genetic marker versus noise in determining which markers to report on the graphs used in determining a match."); Wexler, *supra* note

supposedly "entirely objective"[135] tools, when tested side by side, sometimes yield different results.[136]

The President's Council of Advisors on Science and Technology concluded that probabilistic genotyping represents a significant and welcome advance in the science.[137] But it also urged caution and study when making use of these new tools.[138] Unfortunately, Perlin's persistent and vociferous assertions of trade secrecy surrounding TrueAllele make study more difficult and caution more urgent.

As experience with alcohol breath test devices and probabilistic genotyping software make plain, algorithmic tools for generating crucial evidence of guilt or innocence are multiplying and taking on increased importance. Where these tools are privately developed and shielded by assertions of trade secrecy, however, reliability and validity may be difficult, if not impossible, to verify. In the few cases in which courts have compelled disclosure of private source code for alcohol breath test devices, reviewers identified significant errors in almost every instance.[139] In the one instance in which a court has compelled source code disclosure of probabilistic genotyping software, the State shortly thereafter abandoned use of that tool.[140] The lack of broader access to source code—particularly for probabilistic genotyping software, about which scientific experts have expressed doubts regarding validity and reliability—is therefore deeply troubling.

10, at 23 ("[S]oftware 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.").

[135] Perlin Letter, *supra* note 95, at 3.

[136] *See, e.g.*, MURPHY, *supra* note 8, at 97 ("These models differ in their details, and as a result the predictions they make as regard the same piece of evidence may differ as well."); PCAST REPORT, *supra* note 17, at 79 n.212 (describing an ongoing case in which STRmix and TrueAllele gave conflicting results); Roth, *supra* note 11, at 1273–74 ("[I]n conference simulations involving hypothetical mixtures, TrueAllele and several competing programs have come to different results in terms of guessing mixture ratios."); Wexler, *supra* note 10, at 23–24 ("Competing software programs have been found to produce divergent results from identical test samples. In a recent child homicide case, two software programs reached different conclusions regarding whether a defendant's DNA was included in a crime scene sample." (citations omitted)).

[137] PCAST REPORT, *supra* note 17.

[138] *Id.* ("However, [these probabilistic genotyping software programs] still require careful scrutiny to determine (1) whether the methods are scientifically valid, including defining the limitations on their reliability (that is, the circumstances in which they may yield unreliable results) and (2) whether the software correctly implements the methods."); *id.* ("Appropriate evaluation of the proposed methods should consist of studies by multiple groups, *not associated with the software developers*, that investigate the performance and define the limitations of programs by testing them on a wide range of mixtures with different properties.").

[139] *See supra* notes 79–88 and accompanying text.

[140] Kirchner, *Traces of Crime*, *supra* note 91 ("Earlier this year, the lab shelved [probabilistic genotyping software] and replaced [it] with newer, more broadly used technology.").

C. Secrecy in Sentencing

Finally, privately developed criminal justice algorithms, shielded from disclosure by assertions of trade secret protection, have extended their reach even into criminal sentencing. Most prominently, courts have begun to make sentencing determinations based, at least in part, on recidivism scores generated by software whose weights and measures are, once again, not disclosed on trade secret grounds.[141]

In July 2016, *State v. Loomis* became the first appellate case to address the relationship between asserted private trade secret protection and due process principles in sentencing.[142] In that case, Eric Loomis pled guilty to fleeing the police and driving a stolen car.[143] The trial court's pre-sentence report included a recidivism risk score generated by a program called COMPAS, and Loomis was deemed at high risk of committing another crime.[144] Citing Loomis's COMPAS score, the court sentenced Loomis to six years of imprisonment.[145] The Wisconsin Supreme Court affirmed that sentence.[146] In so doing, the court rejected Loomis's argument that a sentence based on a COMPAS score violates due process "because the proprietary nature of COMPAS prevents defendants from challenging the COMPAS assessment's scientific validity."[147] So long as the COMPAS score is not the only factor on which a judge relies at sentencing, the Wisconsin Supreme Court has sanctioned the use of such scores in deciding whether and for how long a defendant should be incarcerated.[148]

COMPAS, a privately developed proprietary tool owned and sold by Northpointe, Inc., is among the most widely used recidivism risk

---

[141] *E.g.*, State v. Loomis, 881 N.W.2d 749 (Wis. 2016), *cert. denied*, 137 S. Ct. 2290 (2017).

[142] *See id.*; U.S. *Loomis* Brief, *supra* note 15, at *22 ("The United States is not aware of any federal court of appeals or state court of last resort, other than the Wisconsin Supreme Court, that has confronted the federal due process issues that petitioner raises here.").

[143] *Loomis*, 881 N.W.2d at 754.

[144] *Id.* at 754–55; Ethan Chiel, *Secret Algorithms that Predict Future Criminals Get a Thumbs Up from Wisconsin Supreme Court*, FUSION (July 27, 2016), http://fusion.net/story/330672/algorithms-recidivism-loomis-wisconsin-court [https://perma.cc/73ZZ-X7PQ].

[145] Chiel, *supra* note 144.

[146] *Loomis*, 881 N.W.2d at 772.

[147] *Id.* at 753. Loomis also argued that sentencing based on a COMPAS score violates due process "because COMPAS assessments take gender into account." *Id.* The Wisconsin Supreme Court rejected this argument as well.

[148] *Id.* at 753 ("We determine that because the circuit court explained that its consideration of the COMPAS risk scores was supported by other independent factors, its use was not determinative in deciding whether Loomis could be supervised safely and effectively in the community. Therefore, the circuit court did not erroneously exercise its discretion.").

assessment algorithms in the United States.[149] COMPAS generates recidivism scores based principally on an interview with a defendant, as well as information recorded in the defendant's criminal file.[150] COMPAS is designed to measure both "static" variables, like a defendant's age at first arrest and family criminal history, and "dynamic variables," including personal beliefs and criminal associates.[151] After analyzing these data, COMPAS generates three risk scores, one each for "pretrial recidivism," "general recidivism," and "violent recidivism,"[152] which are reported on a 10-point bar chart.[153] That score is designed to represent a relative risk; that is, defendants with higher scores are deemed at higher risk of reoffending than other individuals in the same "norm group."[154]

Critically, defendants, defense counsel, departments of corrections, and courts who make use of COMPAS scores do not know how those scores are generated.[155] That is, although Northpointe has disclosed the 137-question survey that provides informational input for its program, it has refused to disclose how that information is used or weighted to arrive at a particular recidivism risk score.[156] This is because Northpointe, which

[149] Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/4CXA-Z5VK]. In addition to COMPAS, "[t]here are dozens of these risk assessment algorithms in use. Many states have built their own assessments, and several academics have written tools. There are also two leading nationwide tools offered by commercial vendors," of which COMPAS is one. Jeff Larson et al., *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm [https://perma.cc/Y9FF-EJHV]. Not all of these tools are shrouded by trade secrecy; indeed, several states have "develop[ed] and validat[ed] publicly available risk-assessment measures for consideration at sentencing." U.S. *Loomis* Brief, *supra* note 15, at *17 n. 5.

[150] *Loomis*, 881 N.W.2d at 754, 761 (describing Northpointe's explanation about the information inputs used to generate COMPAS scores).

[151] *See id.* at 761; Katherine Freeman, Note, *Algorithmic Injustice: How the Wisconsin Supreme Court Failed To Protect Due Process Rights in* State v. Loomis, 18 N.C. J.L. & TECH. ONLINE 75, 79, 92 (2016).

[152] *Loomis*, 881 N.W.2d at 754.

[153] *Id.*; Freeman, *supra* note 151, at 81.

[154] *See* Freeman, *supra* note 151, at 81–82; *see also Loomis*, 881 N.W.2d at 754. Northpointe has identified eight norm subgroups: "(1) male prison/parole, (2) male jail, (3) male probation, (4) male composite, (5) female prison/parole, (6) female jail, (7) female probation, and (8) female composite." Freeman, *supra* note 151, at 81 (quoting NORTHPOINTE, PRACTITIONER'S GUIDE TO COMPAS CORE 11 (2015), http://www.northpointeinc.com/files/technical_documents/Practitioners-Guide-COMPAS-Core-_031915.pdf [https://perma.cc/SGZ2-ZVAV]).

[155] *Loomis*, 881 N.W.2d at 761 ("[Northpointe] does not disclose how the risk scores are determined or how the factors are weighed."); Chiel, *supra* note 144 ("The Wisconsin Supreme Court doesn't care that the software is considered a proprietary trade secret, because the program's 'Practitioner Guide' includes some of the types of data that are part of the assessment . . . . In other words, what's relevant according to the court is knowing what goes in, not how it's weighted.").

[156] *See Loomis*, 881 N.W.2d at 761; Freeman, *supra* note 151, at 80 (describing the survey).

created and distributes COMPAS, claims that COMPAS is proprietary and a trade secret.[157] As in cases involving TrueAllele, the Intoxilyzer, and Harris's family of stingray technology, trade secret assertion obscures significant information about how data intended to inform criminal justice processes has been generated.

That secrecy affects not only defendants and their counsel but also the courts whose sentences COMPAS scores may inform. Northpointe's assertion of trade secret protection has left each of these criminal justice participants similarly in the dark. As one judge observed in Loomis's case, "this court's lack of understanding of COMPAS was a significant problem in the instant case. At oral argument, the court repeatedly questioned both the State's and defendant's counsel about how COMPAS works. Few answers were available."[158]

Northpointe's secrecy may be of further concern, as COMPAS's use in cases like Loomis's applies the software beyond its intended use. COMPAS was originally designed to aid the Department of Corrections in making placement decisions, managing offenders, and planning treatment.[159] The pre-sentence report in Loomis's case specifically instructed, "risk scores are not intended to determine the severity of the sentence or whether an offender is incarcerated."[160] Yet, as Loomis's case illustrates, judges have based a sentence of imprisonment, or the length of such a sentence, at least in part on the scores that COMPAS generates.

To be sure, the use of data and algorithms in sentencing may not always be problematic. Draft revisions to the Model Penal Code, for instance, "encourage[e] the use of actuarial risk-assessment tools at sentencing."[161] Indeed, algorithmic tools may "offer better predictions of future behavior than the clinical judgments of treatment professionals such as psychiatrists and psychologists, or the intuitions of criminal-justice professionals such as judges and probation officers."[162]

But better predictions are only possible if such tools are, as the revisions note, "well-designed."[163] Unfortunately, there may be good reason

---

[157] *Loomis*, 881 N.W.2d at 761("Northpointe, Inc., the developer of COMPAS, considers COMPAS a proprietary instrument and a trade secret.").

[158] *Id.* at 774 (Abrahamson, J., concurring).

[159] *Id.* at 754 (citing NORTHPOINTE, PRACTITIONER'S GUIDE TO COMPAS CORE 1 (Mar. 19, 2015), http://www.northpointeinc.com/files/technicaldocuments/Practitioners–Guide–COMPAS–Core–031915.pdf [https://perma.cc/SGZ2-ZVAV]).

[160] *Id.* at 755 (emphasis omitted).

[161] MODEL PENAL CODE § 6.03 (Tentative Draft No. 3 2014) (summarizing MODEL PENAL CODE § 6B:09(2) (Tentative Draft No. 2 2011)).

[162] *Id.*

[163] *Id.*

to question COMPAS's design. Emerging evidence indicates that COMPAS is racially biased, generating higher recidivism scores for blacks than for similarly situated whites.[164] In one recent study, ProPublica authors analyzed the COMPAS scores for more than 7,000 people arrested in 2013 and 2014, comparing these scores to the actual incidence of recidivism for those individuals.[165] The authors concluded that COMPAS scores were unreliable predictors of violent crime in particular: "Only 20 percent of the people predicted to commit violent crimes actually went on to do so."[166] Perhaps more troubling, "[t]he formula was particularly likely to falsely flag black defendants as future criminals, wrongly labeling them this way at almost twice the rate as white defendants," while "[w]hite defendants were mislabeled as low risk more often than black defendants."[167] Determining how these algorithmic disparities arise is difficult.[168] It is impossible to do so when the formula that undergirds that disparity is hidden from view. Yet that is precisely what Northpointe's assertion of trade secret protection does.

II. THE HARMS OF CRIMINAL JUSTICE SECRECY

Reliance on trade secrecy in the development of criminal justice tools imposes real harms on the criminal justice process. Those harms are of both practical and potentially constitutional dimensions. This Part first explains why access to source code is often essential to confirm the validity and reliability of criminal justice technologies—and why alternative mechanisms for ensuring these features are likely to fall short in this arena. It next identifies two additional practical harms of reliance on trade secrecy in this arena: diminished public confidence in algorithmic quality and less innovation to create better algorithms. Finally, this Part briefly explores the constitutional costs of criminal justice secrecy.

A. The Importance of Access to Code

Source code secrecy surrounding criminal justice algorithms imposes significant practical harms on the criminal justice system. Chief among

---

[164] *See Loomis*, 881 N.W.2d at 763 ("[T]here is concern that risk assessment tools may disproportionately classify minority offenders as higher risk, often due to factors that may be outside their control, such as familial background and education."); Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/KL7Q-FL25].

[165] Angwin et al., *supra* note 164.

[166] *Id.*

[167] *Id.*

[168] At a minimum, Angwin and other authors concluded that this disparity was not due to "defendants' prior crimes or the type of crimes they were arrested for." *Id.*

these is that such secrecy may give rise to worse algorithms by impeding effective oversight of the validity and reliability of these tools.

Secret code is often less good code. Outside experts repeatedly have identified algorithmic weaknesses and outright errors in proprietary source code revealed in litigation. For instance, outside expert review of the source code of New York City's FST concluded that "the correctness of the behavior of the FST software should be seriously questioned."[169] Similarly, access to the source code for an Intoxilyzer model in use in Minnesota revealed that a "deficient sample" report could indicate a software failure.[170] Based on that information, the Minnesota Supreme Court affirmed the categorical exclusion of such reports, absent other evidence indicating that a software error was not at fault.[171] When source code review of Draeger's Alcotest device in New Jersey revealed that catastrophic error detection was disabled, the state supreme court required its correction.[172] Indeed, the New Jersey Supreme Court required other firmware changes, including that only the manufacturer be able to alter the device software and excluding state "coordinators."[173]

More broadly, research indicates that open-source software—software whose source code is freely available to anyone—has fewer errors than proprietary software.[174] "[P]ublic access to open source codes" thus

---

[169] *See* Kirchner, *supra* note 112. Relatedly, a partial inspection of the source code of STRmix, another popular probabilistic genotyping program, revealed a "minor miscode"—one that affected the reported likelihood of a DNA match in at least sixty cases. David Murray, *Queensland Authorities Confirm 'Miscode' Affects DNA Evidence in Criminal Cases*, THE COURIER-MAIL (Mar. 20, 2015), http://www.couriermail.com.au/news/queensland/queensland-authorities-confirm-miscode-affects-dna-evidence-in-criminal-cases/news-story/833c580d3f1c59039efd1a2ef55af92b [https://perma.cc/SA2X-85LF]; *see also* Chessman, *supra* note 16, at 188–89 (discussing this case); Rebecca Wexler, *Convicted by Code*, SLATE (Oct. 6, 2015), http://www.slate.com/blogs/future_tense/2015/10/06/defendants_should_be_able_to_inspect_software_code_used_in_forensics.html [https://perma.cc/Z37Q-UHVU] ("Coding errors have been found to alter DNA likelihood ratios by a factor of 10, causing prosecutors in Australia to replace 24 expert witness statements in criminal cases.").

[170] *See In re* Source Code Evidentiary Hearings in Implied Consent Matters, 816 N.W.2d 525, 543 (Minn. 2012).

[171] *Id.*

[172] *See* State v. Chun, 943 A.2d 114, 159 (N.J. 2008) ("[W]e direct that the State arrange to have the software corrected to re-enable the catastrophic error detection feature.").

[173] *Id.* at 160–61.

[174] *See* SYNOPSYS, INC., COVERITY® SCAN OPEN SOURCE REPORT 2014, at 4 (2015), http://go.coverity.com/rs/157-LQW-289/images/2014-Coverity-Scan-Report.pdf [https://perma.cc/M7GU-RUQB] (reporting that "[o]pen source software has a considerably lower defect density than commercial software"); Steven J. Vaughan-Nichols, *Coverity Finds Open Source Software Quality Better than Proprietary Code*, ZDNET (Apr. 16, 2014), http://www.zdnet.com/article/coverity-finds-open-source-software-quality-better-than-proprietary-code [perma.cc/R9CY-V2Q7] (discussing Coverity's 2013 report).

"facilitates further investigation and validation of technology."[175] Thus, access to source code is often essential for defendants to verify that the algorithms that have led to their arrest, conviction, or sentence operate as intended.

Other mechanisms intended to ensure the accuracy, validity, and reliability of criminal justice algorithms fall short in the absence of outside source code review.[176] For instance, one group of authors has counseled reliance on validation studies to ensure accuracy and fairness.[177] Validation studies are empirical tests designed to establish that the software or device functions as claimed.[178] For these scholars, "it is significantly less important for judges to pry open this black box than it is for them to establish whether its operation has been tested under conditions similar to those at issue in court."[179]

But reliance on validation studies in place of source code access, rather than alongside it, is likely insufficient to verify that software has performed as its designer claims. In part, this stems from the limited verification that can be gleaned from "black-box testing"—testing that "considers only the inputs and outputs of a system or component."[180] As technologists have explained, "[c]omputer scientists . . . have shown that black-box evaluation of systems is the least powerful of a set of available methods for understanding and verifying system behavior."[181] More powerful and effective is "white-box testing," in which "the person doing a test can see the system's code and uses that knowledge to more effectively search for bugs."[182] Accordingly, researchers have concluded that, to enable

---

[175] Freeman, *supra* note 151, at 102.

[176] In some instances, like the use of a stingray device to locate and arrest an individual, concerns are less about accuracy and reliability than about privacy. Moreover, concerns about nondisclosure of stingray use even to the judges themselves are orthogonal to the accuracy and reliability issues discussed in here. For more on these concerns, see *infra* Section II.B. Where a prosecutor seeks to introduce at trial information generated by a stingray device, however, the same concerns about the accuracy, reliability, and fairness of the source code at issue may arise. *See infra* note 216.

[177] *See, e.g.*, Imwinkelried, *supra* note 8, at 120 (concluding that it is "correct—sometimes" that "a review of available validation studies allows an opponent to determine whether a computer program contains deficiencies without access to the source code" (internal quotation marks omitted)); Jennifer Mnookin, *Of Black Boxes, Instruments, and Experts: Testing the Validity of Forensic Science*, 5 EPISTEME 343, 344–45 (2008) (arguing that, for admissibility, the "inquiry should focus first and foremost on validation—or, more precisely, on the extent to which appropriate empirical testing supports the claims made by the expert—rather than on whether the expert (or, more broadly, the community of experts) can offer a plausible account of the underlying mechanism at work").

[178] *See* Mnookin, *supra* note 177, at 344.

[179] *Id.* at 344–45.

[180] Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PENN. L. REV. 633, 650 (2017).

[181] *Id.* at 661.

[182] *Id.*

effective scientific inquiry, "anything less than the release of source programs is intolerable for results that depend on computation."[183]

The limitations on the insight gleaned from validation testing are exacerbated in the criminal justice arena by the nature of the validation studies on which software developers have principally relied. Many of these validation studies are the product of in-house testing. Of the journal articles touted on Cybergenetics's website, all but two include Perlin—TrueAllele's creator and Cybergenetics's Chief Scientific and Executive Officer—as an author.[184] Similarly, Northpointe's own employees conducted most of the validation studies on which Northpointe has relied in advocating for COMPAS's accuracy.[185] By contrast, the President's Council of Advisors on Science and Technology, in its report on forensic science in criminal courts, recommended that "[a]ppropriate evaluation of the proposed methods should consist of studies by multiple groups, *not associated with the software developers*."[186]

Moreover, existing validation studies are often the product of "idealized conditions unrepresentative of the challenges of real casework."[187] For example, advanced algorithmic tools, like probabilistic genotyping software, are most likely to be called upon "in cases involving less-than-ideal conditions—degraded or highly complex mixtures difficult for human analysts to interpret."[188] Thus, validation studies are not a viable alternative to outside source code review for ensuring reliability and accountability; rather, validation alongside outside source code review is needed.

Building accountability into digital design also is unlikely to be a practical solution to ensuring accuracy and reliability in the absence of outside source code review—at the very least with respect to privately developed technologies already in use. Proponents of accountability by design argue that, rather than merely disclose source code for outside

---

[183] Darrel C. Ince et al., *The Case for Open Computer Programs*, 482 NATURE 485, 485 (2012).

[184] *See* CYBERGENETICS, *Publications*, https://www.cybgen.com/information/publication/page.shtml [http://perma.cc/3YYH-Z8Y9].

[185] *See* Freeman, *supra* note 151, at 82–83.

[186] PCAST REPORT, *supra* note 17, at 79. Accordingly, many current validation studies may fail to satisfy even those scholars most predisposed to accept them, as even those who would accept validation studies alone correctly note that such acceptance is a function of the studies' quality. *See* Imwinkelried, *supra* note 8, at 120.

[187] Roth, *supra* note 20, at 2033.

[188] *Id.* at 1982. Even scholars who are inclined, in principle, to support refusals to disclose source code for criminal justice algorithms recognize that disclosure becomes more necessary as "the test conditions and the conditions in the instant case" increasingly diverge. Imwinkelried, *supra* note 8, at 120; *see also id.* at 123–24 (proposing a "range of validation" for assessing the sufficiency of validation studies).

review, software designers should "publish[] commitments and us[e] zero-knowledge proofs to ensure that commitments correspond to the system's decisionmaking actions."[189] For these technologists, neither source code transparency nor validation studies are sufficient to ensure accuracy and fairness.[190] Designing for accountability, by contrast, "can enable stakeholders to reach accountability goals that could not be achieved by imposing new transparency requirements on existing system designs."[191]

But while designing for accountability might be a worthy aspiration, it is unlikely to mitigate the need for source code access in the near or medium term. There is little evidence that existing tools have adopted such measures. More stubbornly, there is often a lack of consensus about what decision-guiding properties criminal justice algorithms ought to adopt. For instance, as set forth above, scientists and software developers have yet to reach agreement about which mathematical model best resolves complex DNA mixtures.[192] Defining a usable principle of "fairness" in sentencing is likely to be every bit as challenging, if not more so.[193] Thus, it is far from clear that designing for accountability is a practical solution, particularly for tools already in use like stingrays, the Intoxilyzer, TrueAllele, and COMPAS.

Significantly, even the technologists who eschew calls for source code transparency ultimately make one themselves. In their final conclusions, these authors recommend that policymakers "incentivize nongovernmental actors to use" techniques of designing for accountability.[194] The stick for not doing so? "[R]equiring transparency—at least to courts—of code and inputs if they do not employ such technical tools."[195] In other words, outside access to source code is and remains a key component of ensuring the accuracy, validity, and reliability of criminal justice algorithms.

---

[189] Kroll et al., *supra* note 180, at 682. "A zero-knowledge proof is a cryptographic tool that allows a decisionmaker, as part of a cryptographic commitment, to prove that the decision policy that was actually used (or the particular decision reached in a certain case) has a certain property, but without having to reveal either how that property is known or what the decision policy actually is." *Id.* at 668.

[190] *Id.* at 646–53; *see id.* at 657–60 (2017) (discussing "Transparency and Its Limits" and describing "transparency of the source code as well as inputs and outputs for the relevant decisions" as a "naive solution to the problem of verifying procedural regularity").

[191] *Id.* at 637.

[192] *See supra* notes 133–136 and accompanying text.

[193] *See* Kroll et al., *supra* note 189, at 696.

[194] *Id.* at 705.

[195] *Id.*

B. Other Practical Harms of Criminal Justice Secrecy

In addition to undermining the overall quality of code, shielding source code from outside scrutiny may also inflict other practical harms on the criminal justice system. For one thing, source code secrecy can undermine public confidence in that quality. A lack of confidence is understandable; in recent years, outside review has exposed numerous previously well-regarded forensic sciences as unreliable or scientifically unsound.[196] Forensic arson investigation, bite mark analysis, bullet lead examination, hair analysis, and even fingerprint analysis have been criticized or even discontinued in light of a lack of scientific evidence or reliability.[197] It is similarly unclear whether recidivism risk statistics spring from a scientifically sound basis.[198] And there is little reason to believe that new methods of breath or DNA analysis, though originating from sound science, are free from methodological or coding error.

Insofar as access to source code is significant in assuring the validity and reliability of such analyses—and it is[199]—lack of access to source code may reasonably undermine public and judicial confidence in these criminal justice tools. By contrast, source code access can increase judicial and public confidence in otherwise abstruse technology. When the New Jersey Supreme Court approved continued use of the state's alcohol breath test devices following full review of the device's source code, the court emphasized that its "evaluation of the exhaustive record relating to the source code leaves us confident that its errors have been revealed."[200]

Finally, lack of source code access may inhibit innovation of better software and other criminal justice tools. As a general matter, when it comes to incentives for innovation, American law has typically preferred information-forcing policies, like patents, over information-shielding ones, like trade secrecy.[201] Among other benefits provided by information-forcing

---

[196] *See* NAS REPORT, *supra* note 115, at 8 ("[T]here is a notable dearth of peer-reviewed, published studies establishing the scientific bases and validity of many forensic methods."); Ram, *supra* note 114, at 427.

[197] Ram, *supra* note 114, at 427–28 (summarizing the state of forensic science).

[198] *See* Angwin et al., *supra* note 164 (finding that risk scores "proved remarkably unreliable in forecasting violent crime: Only 20 percent of the people predicted to commit violent crimes actually went on to do so").

[199] *See supra* Section II.A.

[200] State v. Chun, 943 A.2d 114, 151, 160 (N.J. 2008).

[201] *See* Price, *supra* note 23, at 1779–80. The disclosure requirement for patents, compared with the secrecy required for trade secret protection, is not the only way in which patent and trade secret law differ. *See id.* at 1774–83; *infra* Section III.A. Indeed, scholars debate whether disclosure can justify the monopoly rights that the patent system creates. *Compare* Jeanne C. Fromer, *Patent Disclosure*, 94 IOWA L. REV. 539, 542 (2009) (arguing for the "centrality in the patent system" of disclosure), *with* Mark A. Lemley, *The Myth of the Sole Inventor*, 110 MICH. L. REV. 709, 745 (2012) ("Disclosure

policies, disclosure is thought to spur follow-on innovation.[202] Far less innovation can flow from secret information, like the proprietary source code that Harris, CMI, Cybergenetics, and Northpointe are at pains to protect. Thus, criminal justice secrecy not only inhibits a defendant from ensuring that he is not wrongly identified, convicted, or sentenced; it may "prevent[] the technology from potentially advancing."[203]

In sum, lack of access to source code yields lower quality code, lower confidence in that code, and less follow-on innovation to create better code.

C. Constitutional Concerns About Criminal Justice Secrecy

Trade secret assertion in the context of criminal justice tools also raises constitutional concerns. Secrecy surrounding the existence, use, and function of criminal justice tools interferes with defendants' and courts' efforts to ensure that the government does not engage in unreasonable searches. Such secrecy is also at least in tension with, if not in violation of, defendants' ability to vindicate their due process interests throughout the criminal justice process, as well as their confrontation rights at trial. A comprehensive constitutional argument, much less a series of them, is beyond the scope of this Article. Indeed, each of these constitutional concerns could occupy an entire article.[204] For present purposes, it is enough to conclude that trade secrecy here treads close to significant constitutional principles, such that, all else being equal, less trade secrecy would be better.

1. Fourth Amendment Concerns

As an initial matter, the undisclosed use of stingray devices in criminal investigations raises concerns under the Fourth Amendment's protection against unreasonable searches and seizures.[205] As Kerron Andrews's case demonstrates, pursuant to nondisclosure agreements, law enforcement officers have intentionally concealed their use of stingray

theory cannot . . . support the modern patent system."). On the availability (or lack thereof) of patent protection for software algorithms, see *infra* Section III.A.

[202] Katherine J. Strandburg, *What Does the Public Get? Experimental Use and the Patent Bargain*, 2004 WIS. L. REV. 81, 112. This, too, is a subject of scholarly debate and criticism. *See* Price, *supra* note 23, at 1781–83; Benjamin N. Roin, Note, *The Disclosure Function of the Patent System (or Lack Thereof)*, 118 HARV. L. REV. 2007, 2017–23 (2005).

[203] Freeman, *supra* note 151, at 103.

[204] *Cf.* Roth, *supra* note 20, at 2040 ("briefly" addressing the Confrontation Clause and criminal justice algorithms, while observing that separate Article-length treatment is warranted).

[205] U.S. CONST. amend. IV. The Fourth Amendment does not require a state to obtain a warrant before compelling an individual to submit to an alcohol breath test. *See* Birchfield v. North Dakota, 136 S. Ct. 2160, 2185 (2016) (concluding that a warrant is not required to conduct an alcohol breath test, which "may be administered as a search incident to a lawful arrest for drunk driving").

devices not only from defendants and defense counsel but also from courts.[206] Rather than disclose their intent to use a stingray device, police in Andrews's case sought authorization for a pen register, which imposes different and less stringent requirements than those for a warrant.[207] But as the Maryland Court of Special Appeals concluded, a stingray is meaningfully different and more invasive than a pen register, and thus a warrant was required.[208] The court expressed particular concern that police obfuscated their true intent in seeking authorization for a pen register while intending to deploy the more invasive stingray device.[209]

In that case, secrecy was not itself a constitutional violation; rather, secrecy created circumstances in which a constitutional violation might escape review because it is hidden from view. As the court emphasized, the secrecy required under the Baltimore police department's nondisclosure agreement "prevents the court from exercising its fundamental duties under the Constitution."[210] The Fourth Amendment's requirement that searches be "reasonable" calls for balancing an individual's right to personal security against the public interest.[211] Nondisclosure agreements, driven by assertions of trade secrecy, "obstruct[] the court's ability to make the necessary constitutional appraisal" by preventing law enforcement officers from revealing significant information about "the functionality of the surveillance device and the range of information potentially revealed by its use."[212]

2. Due Process Concerns

Moving beyond the investigative uses of trade secret-protected technologies, the use of such technologies to generate evidence admissible at trial also generates tensions with the Due Process Clauses of the Fifth and Fourteenth Amendments. These constitutional provisions guarantee to every individual the right to "due process of law."[213] The Supreme Court has explained that this guarantee affords "criminal defendants 'a meaningful opportunity to present a complete defense.'"[214] This right

---

206 State v. Andrews, 134 A.3d 324, 329 (Md. Ct. Spec. App. 2016).

207 *Id.* at 354, 360.

208 *Id.* at 327, 360.

209 *Id.* at 360 ("[W]e are troubled that the application for a pen register\trap & trace order did not fully apprise the circuit court judge from whom it was sought of the information that it would yield.").

210 *Id.* at 338.

211 *Id.*

212 *Id.*

213 U.S. CONST. amends. V, XIV.

214 Crane v. Kentucky, 476 U.S. 683, 690 (1986) (quoting California v. Trombetta, 467 U.S. 479, 485 (1984)).

encompasses a defendant's ability to impeach witnesses and evidence that the state may introduce against him.[215] Where that evidence results from the use of stingray[216] or breath test devices, or from analysis by probabilistic genotyping software, the surest and perhaps only way to thoroughly cross examine such evidence may be by reviewing the source code of that criminal justice tool.[217] Indeed, at least one federal judge has recognized the essential role of adequate discovery of forensic science tools in ensuring a fair trial.[218] In a letter resigning from the National Commission on Forensic Science, Judge Jed Rakoff explained, "if an adversary does not know in advance sufficient information about the forensic expert and the methodological and evidentiary bases for that expert's opinions, the testimony of the expert is nothing more than trial by ambush."[219]

To be sure, the Supreme Court has emphasized that the "accused does not have an unfettered right to offer evidence that is . . . privileged."[220] But the Court has also, in significant circumstances, disregarded assertions of privilege in vindicating due process principles.[221] In ordering the President of the United States to turn over secret White House recordings, the Supreme Court explained that allowing the President to "withhold evidence that is demonstrably relevant in a criminal trial" based on the President's

---

[215] *Cf.* Strickler v. Greene, 527 U.S. 263, 280 (1999) (explaining that the government's obligations under *Brady* "encompass[] impeachment evidence as well as exculpatory evidence"); Brady v. Maryland, 373 U.S. 83, 87 (1963) (recognizing that, under the Due Process Clause, prosecutors have a constitutional obligation to preserve and give to a defendant material evidence pertinent to his defense).

[216] Although the typical use of a stingray device implicates the Fourth Amendment's protection against unreasonable searches and seizures, *see supra* notes 205–212, due process principles would be implicated if the government sought to introduce information generated by a stingray device into evidence for its truth. For instance, if the government sought to use stingray-generated information placing the defendant at a particular location at a particular time to establish the defendant's location as a matter of fact, this would implicate the defendant's trial rights. Such use might also implicate the Confrontation Clause, for the reasons discussed *infra*, notes 237–253.

[217] *See supra* Section II.A.

[218] *See* Jed S. Rakoff, *Full Text: Judge's Protest Resignation Letter*, WASH. POST (Jan. 29, 2015), https://www.washingtonpost.com/local/full-text-judges-protest-resignation-letter/2015/01/29/41659da6-a7e1-11e4-a2b2-776095f393b2_story.html [https://perma.cc/RJP5-U863].

[219] *Id.* Judge Rakoff resigned from the Commission after he was informed that "the subject of pre-trial forensic discovery—i.e., the extent to which information regarding forensic science experts and their data, opinions, methodologies, etc., should be disclosed before they testify in court—is beyond the 'scope' of the Commission's business and therefore cannot properly be the subject of Commission reports or discussions in any respect." *Id.* Shortly after this resignation, the U.S. Department of Justice reversed that determination as to the scope of the Commission's work, and Judge Rakoff rejoined the Commission. Spencer S. Hsu, *Judge Rakoff Returns to Forensic Panel After Justice Department Backs Off Decision*, WASH. POST (Jan. 30, 2015), https://www.washingtonpost.com/local/crime/in-reversal-doj-lets-forensic-panel-suggest-trial-rule-changes-after-us-judge-protests/2015/01/30/2f031d9e-a89c-11e4-a2b2-776095f393b2_story.html [https://perma.cc/5UC8-PG54].

[220] Montana v. Egelhoff, 518 U.S. 37, 42 (1996) (quotation marks and alterations omitted).

[221] United States v. Nixon, 418 U.S. 683, 713 (1974).

asserted need for confidentiality in presidential communications "would cut deeply into the guarantee of due process of law and gravely impair the basic function of the courts."[222] Of course, in *Nixon*, it was the prosecutor who sought to compel disclosure of third-party privileged material.[223] But insofar as the Court in *Nixon* prioritized general due process principles over confidentiality, its conclusion must be all the more compelling where the specific constitutional criminal defense protections are at issue. Thus, "when the ground for asserting privilege as to subpoenaed materials sought for use in a criminal trial is based only on the generalized interest in confidentiality, it cannot prevail over the fundamental demands of due process of law in the fair administration of criminal justice."[224]

Moreover, even if a defendant's due process right to present a defense is insufficient to directly vindicate a defendant's request for source code access, that right makes plain the harms of trade secrecy in the criminal justice context. Absent an assertion of trade secret protection, a defendant would likely be able to access the source code necessary to present his defense.[225] It is the assertion of trade secret protection that threatens the defendant's right to present a defense, regardless of whether the due process clause would itself vindicate that right by surmounting the assertion of trade secrecy.

The Due Process Clause also establishes minimum fairness standards for sentencing.[226] The Supreme Court has made clear that due process guards against sentencing based on "materially false" information that a defendant has no effective "opportunity to correct."[227] The Court has similarly suggested that sentencing a defendant "on the basis of confidential information which is not disclosed to the defendant or his counsel" can run afoul of due process.[228] In *Gardner*, a plurality opinion concluded that due process will not abide a sentence "imposed, at least in

---

[222] *Id.* at 712.

[223] *Id.* at 686.

[224] *Id.* at 713.

[225] In some instances, independent bases for continued secrecy may exist. For a discussion of these alternative bases for nondisclosure and their prospects for success, see *infra* notes 401–404 and accompanying text.

[226] Gardner v. Florida, 430 U.S. 349, 358 (1977) (plurality opinion) ("[T]he sentencing process, as well as the trial itself, must satisfy the requirements of the Due Process Clause."); *see* Townsend v. Burke, 334 U.S. 736, 741 (1948) (invalidating a sentence because proceedings lacked due process).

[227] *Townsend*, 334 U.S. at 741.

[228] *Gardner*, 430 U.S. at 358.

part, on the basis of information which [the defendant] had no opportunity to deny or explain."[229]

In challenging Wisconsin's use of COMPAS in sentencing, Eric Loomis invoked *Gardner* to argue that shielding COMPAS's formula for weighting and calculating recidivism risk scores leads to sentences based, at least in part, on information a defendant has no "opportunity to correct" and "no opportunity to deny or explain."[230] The Wisconsin Supreme Court rejected this argument, concluding that disclosure of—and opportunity to correct, deny, or explain—the questions and answers entered into COMPAS largely suffices.[231]

But this misses the point. Although Northpointe discloses the informational input for its program, that is no guarantee that the scores that it produces based on its proprietary weighting of that information are valid. Due process is intended to ensure that a sentence derives from accurate facts. If a sentence is based, even in part, on a recidivism risk score determined by an unsound algorithm, that amounts to a sentence based on an inaccurate fact. The inability to ascertain the validity or reliability of the methodology underlying COMPAS's recidivism risk scores thus runs counter to this due process principle. As no less an authority than the Solicitor General of the United States has conceded, "a court's use of a risk assessment based on an undisclosed scoring methodology creates at least the possibility not only of scoring error, but of a flawed actuarial approach that a defendant cannot effectively counter through other types of evidence."[232] Indeed, the Solicitor General acknowledged that "[s]ome uses of an undisclosed risk-assessment algorithm might raise due process concerns."[233] For instance, were recidivism risk scores made a "part of a sentencing 'matrix'" or deemed to "establish a 'presumptive' term of imprisonment," this might well run afoul of the Due Process Clause.[234]

---

[229] *Id.* at 362; *see* State v. Loomis, 881 N.W.2d 749, 760 (Wis. 2016), *cert. denied*, 137 S. Ct. 2290 (2017). Though the Wisconsin Supreme Court has held explicitly that *Gardner*'s reasoning applies beyond capital cases, *see* State v. Skaff, 447 N.W.2d 84, 87 (Wis. Ct. App. 1989), the U.S. Supreme Court has not, *see* O'Dell v. Netherland, 521 U.S. 151, 162 (1997) (confining *Gardner* to a case concerned with Eighth Amendment limits in capital cases). *But see id.* at 173–75 (Stevens, J., dissenting) (criticizing the *O'Dell* majority as misreading *Gardner* and later cases accepting *Gardner*'s due process rationale).

[230] *Loomis*, 881 N.W.2d at 761.

[231] *Id.* at 761.

[232] U.S. *Loomis* Brief, *supra* note 15, at *17.

[233] *Id.* at *18.

[234] *Id.* The Solicitor General argued that Loomis's case did not present such concerns because, among other things, the sentence in that case "was not based—even in part—on undisclosed information." *Id.* at *15. That is, the Solicitor General argued that Loomis's sentence was not based, even in part, on the COMPAS scores appearing in his presentence report. This is a questionable reading

Once again, it is the assertion of trade secrecy that presses on this due process norm. As the Solicitor General observed in his brief, several states have avoided this due process difficulty "by developing and validating publicly available risk-assessment measures for consideration at sentencing."[235] That is, but for the assertion of source code secrecy, this due process concern would not arise.

3. Confrontation Concerns

Finally, the Constitution operationalizes its concern for fair trial procedures through a panoply of Sixth Amendment criminal defense rights.[236] Of these, the Confrontation Clause has received the most attention in this arena.[237] The Confrontation Clause affords a criminal defendant the right to be "confronted with the witnesses against him."[238] In a recent article, Professor Andrea Roth argues that "machine sources sometimes may, indeed, trigger a right of confrontation."[239] The Supreme Court has explained, "the principal evil at which the Confrontation Clause was directed was the civil-law mode of criminal procedure, and particularly its use of *ex parte* examinations as evidence against the accused."[240] Roth elaborates that a chief danger of such ex parte statements was that they were "impressive-looking" but "unconfrontable," leaving defendants with "little chance of disputing them."[241] Unfortunately, "[a]llowing the state to build or harness machines to render accusations, without also providing the defendant a constitutional right to test the credibility of those machine sources, resembles trial by ex parte affidavit."[242] A lab analyst or law enforcement officer reports the results of an algorithmic process, like an individual reading an ex parte affidavit into evidence.[243] That witness cannot speak to the underlying accuracy or reliability of the report they

---

of the sentencing court's decision. As discussed above, the sentencing court specifically cited Loomis's COMPAS score in imposing its sentence. *See* Chiel, *supra* note 144.

235 U.S. *Loomis* Brief, *supra* note 15, at *17 n.5.

236 U.S. CONST. amend. VI.

237 *See, e.g.*, Imwinkelried, *supra* note 8, at 118 ("The U.S. Supreme Court has held that in criminal cases, the defendant's right to attack the weight of the prosecution's evidence is of constitutional dimension under the Sixth Amendment Confrontation Clause."); Roth, *supra* note 20, at 2040–48 ("[M]achine sources sometimes may, indeed, trigger a right of confrontation."); Wexler, *supra* note 10, at 22 ("[S]cientific relevance is a floor not a ceiling to legal relevance."). The Confrontation Clause does not apply at sentencing. *See* Williams v. New York, 337 U.S. 241 (1949).

238 U.S. CONST. amend. VI.

239 Roth, *supra* note 20, at 2040.

240 Crawford v. Washington, 541 U.S. 36, 50 (2004).

241 Roth, *supra* note 20, at 2041.

242 *Id.* at 2043.

243 *Id.*

read. And yet that report, like an ex parte affidavit, is surely "impressive-looking."[244]

On this view, the defendant's right of confrontation should encompass the opportunity to impeach the machine source itself. Cross-examining a software developer is not a suitable substitute for examining the software source code itself because code will never exactly embody a developer's intent. As discussed above, errors may arise from coding mistakes and software rot of which the developer is unaware,[245] as well as from predictable false positive results.[246] Once again, assertions of trade secrecy conflict with constitutional principles, here the right of the accused to cross-examine his accusers.

The same result may flow from the Supreme Court's recent focus on "testimonial hearsay" as the key for the confrontation right to apply.[247] In *Crawford v. Washington*, the Court defined "testimony" as "[a] solemn declaration . . . made for the purpose of establishing or proving some fact."[248] Pursuant to that definition, the Court has held that a defendant has a near-sacrosanct right to cross examine the particular forensic analyst who certifies the results of a laboratory process.[249] More generally, statements are testimonial where they are made in response to police interrogation, where "the primary purpose of the interrogation is to establish or prove past events potentially relevant to later criminal prosecution."[250]

The results produced by criminal justice algorithms fall comfortably within the scope of this understanding of "testimonial." Such results are "solemn" and produced "for the purpose of establishing or proving some fact."[251] As they arise from law enforcement requests or direct use of criminal justice technologies, it makes sense to think of these results as the product of a kind of "police interrogation," the primary purpose of which is

---

[244] *Id.* at 2041.

[245] *See supra* notes 83–85 and accompanying text; *see also* Chessman, *supra* note 16, at 186–92 (identifying "structural sources of error" that may unintentionally cause software to be unreliable or faulty, including "accidental errors," "software updates to legacy code," and "software rot").

[246] *See supra* notes 81–83 and accompanying text.

[247] For recent cases focusing on the scope of "testimonial hearsay" for purposes of the Confrontation Clause, see Williams v. Illinois, 567 U.S. 50 (2012); Bullcoming v. New Mexico, 564 U.S. 647 (2011); Melendez-Diaz v. Massachusetts, 557 U.S. 305 (2009); Davis v. Washington, 547 U.S. 813 (2006); Crawford v. Washington, 541 U.S. 36 (2004).

[248] *Crawford*, 541 U.S. at 51.

[249] *See Bullcoming*, 564 U.S. at 652; *Melendez-Diaz*, 557 U.S. at 310–11. The Confrontation Clause does not apply, however, where an analyst testifies about forensic reports as the basis for an expert opinion and does not submit the reports themselves for their truth. *Williams*, 567 U.S. 50.

[250] *Davis*, 547 U.S. at 822.

[251] *Crawford*, 541 U.S. at 51.

to inform a criminal investigation and possible prosecution.[252] As Roth explains, "[i]f the point of targeting solemnity is to capture what is particularly abusive about the state purposely relying on impressive but unconfronted allegations of crime as a substitute for testimony, then machine sources would seem to be squarely implicated."[253] The result is that source code should be disclosed for purposes of cross-examination and impeachment. When assertions of trade secrecy prevent such disclosure, those assertions once again impose constitutional risks, if not outright harms.

* * *

Assertions of trade secrecy interfere with defendants' abilities to vindicate their due process and confrontation rights at trial and their due process interests at sentencing; they also hamstring defendants and courts alike in their efforts to ensure that the government does not engage in unreasonable searches. Regardless of whether these trade-secret-related difficulties rise to the level of independent constitutional violations, they make plain that trade secret assertion in the criminal justice context exists in tension with bedrock constitutional principles.

III. THE MANY TOOLS OF INNOVATION POLICY

In light of established and potential harms of criminal justice secrecy—both practical and constitutional—less trade secrecy and less deference to asserted trade secret status would be an improvement. Yet courts have largely declined to examine vigorously the assertions of trade secret protection in these criminal contexts.[254] Moreover, in rejecting requests for source code access, courts have often deferred to private developers' assertions of dire competitive harm should their asserted trade secret be revealed.[255] Law enforcement entities have worked hand in glove with private developers to shield criminal justice technologies from outside scrutiny.[256] Some scholars have likewise adopted ominous predictions in

---

[252] *See Davis*, 547 U.S. at 822.

[253] Roth, *supra* note 20, at 2048.

[254] *See* Wexler, *supra* note 10, at 40–42 (describing likely instances of over-claiming and abuse in private assertions of trade secret protection in the criminal justice context).

[255] *See, e.g.*, Memorandum Order at 2, Commonwealth v. Robinson, No. CC 201307777 (Pa. Ct. Com. Pl. Feb. 4, 2016) (refusing to order disclosure of TrueAllele's source code because it "would cause irreparable harm to the company, as other companies would be able to copy the code and potentially put him out of business").

[256] *See, e.g.*, *supra* notes 50–58 and accompanying text (discussing FBI collaboration with Harris to assure stingray secrecy); *see supra* notes 74–76, 80 and accompanying text (discussing state

support of trade secrecy. As one author explains, "[i]f the information is publicly circulated and copied, the company can lose licensing revenue. If the software in question is one of the company's most valuable assets, the result might be the bankruptcy of the company."[257]

Among other things, these responses reflect concern that, absent trade secret protection, developers will be unable to continue and improve upon their work. Concern that judicial action may inhibit innovation is laudable. After all, well-designed criminal justice algorithms promise a more fair and more just criminal justice system. As set forth above, the President's Council of Advisors on Science and Technology described probabilistic genotyping as a significant and welcome advance in the science.[258] Similarly, draft revisions to the Model Penal Code explain that "well-designed actuarial risk-assessment tools offer better predictions of future behavior than the clinical judgments of treatment professionals such as psychiatrists and psychologists, or the intuitions of criminal-justice professionals such as judges and probation officers."[259]

Concern that judicial action may inhibit innovation is also common when courts encounter advanced technology. For instance, similar concerns pervaded *Moore v. Regents of the University of California*, in which the California Supreme Court famously denied that an individual has any property right in cells removed from his body that are used in scientific research.[260] In reaching that holding, the court opined that recognizing a property right in one's cells would have a chilling effect on socially beneficial medical research.[261]

Yet, such concern is misplaced when it comes to mediating the relationship between private developers of criminal justice algorithms and the criminal defendants (and sometimes courts) who wish to examine their source code.[262] Focusing on the potential costs of breaching trade secret protection in fact answers the wrong question. Trade secrecy is but one tool

avoidance of source code possession for alcohol breath test devices); *see also infra* notes 399–401 and accompanying text (acknowledging and discussing alternative bases for continued source code nondisclosure, apart from trade secrecy).

257 Imwinkelried, *supra* note 8, at 125 (citations omitted).

258 PCAST REPORT, *supra* note 17, at 79 ("These probabilistic genotyping software programs clearly represent a major improvement over purely subjective interpretation.").

259 MODEL PENAL CODE: SENTENCING § 6.03 cmt. f (Tentative Draft No. 3 2014).

260 793 P.2d 479, 489 (Cal. 1990).

261 *Id.* at 493 (emphasizing the need not to threaten "innocent parties who are engaged in socially useful activities" with "disabling civil liability").

262 Existing scholarship, where it tackles trade secrecy in this field at all, treats such secrecy as inevitable. Such scholarship accordingly argues for disclosure-forcing mechanisms within the confines of existing trade secret and evidence law. *See* Wexler, *supra* note 10. This is an important project, but it is narrower than the one to which this Article is addressed.

of many that the government may deploy to spur innovation. Moreover, those tools may be uniquely within the government's reach in the field of criminal justice algorithms because government entities are the primary (or sole) purchasers of such technologies.[263]

This Part identifies the array of policy mechanisms available for incentivizing innovation in the field of criminal justice algorithms. The literature on innovation policy is vast,[264] and so this Part aims to synthesize that literature to identify how these innovation levers differ and which may best be applied to spur the development of criminal justice algorithms. Some of these levers more easily advance the goal of device and source code disclosure. Some are more easily implemented than others in the criminal justice context. Some are already in use. Thus, 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.

A. Patents and Trade Secrets

Patents are the traditional foil to trade secrecy.[265] Together, patents and trade secrecy function as mechanisms of innovation policy that award what amounts to a property right to inventors.[266] But each form of intellectual property offers a different scope of protection and different burdens.

Only a brief overview of trade secret law is needed to situate alternative innovation policy mechanisms by comparison. Trade secret protection springs largely from state law, though the basic contours of the doctrine are fairly consistent across jurisdictions.[267] As set forth above, a

---

[263] *See infra* Section IV.A.

[264] *E.g.*, Peter S. Menell & Suzanne Scotchmer, *Intellectual Property Law*, *in* 2 HANDBOOK OF LAW AND ECONOMICS 1473, 1530–34 (A. Mitchell Polinsky & Steven Shavell eds., 2007) (comparing patents, prizes, and grants); Hemel & Ouellette, *supra* note 19, at 317–26 (summarizing the literature on patents versus prizes versus grants and adding tax incentives to the range of innovation policy levers); *see also* Michael Abramowicz, *Perfecting Patent Prizes*, 56 VAND. L. REV. 115, 119–21 (2003) (describing a prize alternative to patents); Yaniv Heled, *Regulatory Competitive Shelters*, 76 OHIO ST. L.J. 299, 308–09 (2015) (identifying regulatory competitive shelters as an additional tool for spurring innovation in highly regulated fields).

[265] *See, e.g.*, Price, *supra* note 23, at 1769 ("Inventors face a stark choice between two intellectual property systems of protecting innovative ideas: patents and trade secrecy."); Derek Handova, *The Business of IP: Choosing Between Patents and Trade Secrets*, IP WATCHDOG (May 25, 2016), http://www.ipwatchdog.com/2016/05/25/choosing-patents-and-trade-secrets/id=69368 [https://perma.cc/L25Q-WFQ2] ("Patents and trade secrets represent two of the most common methods to protect IP. However, the most astute lawyers know when to favor one over the other.").

[266] *See* Price, *supra* note 23, at 1775–76.

[267] *Id.* at 1776 n.30. Federal law also provides some trade secret protection through the Economic Espionage Act, 18 U.S.C. § 1831 (2012), and the recently enacted Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified as amended in scattered sections of 18, 28 U.S.C.).

trade secret is information that is "subject to reasonable efforts to maintain secrecy and derives independent economic value from its secrecy."[268] Trade secret protection depends on continued secrecy; public disclosure is anathema to it.[269] Indeed, absent public disclosure, a trade secret may persist indefinitely. The scope of trade secret protection, however, is quite narrow. Trade secret law protects secret information only from its misappropriation.[270] Legal liability attaches where a person "uses or discloses trade secret information in violation of a duty of confidence or after acquiring the information by theft or fraud."[271] But trade secret law gives no relief where others reverse engineer an innovation or independently invent it.[272] As the preceding discussion has made evident, trade secret holders routinely assert a privilege against disclosure in litigation to bar or limit discovery of its protected information.

Patent law, by contrast, is a creature exclusively of federal law. An invention is patentable only if it comprises patentable subject matter and is new, useful, and nonobvious.[273] Moreover, and most significantly for present purposes, patent law requires public disclosure of an invention as a condition for obtaining a patent.[274] Indeed, "[t]he traditional quid pro quo view of the patent system imagines the patent grant as the carrot used to entice inventors to reveal their valuable secrets to the public."[275] Disclosure is satisfied by "a written description of the invention, and of the manner and process of making and using it," sufficient to enable a person of ordinary skill in the art to make and use it as well.[276] This disclosure must accompany an application for a patent, and such applications typically are published eighteen months after the filing date.[277] A successful patentee gains broad exclusive rights to his invention, including the right to make, use, or sell that invention in the United States.[278] Unlike a trade secret,

---

[268] Price, *supra* note 23, at 1776.

[269] *Id.* at 1777.

[270] *Id.*; *see also* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241, 244 (1998) (emphasizing trade secret law's basis in relational duties).

[271] Bone, *supra* note 270, at 244.

[272] UNIF. TRADE SECRETS ACT § 1 cmts. 1–2 (UNIF. LAW COMM'N, amended 1985).

[273] 35 U.S.C. §§ 101–03 (2012).

[274] *See* 35 U.S.C. § 112 (2012) (listing what the inventor must include in the public disclosure).

[275] J. Jonas Anderson, *Secret Inventions*, 26 BERKELEY TECH. L.J. 917, 919 (2011). Scholars debate whether patent law's disclosure requirements actually facilitate meaningful disclosure. *See supra* note 201. That debate is beyond the scope of this Article.

[276] 35 U.S.C. § 112(a).

[277] 35 U.S.C. §§ 111, 112, 122(b) (2012).

[278] *See* 35 U.S.C. § 271 (2012) (covering patent infringement and the inventor's remedies for enforcing exclusivity rights).

reverse engineering or independent invention of a patented innovation nonetheless constitutes infringement.[279] Further, patent protection is time-limited. Under current law, patent rights expire twenty years after the date of the patent application.[280]

In recent years, the Supreme Court has devoted considerable attention to the scope of patentable subject matter.[281] The Court has long held that the patentable subject matter provision "contains an important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable."[282] Within the last decade, however, the Court has enforced this exception with renewed vigor, holding that methods for hedging risk,[283] calibrating drug dosing,[284] and mitigating settlement risk each amounted to an invalid effort to patent an abstract idea.[285] The Supreme Court also held that patents on isolated DNA sequences are invalid because such sequences are a "product of nature."[286]

Under this line of cases, many criminal justice algorithms might well be nonpatentable subject matter. The Court has held that mathematical processes are abstract ideas ineligible for patent protection, at least insofar as those ideas are not inventively applied some real-world application.[287] Consequently, because computer algorithms are mathematical processes, they often cannot be protected with patents. The addition of a physical computer on which such an algorithm can run, the Court has emphasized, is not enough to render it patentable.[288] Rather, to be patent-eligible, an invention directed at an abstract idea—such as an algorithm—must include an "inventive concept" that "ensure[s] that the patent in practice amounts to significantly more than a patent upon the natural law itself."[289] Criminal justice algorithms like TrueAllele and COMPAS, which are simply

---

279 *See* ROBERT P. MERGES ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 37 (2017) ("The patent grant is nearly absolute, barring even those who independently develop the invention from practicing its art.").

280 35 U.S.C. § 154(a)(2) (2012).

281 *See* Alice Corp. Pty. v. CLS Bank Int'l, 134 S. Ct. 2347 (2014); Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 569 U.S. 576 (2013); Mayo Collab. Servs. v. Prometheus Labs., Inc., 566 U.S. 66 (2012); Bilski v. Kappos, 561 U.S. 593 (2010).

282 *Ass'n for Molecular Pathology*, 569 U.S. at 589 (internal quotation marks and brackets omitted).

283 *Bilski*, 561 U.S. 593.

284 *Mayo*, 566 U.S. 66.

285 *Alice*, 134 S. Ct. 2347.

286 *Ass'n for Molecular Pathology*, 569 U.S. at 580.

287 *See Alice*, 134 S. Ct. at 2357.

288 *Id.* at 2358 ("[T]he mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention.").

289 *Mayo*, 566 U.S. at 72–73; *see also Alice*, 134 S. Ct. at 2357.

sophisticated software programs, may be particularly susceptible to exclusion from patentability.[290]

In light of the difficulty of patenting criminal justice algorithms and the traditional dichotomy of patents and trade secrets, it is unsurprising that many private developers of these algorithms have pursued trade secret protection. As set out above, however, the harms flowing from this choice are significant.[291] Fortunately, patents and trade secrets are not the only tools available for incentivizing innovation.

B. Prizes

Prizes as a tool to spur innovation have a distinguished pedigree. In 1714, the British government offered a prize of £20,000 (worth more than £1 million today) to the inventor of a method for determining longitude at sea.[292] More recently, prizes have won renewed interest. In 2014, the British government reconvened the Longitude Committee to facilitate a modern prize process.[293] In the United States, the National Academy of Engineering recommended that the federal government invest more extensively in certain prize competitions.[294] In 2009, the President urged agencies to increase their use of prizes as incentives for innovation, and to date, federal agencies have offered more than $250 million in more than 803 "challenge and prize competitions."[295] These competitions include prizes for "develop[ing] algorithms that advance place-based crime forecasting,"[296]

---

[290] Cybergenetics, which created and sells TrueAllele, lists several TrueAllele patents on its website. *Patents*, CYBERGENETICS, https://www.cybgen.com/information/patents.shtml [https://perma.cc/FG5L-Q9CB]. All of these patents claim methods or systems related to genetic analysis. *See id.* All but two, however, were issued well before the Supreme Court's renewed focus on patentable subject matter. *See id.*; U.S. Patent No. 8,898,021 (filed Feb. 2, 2001) (issued Nov. 25, 2014); U.S. Patent No. 9,708,642 (filed Nov. 20, 2014) (issued July 18, 2017). Sophisticated criminal justice algorithms may also face patenting difficulties for written description and enablement reasons. *See* W. Nicholson Price II, *Describing Black-Box Medicine*, 21 B.U. J. SCI. & TECH. L. 347, 348, 351–52 (2015) (concluding that satisfying the written description and enablement requirements is difficult, but not insurmountable, for "black-box" medicine, and defining "black-box" medicine as medically related algorithms that are opaque because they are so complex as to be "practically nontransparent" or because they are the product of machine learning).

[291] *See supra* Part II.

[292] *See* SUZANNE SCOTCHMER, INNOVATION AND INCENTIVES 32 (2004); Martin Rees, *A Longitude Prize for the Twenty-First Century*, 509 NATURE 401, 401 (2014).

[293] Rees, *supra* note 292.

[294] NAT'L ACAD. OF ENG'G, CONCERNING FEDERALLY SPONSORED INDUCEMENT PRIZES IN ENGINEERING AND SCIENCE 1 (1999).

[295] *About*, CHALLENGE.GOV, https://www.challenge.gov/about [https://perma.cc/6PW2-26R5]; *Challenges*, CHALLENGE.GOV, https://www.challenge.gov/list [https://perma.cc/JFS5-NTLT] ("803 Competitions Found").

[296] *Real-Time Crime Forecasting Challenge*, CHALLENGE.GOV, https://www.challenge.gov/challenge/real-time-crime-forecasting-challenge [http://perma.cc/T4JW-S8M7].

determining "the amount and rate of change of the ballistic performance of" individual body armor vests,[297] and designing "new automated detection algorithms . . . that improve the speed, accuracy, and detection of small threat objects and other prohibited items during the airport passenger screening process."[298]

The prizes best suited for encouraging innovation are inducement prizes—those "designed to foster progress toward or achievement of a specific objective by offering a named prize or award."[299] Inducement prizes typically reward those "who provide the best entry in a contest or who first meet some specified technical goal."[300] Governments are not the only entities capable of establishing and awarding prizes. Some of the best-known modern prizes spring from private sources, including the famed Ansari XPRIZE, which offered $10 million for a privately financed, reusable spacecraft "capable of carrying three people to 100 kilometers above the Earth's surface twice within two weeks."[301]

Unlike patents, which demand public disclosure, or trade secrets, which shun public disclosure, prizes are agnostic on the matter of disclosure.[302] Prizes can condition their rewards on disclosure of the winning or participating entrants, though many existing prizes have declined to impose such conditions.[303] Although prizes typically exist alongside traditional intellectual property regimes, some scholars have proposed utilizing prizes in place of such regimes.[304] These proposals largely rely on government-managed prizes.[305]

In assessing the comparative virtues and vices of patents and prizes, some key differences appear. First, patents differ from many other

---

[297] *National Institute of Justice Body Armor Challenge: How Long Does Body Armor Really Last?*, NAT'L INST. OF JUSTICE, https://www.nij.gov/funding/Pages/fy12-body-armor-challenge.aspx [https://perma.cc/XMY8-BLDB].

[298] *Passenger Screening Algorithm Challenge*, CHALLENGE.GOV, https://www.challenge.gov/challenge/passenger-screening-algorithm-challenge [https://perma.cc/2WF9-RXTJ].

[299] NAT'L ACAD. OF ENG'G, *supra* note 294, at 1. Prizes can also be awarded in recognition of past achievements. *See id.* at A-1 (contrasting recognition and inducement prizes).

[300] *Id.*

[301] *Ansari XPRIZE®*, XPRIZE FOUND., http://ansari.xprize.org [https://perma.cc/KD99-YXLD]. The prize was awarded in 2004. *Id.*

[302] *See* Hemel & Ouellette, *supra* note 19, at 355–56.

[303] *See id.* at 356 & n. 231 (citing GOOGLE LUNAR X PRIZE, MASTER TEAM AGREEMENT, VERSION 1.0 §§ 11.1-11.5 (Nov. 24, 2009), https://ia801304.us.archive.org/20/items/wikileaks-archive/googlelunarx-prize-final-master-team-agreement-review.pdf [https://perma.cc/2TQB-4EN9]).

[304] *See* Michael Abramowicz, *Perfecting Patent Prizes*, 56 VAND. L. REV. 115, 119–21 (2003) (surveying the literature).

[305] *See id.* at 121 ("Prize system advocates recognize that the devil is in the details and that the devil for a prize system is the government's ability to dispense rewards accurately.").

innovation mechanisms, including prizes, in "*who decides* which projects to reward and how much to reward them."[306] Under the patent system, once a patent issues, market forces of supply and demand determine whether and how much an innovation is worth through consumer purchases (or lack thereof) at supracompetitive prices.[307] The same is true for trade secrets. So long as trade secrecy is intact, market forces determine what supracompetitive price is acceptable.[308] By contrast, prize administrators typically fix the amount of a prize when the prize is announced, rather than when it is awarded, and they bear responsibility for determining when a submission has succeeded.[309] These differences require a prize giver to accurately forecast the value of a potential innovation, as well as the difficulties it might face in reaching fruition.[310] Prizes accordingly give the government, rather than the market, power to determine the amount of the economic reward for innovation.

Second, prizes typically diverge from traditional intellectual property doctrines on the matter of who pays the supracompetitive reward for innovation. When the government administers a prize, its funds are often drawn from general tax revenue.[311] Conversely, trade secrets and patents extract supracompetitive revenue only from their own consumers.[312] They thus eschew enlisting the general public in paying for a particular innovation and place the burden on the purchasers of IP-protected products.[313]

Yet these policy differences may not be so significant in the context of criminal justice tools. Both of the major policy divides between prizes, on the one hand, and patents and trade secrets, on the other, turn on the greater role the government typically plays in administering prizes. But in the criminal justice context, government entities also dominate the role of "the market" that is central to patent and trade secret policy. Tools like stingrays, alcohol breath test devices, probabilistic genotyping software

---

306 *See* Hemel & Ouellette, *supra* note 19, at 327.

307 *Id.* at 327.

308 *Id.* at 346–47 ("Trade secret protection, like patent protection, is an *ex post*, market-set transfer . . . .").

309 *Id.* at 327.

310 *Id.* Prizes need not always suffer the full force of these forecasting difficulties; some prizes scale rewards with market performance. *See* Tania Cernuschi et al., *Advance Market Commitment for Pneumococcal Vaccines: Putting Theory into Practice*, 89 BULL. WORLD HEALTH ORG. 913 (2011) (describing the Advance Market Commitment (AMC) program for pneumococcal vaccines, which guarantees a minimum price per vaccine dose sold); Hemel & Ouellette, *supra* note 19, at 318–19.

311 Hemel & Ouellette, *supra* note 19, at 346.

312 *Id.* at 347; *see also id.* ("Patents and trade secrets come closest to satisfying the user-pays principle.").

313 *Id.* at 346–47.

programs, and recidivism risk statistic packages are largely, if not exclusively, purchased by government entities, usually law enforcement.[314] It might even be unlawful for a nongovernment actor to procure such devices.[315]

Prizes might be operationalized in the criminal justice sphere in at least two ways. First, discrete technological tools the government is interested in developing and using might be the subject of a one-time inducement prize. As set forth above, at least one such prize has already been offered. The federal government's Office of Justice Programs issued a challenge prize to "develop algorithms that advance place-based crime forecasting."[316] Second, law enforcement or judicial procurement offices may already functionally be paying prize-like bounties for the criminal justice tools they acquire by paying supracompetitive prices.[317] In particular, exclusive government procurement contracts netting supracompetitive profits are quite a significant prize to capture.[318]

C. Grants

Government grants are disbursements of funds that provide direct financial support to undertake or complete a project.[319] In 2015, total federal research and development (R&D) spending exceeded $130 billion.[320] More than half of these funds supported defense-related R&D,[321]

---

[314] *See infra* Section IV.A.

[315] *See, e.g.*, Harris Letter, *supra* note 13, at 1 (proposing, as a condition of FTC approval for Harris's sale of stingray devices, that "[t]he marketing and sale of these devices shall be limited to federal/state/local public safety and law enforcement officers only").

[316] *Real-Time Crime Forecasting Challenge*, CHALLENGE.GOV, https://www.challenge.gov/challenge/real-time-crime-forecasting-challenge [http://perma.cc/T4JW-S8M7].

[317] Hemel and Ouellette categorize "procurement contracts" as a form of government grant. Hemel & Ouellette, *supra* note 19, at 320–21 n.73. As discussed below, however, grants are typically defined by their infusion of government funds to support research and development, rather than to purchase completed inventions. *See infra* text accompanying note 329. Law enforcement or other procurement of tools deployed to investigate, prosecute, or sentence criminals is closer to an ex post prize than an ex ante grant.

[318] *See also infra* notes 351–353 and accompanying text (discussing exclusive contracts in the context of regulatory exclusivities).

[319] Hemel & Ouellette, *supra* note 19, at 320 & n.73. Grants can encompass both funds awarded to nongovernment researchers and direct spending in government research laboratories, *id.* at 320, though the former is of primary interest here.

[320] Michael Yamaner, *Total Federal Research and Development Funding Down 1% in FY 2015, but Funding for Research Up 1%*, INFOBRIEF at 1 (Mar. 2017), https://www.nsf.gov/statistics/2017/nsf17316/nsf17316.pdf [https://perma.cc/5HAJ-VADT].

[321] OFFICE OF MGMT. & BUDGET, HISTORICAL TABLES: BUDGET OF THE UNITED STATES GOVERNMENT 217 tbl.9.7 (2016) https://www.gpo.gov/fdsys/pkg/BUDGET-2016-TAB/pdf/BUDGET-2016-TAB.pdf [https://perma.cc/5SMJ-EHAM].

a common birthplace for criminal justice algorithms and other tools.[322] Moreover, state governments also invest significantly in research grants, though much of that money is allocated to university research.[323]

Grant funding may, but need not, be conditioned on disclosure of the fruits of that funding. In general, grant recipients are required to disclose to the federal government any patentable inventions arising from grant-funded research.[324] Grant recipients typically are not required to disclose non-patentable discoveries—and encouraging such disclosure can be challenging.[325] This is not to say that more rigorous disclosure requirements would be inconsistent with the regulatory framework of grant funding. Rather, in the context of criminal justice technologies, grant-making agencies might well conclude that a more robust disclosure requirement is appropriate. For instance, just as the federal government requires communication of patentable inventions "within a reasonable time after [such invention] becomes known," the government might require disclosure of grant-supported trade secret information "within a reasonable time after" such information is developed.[326]

Like prizes, grants allocate to the government both determination of the amount of the innovation incentive and the obligation to pay for it, usually from general funds.[327] But grants differ from prizes, as well as trade secrets and patents, because grant funding infuses capital to potential innovators before a completed or commercial product is available, rather than rewarding successful inventors ex post.[328] This earlier distribution of

---

[322] *See, e.g.*, Jemal R. Brinson, *Cell Site Simulators: How Law Enforcement Can Track You*, CHI. TRIB. (Feb. 18, 2016), http://www.chicagotribune.com/news/plus/ct-cellphone-tracking-devices-20160129-htmlstory.html [https://perma.cc/R2KY-Q4RW] ("[Stingray technology] was initially developed and used by military and intelligence agencies and over time made its way to state and local law enforcement agencies.").

[323] *See* RONDA BRITT, NAT'L CTR. FOR SCI. & ENG'G STATS., UNIVERSITIES REPORT HIGHEST-EVER R&D SPENDING OF $65 BILLION IN FY 2011, at 2 (2012), https://www.nsf.gov/statistics/infbrief/nsf13305/nsf13305.pdf [https://perma.cc/Q93V-2TG5]; CHRISTOPHER PECE, NAT'L CTR. FOR SCI. & ENG'G STATS., STATE GOVERNMENT R&D EXPENDITURES TOTAL MORE THAN $2.2 BILLION IN FY 2015, at 1 (2016), https://www.nsf.gov/statistics/2017/nsf17307/nsf17307.pdf [https://perma.cc/F8D5-MGAG] ("State government agency expenditures for research and development totaled $2.2 billion in [fiscal year] 2015, an increase of 16.9% from FY 2014"). (Noting that, from fiscal year 2010 to fiscal year 2011, "[i]nstitution-funded R&D rose by over $500 million to $12.4 billion").

[324] 35 U.S.C. §§ 201(d)–(e), 202(c)(1) (2012).

[325] *See* Hemel & Ouellette, *supra* note 19, at 356, 356 n.226 (citing Rebecca S. Eisenberg, *Public Research and Private Development: Patents and Technology Transfer in Government-Sponsored Research*, 82 VA. L. REV. 1663, 1674–75 (1996)).

[326] 35 U.S.C. § 202(c)(1).

[327] *See* Hemel & Ouellette, *supra* note 19, at 327, 345.

[328] *See id.* at 333, 348.

funds may enable more and smaller companies to enter the market, as it reduces the private capital investments required for innovation.[329]

Grants appear already to be in use to support the development of some criminal justice technologies. Mark Perlin, the creator of TrueAllele, was the successful recipient of several federal government research grants. Between 1997 and 2000, Cybergenetics, Perlin's company, received four grants under the Small Business Innovation Research (SBIR) program.[330] At least two of these grants appear directly related to the development of TrueAllele.[331] Each grant was administered by the Department of Health and Human Services.[332]

On the whole, however, direct grant funding is likely to be less well suited than other innovation policy mechanisms for encouraging innovation in criminal justice technologies, particularly for development by private companies like the ones now asserting trade secret protection. For one thing, grant funding for private sector R&D is simply less common than similar funding for R&D at universities or within government itself.[333] For another, grants in this context may be particularly subject to the inefficiencies believed to accompany government-set rewards.[334] In particular, scholars have frequently critiqued grants as a tool of innovation policy because grant-funding decisions are believed to rely on "decision-making by centralized government bureaucrats who often lack market actors' superior knowledge."[335] On this view, grants require the government to accurately identify which potential innovations to pursue, determine who is most likely to produce viable results, and calculate the value of those innovations and the cost of development.[336]

---

[329] *Id.* at 336–39; *see also About SBIR*, SBIR-STTR: AMERICA'S SEED FUND, https://www.sbir.gov/about/about-sbir [https://perma.cc/4N8K-C3C4] (discussing the Small Business Innovation Research (SBIR) program, which "funds the critical startup and development stages" of technological innovation at small businesses through "a competitive awards-based program").

[330] *Cybergenetics Corporation*, SBIR-STTR: AMERICA'S SEED FUND, https://www.sbir.gov/sbirsearch/detail/139893 [https://perma.cc/S785-MFGX].

[331] *Id.* (reciting two grants for "automated microsatellite genotyping").

[332] *Id.*

[333] University R&D investments, for instance, significantly outpace other state R&D expenditures. *Compare* PECE, *supra* note 323, at 1 (reciting $2.2 billion in R&D expenditures flowing from state government agencies in fiscal year 2015), *with* BRITT, *supra* note 323, at 2 (reciting institution-funded R&D exceeding $12 billion in fiscal year 2011); *see also About SBIR*, *supra* note 329 (explaining that federal agencies with large R&D budgets must allocate 3.2% of those funds to the SBIR program).

[334] *See* W. Nicholson Price II, Grants 11–18 (Dec. 5, 2017) (unpublished manuscript) (on file with author) (summarizing the three primary critiques of grants as a tool of innovation policy: bureaucratic decision-making, unaccountable ex ante incentives, and problematic risk allocation between funder and grantee).

[335] *Id.* at 13; *see id.* at 13–14.

[336] Hemel & Ouellette, *supra* note 19, at 327.

In practice, this critique is somewhat misplaced, at least for many traditionally grant-funded fields. For instance, the National Institutes of Health (NIH), the largest nondefense grant funder of research, often enlists outside experts to assist the agency in determining both what areas of innovation to fund and which specific projects to fund.[337] In so doing, the NIH can capture, at least in part, the "special advantage" associated with harnessing private information in directing innovation.[338] But this internalization of outside expertise is likely to be more difficult where innovating criminal justice algorithms is at issue. In this field, available outside experts are more likely to be for-profit competitors (or other government entities), rather than academic colleagues. This is likely to heighten the risk of conflicts of interest and make even-handed grant evaluation difficult to achieve.

D. Regulatory Exclusivities

Regulatory exclusivities are "competitive advantages resulting from statutory bars on regulatory action where such action is otherwise mandated and would have taken place but for the triggering of the bar."[339] Such exclusivity arises where a government entity is barred from taking some action that would introduce or enhance competition in a product or market.[340] Government nonaction effectively "shelters" from competition the beneficiary of earlier government action, granting that beneficiary a competitive advantage, if not a de facto monopoly, in the relevant market.[341] Regulatory exclusivities arise most frequently under the auspices of the Food and Drug Administration (FDA).[342] For instance, under the Orphan Drug Act, once the FDA approves a drug product to treat a particular "rare disease or condition" (an "orphan condition"),[343] it is barred from approving another drug for that condition for a period of seven years.[344]

---

[337] *See* Price, *supra* note 334, at 24–25 (discussing the role of outside experts in soliciting research—deciding what areas of innovation to fund); *id.* at 26–28 (discussing the role of outside experts in peer review of grant applications—deciding what specific projects and innovators to fund).

[338] Hemel & Ouellette, *supra* note 19, at 327–28 (quoting Brian D. Wright, *The Economics of Invention Incentives: Patents, Prizes, and Research Contracts*, 73 AM. ECON. REV. 691, 703 (1983)).

[339] Heled, *supra* note 264, at 305.

[340] *Id.*

[341] *Id.*

[342] *Id.* at 353–54.

[343] *See* 21 U.S.C. § 360bb(a)(2) (2012) (defining "rare disease or condition"). Well-known examples of orphan (that is, rare) diseases include Huntington's disease and amyotrophic lateral sclerosis (ALS/Lou Gehrig's disease). Heled, *supra* note 264, at 336 n.145.

[344] 21 U.S.C. § 360cc(a)(2) (2012); *see also* Heled, *supra* note 264, at 302 (discussing the Orphan Drug Act).

As operationalized in the Orphan Drug Act and similar programs, regulatory exclusivities operate as patent-like rewards for innovation.[345] These exclusivities reward completed innovation, with supracompetitive prices determined by what amounts to a market monopoly and paid by product purchasers, rather than the broader public.[346] Unlike patents, however, regulatory exclusivities do not, by definition, require public disclosures of any kind. The government may impose disclosure demands as a condition of exclusivity, of course, because the government sets the terms for the creation and awarding of these exclusive rights.[347]

Insofar as patent-like protection would be desirable for criminal justice algorithms but is unavailable due to difficulties qualifying as patentable subject matter,[348] regulatory exclusivities may offer a way forward. To be sure, during a period of exclusivity, innovation directed at a particular way of solving a particular problem may be slowed. But that is a consequence of exclusive rights, whether they arise from patent law, FDA regulations, or procurement policy. Moreover, robust exclusive rights often pair well with robust disclosure requirements, as in patent law,[349] suggesting that regulatory exclusivities in this context may be particularly generative.

Indeed, such exclusivities may already effectively be in place for some technologies. For many criminal justice technologies, government entities enter into exclusive contracts with a single private company to obtain a particular kind of technology. For instance, Mark Perlin, TrueAllele's creator, objected when he learned that the FBI proposed to enter into a "sole source contract" to obtain STRmix for probabilistic genotyping.[350] Northpointe, meanwhile, holds an exclusive contract to

---

[345] *See* Rebecca S. Eisenberg, *The Role of the FDA in Innovation Policy*, 13 MICH. TELECOMM. & TECH. L. REV. 345, 359 (2007) (describing FDA exclusivities in the context of pharmaceutical technologies as "pseudo-patents"); Heled, *supra* note 264, at 300 (noting that this mechanism for encouraging and rewarding innovation has been described not only as a "regulatory exclusivit[y]" but also as a "pseudo-patent exclusivit[y]");

[346] *See supra* text accompanying notes 307–308, 312, 328.

[347] Requiring or enforcing disclosure may be more difficult in view of the fact that different government components are typically responsible for creating and administering regulatory exclusivities. These exclusivities arise from statute, but they are typically administered by agencies (principally the FDA). *See* Heled, *supra* note 264, at 305. If the statutory scheme fails to specify a disclosure obligation, the agency may be constrained from imposing one itself. *See* 5 U.S.C. § 706(2) (2012).

[348] *See supra* Section III.A.

[349] *See* MERGES ET AL., *supra* note 279, at 245 ("A patent can be a potent property right. In exchange for this grant from the government, an inventor must disclose the workings of his or her invention in enough detail to be informative to other people working in the same field.").

[350] Perlin Letter, *supra* note 95, at 1.

provide the State of Wisconsin with recidivism risk statistics.[351] These exclusive arrangements might well function like regulatory exclusivities, particularly if they carry a minimum term of exclusivity.

E. Tax Incentives

The government invests in innovation not only by spending its money on grants and prizes but also by granting favorable tax treatment to certain R&D activities.[352] The two largest existing R&D tax expenditures allow taxpayers to expense research and experimental spending and to claim a tax credit for certain increases in a taxpayer's research spending.[353] Most states also give favorable tax treatment to R&D expenditures.[354] A majority of these states pattern their R&D tax incentives on their federal counterpart.[355] Nine states, however, employ partially or fully refundable tax credits, which permit a company to claim the credit even if it has too little income against which to offset that credit.[356]

All of these policies provide tax relief tied to expenditures for research itself, rather than the results of that research. Accordingly, these tax incentives, like grants, reward potential innovators ex ante by permitting more capital to stay with innovators.[357] Like grants, these tax incentives may encourage not only more innovation but also innovation by more participants.[358] Like patents, trade secrets, and regulatory exclusivities, however, tax incentives permit the market to dictate the measure of

---

[351] Freeman, *supra* note 151, at 92.

[352] *See* CONG. RESEARCH SERV., S. PRT. 113–32, TAX EXPENDITURES: COMPENDIUM OF BACKGROUND MATERIAL ON INDIVIDUAL PROVISIONS 83–105 (comm. print 2014) (summarizing the principle provisions); Hemel & Ouellette, *supra* note 19, at 321–26 (same).

[353] CONG. RESEARCH SERV., *supra* note 352, at 83–105.

[354] *See* LEGISLATIVE BUDGET BOARD, MEMORANDUM: OVERVIEW OF RESEARCH AND DEVELOPMENT TAX INCENTIVES 5 (2013), http://bit.ly/2tKOpYB [https://perma.cc/KT82-AFXE] ("Forty-three states offer some type of R&D specific tax incentive with 16 states offering a business tax incentive, 3 states offering a sales tax incentive, and 24 states offering both.").

[355] *Id.* at 6 ("A majority of states (31) use the federal definition of [qualified research expenses] from the Internal Revenue Code, Section 41, with a modification to include only expenses incurred within the state.").

[356] *Id.*

[357] Hemel & Ouellette, *supra* note 19, at 331–32.

[358] As Hemel and Ouellette observe, the existing federal R&D tax incentives, and the majority of existing state R&D tax incentives, favor well-established corporations because their benefits can be realized only if a taxpayer has income to offset. *Id.* at 337. But the skew towards established companies is not an inherent feature of tax incentives for research. *See id.* Indeed, nine states have enacted refundable R&D tax credits, which allow a taxpayer to collect the credit regardless of whether the business reports taxable income. *Id.*

financial reward: up to a point, the more an innovator invests in research, the greater the tax break.[359]

Unfortunately, existing tax incentives for R&D facilitate developer secrecy much more than disclosure. Taxpayers who claim an R&D tax benefit must maintain records establishing their entitlement to that benefit,[360] but that hardly constitutes meaningful access for anyone other than the Internal Revenue Service (IRS). Tax return information is confidential,[361] and so the IRS is severely restricted in its ability to disclose supporting paperwork.[362] Yet, the contours of existing tax incentives do not foreclose disclosure-facilitating amendments or alternatives. Secrecy is not inherent in tax incentive policy the way it is in trade secret law. To the contrary, tax credits might well be conditioned on certain public disclosures.[363] As long as the value of the tax credit exceeds any losses due to increased competition stemming from disclosure, a rational developer should choose disclosure.

More troubling for the use of tax policy to encourage innovation is the fact that, though R&D tax credits are widespread, they are largely motivated by concerns other than encouraging innovation.[364] Indeed, the most common motivation is economic development—new jobs—rather than innovation—new knowledge.[365] Insofar as incentivizing innovation is merely a beneficial secondary effect of tax policy, that policy is unlikely to reflect best practices for innovation, like public disclosure, that are orthogonal to a policy's true goal.

* * *

A multitude of policy mechanisms are available for incentivizing innovation, including in developing criminal justice technology. Trade secrecy is merely one innovation policy lever among many. Some of these levers, like trade secret protection, increase the likelihood and scope of nondisclosure and other forms of secrecy. Others, including patents, prizes, grants, regulatory exclusivities, and tax incentives coupled with appropriate

---

[359] *Id.* at 328, 333.

[360] *See, e.g.*, 26 C.F.R. § 1.41-4(d) (2016) (recordkeeping requirements for claiming the tax credit for increasing research activities).

[361] *See* I.R.C. § 6103(a) (2016) (confidentiality of tax return information).

[362] Hemel & Ouellette, *supra* note 19, at 356.

[363] *Id.* ("[T]ax credit[s] should be conditioned on public disclosure to the extent that such disclosure does not significantly undermine the innovation incentive.").

[364] *See* Chad R. Miller & Brian Richard, *The Policy Diffusion of the State R&D Investment Tax Credit*, 42 STATE & LOCAL GOV'T REV. 22 (2010).

[365] *Id.* at 24.

disclosure requirements, decrease that likelihood. Together, this panoply of policy tools makes plain that alternative mechanisms exist for spurring helpful innovation in the criminal justice field without sacrificing the practical and constitutional necessities of access to source code.

IV. INNOVATING CRIMINAL JUSTICE

Innovation policy is more than simply intellectual property rights like trade secrets and patents. As discussed above, mechanisms for encouraging innovation can fund companies doing research or reward companies for the successful products of that research. Most of these mechanisms can be coupled with a requirement to disclose source code or other relevant information beyond the confines of a protective order or nondisclosure agreement. This Part accordingly articulates how courts and policymakers can best encourage or enforce optimal source code disclosure. It first explains that implementing alternative innovation policy mechanisms may be particularly efficient and effective in the context of criminal justice algorithms because government entities are the primary (or sole) purchasers of such technologies. In view of the range of alternative innovation policies on which the government can draw, secrecy is not necessary for adequate innovation. Indeed, many of the tools of innovation policy are already a part of funding the development and purchase of criminal justice technology.

Turning to the mechanics of an appropriate disclosure requirement, this Part next argues that, to alleviate the practical and potentially constitutional harms of source code secrecy, optimal source code disclosure should be both broad and early. Broad disclosure means disclosure that reaches beyond the parties in a particular criminal prosecution and may include public disclosure. Early disclosure means disclosure that precedes a technology's use in a particular criminal investigation, prosecution, or sentencing. Acknowledging that government policymakers are best suited to require broad and early disclosure, this Part nonetheless contends that courts need not wait for these regulators to act before ordering source code disclosure in individual cases. If courts order disclosure, policymakers may follow that lead, implementing complementary innovation incentives as needed along the way. Indeed, recent experience supports a court-initiated movement toward transparency.

A. Efficient Alternative Innovation Policies

The government, as both a funder of research and the primary purchaser of criminal justice technologies, is uniquely well positioned to implement alternative innovation policies in an efficient and effective

manner. Innovation policy typically must make choices about whether to put pricing power and payment obligations in government hands or users' hands. But for criminal justice algorithms and related tools, these amount to much the same thing. Government entities enjoy a monopsony (or at least an oligopsony) for many criminal justice algorithms.[366] That is, government entities are the only (or near only) purchasers of these technologies.[367]

Some separation between innovation payor and product purchaser may arise where the government entity that purchases technology is not the same entity as the one that awarded the developer a prize, grant, or tax credit. For instance, the City of Baltimore will bear the costs of innovation differently depending on whether the federal government pursues innovation policy principally through patents (in which Baltimore will pay supracompetitive prices for a product) or prizes (in which the federal government will shoulder some of the premium for innovation, yielding potentially lower prices to product purchasers).

But the relatively limited number of possible purchasers for criminal justice algorithms—law enforcement, departments of corrections, and judicial officers—creates less disjunction between payor and purchaser than typically exists. Moreover, when a single government entity (whether local, state, or federal) contemplates what innovation policy to adopt to facilitate its own acquisition of new tools, it will be both payor and purchaser regardless of whether it awards grants or tax credits. This multiplies the range of innovation policy levers the government may efficiently utilize to calibrate the financial rewards for accurate, reliable, and transparent criminal justice tools.

Moreover, many innovation policy mechanisms are already in place, awaiting the addition of a proper disclosure requirement. As suggested earlier, government procurement of criminal justice tools resemble—or could be made to resemble—prizes or regulatory exclusivities.[368] Government procurement policy can act as both purchase and prize where the government is the only authorized buyer. If a government entity exerts its monopsony power to extract unusually low prices, it is likely to under-induce innovation and development in the field. By contrast, if the government pays supracompetitive prices, that economic windfall to the developer functions as an ex post, government-set prize.[369] If government

---

[366] Monopsony is a market condition in which there is only one buyer but many sellers. *See* NEVA GOODWIN ET AL., PRINCIPLES OF ECONOMICS IN CONTEXT 234 (2014). Oligopsony is a market condition in which there are a relatively small number of buyers. *Id.* at 235.

[367] *See, e.g.*, Harris Letter, *supra* note 13, at 1; *supra* text accompanying notes 314–315.

[368] *See supra* text accompanying notes 317, 350–351.

[369] *See* Hemel & Ouellette, *supra* note 19, at 333.

purchases are coupled with sole source agreements—agreements to buy a particular kind of technology or service from only one supplier—this arguably constitutes a form of regulatory exclusivity.[370] This too is already occurring: Recall that Mark Perlin was particularly aggrieved to be excluded from the FBI's proposal to enter a "sole source contract" to purchase probabilistic genotyping software.[371] A sole source contract granted to a competitor was not merely the loss of one sale for Perlin; it was exclusion from a lucrative market.[372]

As mentioned above, more traditional innovation mechanisms are also already in use, in at least small measure. The federal government previously has established formal prizes for innovators in this field, including a prize for "develop[ing] algorithms that advance place-based crime forecasting."[373] Government grants have also supported work to develop criminal justice algorithms. For instance, Perlin received multiple grants under the SBIR program, some of which appear to have supported TrueAllele's development.[374]

To be sure, vigorous assertions of trade secret protection in this field may suggest that existing alternative incentives are not yet adequate to obviate the commercial value of secrecy.[375] If that is so, these existing alternative incentives for innovation offer a framework for recalibrating the rewards of innovation to do so. For instance, in exchange for source code disclosure, government purchasers might guarantee a higher purchase price or longer single source contract term for the successful private developer of a criminal justice algorithm or related tool. The federal government, in particular, may be well suited to establish new prizes or grants for the development of such technologies. The precise details of which alternative innovation mechanisms are best deployed—and in what measure—must await further experience with innovation in the shadow of adequate disclosure requirements. For now, it is enough to appreciate that alternative mechanisms for encouraging innovation exist, are already in use in some

---

370 *See supra* text accompanying notes 350–351.

371 *See* Perlin Letter, *supra* note 95, at 1.

372 *Cf.* Heled, *supra* note 264, at 300–02 (describing regulatory exclusivities as frequently requiring a regulator to refrain from approving a second market entrant for a period of time after approving the first market participant—thus excluding second comers from the market for a set period of time).

373 *Real-Time Crime Forecasting Challenge*, *supra* note 296.

374 *Cybergenetics SBIR grants*, *supra* note 330.

375 *See, e.g.*, MURPHY, *supra* note 8, at 101 ("Perlin admitted that no other scientists had seen his code or reviewed it directly, and he stood by his refusal to make it available, defending it as a 'trade secret.'"); Ruger, *supra* note 75 (reporting that CMI initially refused to disclose source code for an Intoxilyzer device despite a court order and despite the imposition of more than $500,000 in sanctions for that refusal).

measure in the criminal justice field, and can be modified as needed to achieve independence from secrecy.

Indeed, in light of the panoply of existing innovation policy mechanisms, policymakers might conclude that, even absent trade secrecy, these existing benefits are sufficient to spur innovation. Trade secrecy, in other words, may simply arrogate a particularly harmful windfall to developers. This is not a far-fetched conclusion. For both probabilistic genotyping and recidivism risk score software packages, the market already includes competitors with publicly available source code.[376] Insofar as maintaining source code secrecy is unnecessary for either competitive success or valuable innovation, requiring government contractors to exchange trade secrecy for disclosure may not yield a worrisome lack of innovation.

B. Innovating Optimal Disclosure

While appropriate innovation policy for criminal justice algorithms may avoid typically difficult choices about who pays for innovation due to the purchasing role of government entities, policy setting in this field may underscore a different kind of policy difference, turning on the scope and timing of disclosure. As set forth above, alternative innovation policy mechanisms are readily available and may be readily paired with disclosure requirements. Apart from patents, however, use of an innovation policy tool does not inherently establish the scope and timing of relevant disclosure.[377] For criminal justice technologies, disclosure that is broad and early offers significant advantages over disclosure that is confined to an individual criminal case in either scope or timing.

First, source code disclosure, or disclosure that a criminal justice technology is in use, may extend either narrowly or broadly. If narrowly, only individuals involved in a particular case would gain access to this information. This might arise where a court orders source code disclosure subject to a protective order.[378] A broader remedy might demand public

---

[376] *See* U.S. *Loomis* Brief, *supra* note 15, at *17 n.5 (observing that several states have "develop[ed] and validat[ed] publicly available risk-assessment measures for consideration at sentencing"); PCAST REPORT, *supra* note 17, at 78–79; Roth, *supra* note 20, at 2019.

[377] On timing of patent disclosure, see 35 U.S.C. § 122(b) (2012).

[378] *See* State v. Chun, 943 A.2d 114, 122–23 (N.J. 2008) (describing the efforts undertaken by the courts and parties to examine the source code of the alcohol breath test device at issue while preventing broader disclosure of that code); Protective Order Regarding the Confidentiality of the Forensic Statistical Tool (FST) Source Code and Related Documents, United States v. Johnson, No. 1:15-CR-00565 (S.D.N.Y. July 18, 2016) (putting in place a protective order for FST, which order was subsequently vacated in October 2017); Wexler, *supra* note 10, at 50–53 (arguing that protective orders,

disclosure. A court might order source code disclosure absent any protective order.[379] Conversely, legislatures and agencies setting the terms for prizes, grants, regulatory exclusivities, and tax incentives, as well as procurement offices preparing purchase agreements, might more easily and efficiently condition those awards, rewards, and sales on public disclosure.[380]

Broad disclosure offers several advantages over narrow disclosure. As discussed earlier, outside review of source code has identified algorithmic weaknesses and errors on numerous occasions.[381] Public access to source code facilitates thorough investigation by multiple reviewers, making it more likely that errors will be identified and corrected.[382] Broad disclosure also enables multiple groups, including nonprofit criminal defense organizations, to share the financial and other costs of validating a software program and examining software updates and software status on an ongoing basis.[383] Finally, broad disclosure may itself act as an incentive for further innovation by providing more material on which new innovation can build.[384]

---

not nondisclosure, are the appropriate response to assertions of trade secrecy in the context of criminal justice algorithms).

[379] To date, only one court has made public the source code disclosed as part of criminal discovery. Order, United States v. Johnson, No. 1:15-CR-00565 (S.D.N.Y. Oct. 16, 2017); Kirchner, *supra* note 112. Note, however, that the software at issue in that case, FST, was not developed by a private company but rather by the New York City crime laboratory in the Office of the Chief Medical Examiner. Kirchner, *supra* note 112. Accordingly, public disclosure of this code raises somewhat different secrecy and innovation concerns.

Indeed, given current experience, it seems unlikely that a court would order source code disclosure absent a protective order. This is particularly unlikely if a private developer's assertion of trade secret protection arrives in court with trade secret status intact. For the reasons set out below, courts may have greater flexibility to order broad disclosure if other government entities have already secured the relevant disclosures by other means (e.g., as a condition of receiving a prize, grant, regulatory exclusivity, or tax benefit). *See infra* text accompanying notes 386–404. In light of the multitude of alternative innovation policy mechanisms available in this field, however, courts should be increasingly inclined to order at least some source code disclosure where relevant. *See* Wexler, *supra* note 10, at 25 ("[I]ntellectual property should not receive such special treatment."); *cf.* 3 MELVIN F. JAGER, TRADE SECRETS LAW § 27:13 (under Florida's trade secret law, "[s]uch factors as . . . protection afforded by copyright and patent laws . . . may guide the court in deciding whether to order disclosure").

[380] *Cf.* Hemel & Ouellette, *supra* note 19, at 356 ("[T]he award of a grant, prize, or tax credit should be conditioned on public disclosure to the extent that such disclosure does not significantly undermine the innovation incentive.").

[381] *See supra* text accompanying notes 166–175.

[382] Freeman, *supra* note 151, at 102.

[383] Broad disclosure coupled with alternative innovation policies may yield additional advantages. For instance, at the same time that the government invests in grants to develop new or improved criminal justice algorithms, it might pioneer new grants for outside criminal justice organizations to examine and validate those algorithms.

[384] *See supra* text accompanying notes 201–203.

Second, source code disclosure, or disclosure that a criminal justice technology is in use, may come at two different times: either when software is created or offered for sale, regardless of its acceptance in court; or when software is used in a particular case. This choice may be interdependent with the scope of disclosure. Early disclosure will likely be broader in scope, as it would not arise from a particular prosecution within which disclosure could be confined. Indeed, courts have little opportunity to opine upon or order preprosecution disclosure because court authority is limited to adjudicating the individual cases before the court. Conversely, legislatures and agencies establishing and administering innovation policies, as well as procurement offices purchasing technology, may require disclosure prior to disbursement of a reward like a prize or regulatory exclusivity, or following completion of a grant or tax credit-supported research project.

Earlier disclosure, like broad disclosure, offers several advantages over case-dependent disclosure. By the time a criminal case is underway, the government has likely already committed significant resources to selecting, buying, and learning how to use a particular piece of technology. The costs of responding to a product's failure of reliability or validity will be lower the earlier that failure is brought to light.[385] Discovering a technology failure in the midst of a criminal case is particularly costly, as that failure jeopardizes the defendant's right to a fair trial and the state's interest in prosecuting law breakers.[386] Moreover, earlier disclosure would empower courts to order source code disclosure more readily, as developers would already have traded trade secret protection for other innovation incentives. Thus, disclosure may be most efficient, and efficiently enforced, when it is required at the time a developer submits a bid for an exclusive government contract,[387] requests a necessary preapproval for sale,[388] or simply solicits sales from the state.

---

[385] *See* S.J. Liebowitz & Stephen E. Margolis, *Path Dependence, Lock-In, and History*, 11 J.L. ECON. & ORG. 205, 207 (1995) (describing third-degree path dependence, where dependence on initial conditions results in an inefficient but avoidable outcome).

[386] Consider the case of Nick Hillary. In that case, two different probabilistic genotyping software programs, TrueAllele and STRmix, returned inconsistent results about whether Hillary's DNA matched DNA recovered from a murder scene. *See* Wexler, *supra* note 10, at 23–24. In light of the inconsistent test results, the judge excluded the matching result from trial, and Hillary was acquitted. *See* Roth, *supra* note 20, at 2019–20 (describing the Hillary case).

[387] *See, e.g.*, Perlin Letter, supra note 95, at 1 (noting that the FBI proposed a "sole source contract" for probabilistic genotyping software).

[388] *See, e.g.*, Roth, *supra* note 20, at 2023 ("In the machine context, states have imposed protocols most conspicuously for breath-alcohol tests, requiring that testers use an approved machine . . . ."); Patrick, *supra* note 39 (describing Harris's efforts to obtain FCC approval to sell stingray devices to state and local law enforcement entities).

In sum, optimal disclosure would be both broad and early. Like optimal innovation policy, optimal disclosure policy is principally the province of legislators and regulators, rather than courts. Although courts may be well situated to order broad as well as party-limited disclosure, courts are not well situated to order early disclosure. As discussed below, this does not mean that judicial disclosure decisions are immaterial to achieving appropriate innovation policy.[389] But it does necessitate that optimal standard setting in this field enlist legislatures, agencies, and procurement offices in requiring broad and early disclosure as a condition of accessing innovation rewards.

C. Innovation and Judicial Disclosure Decisions

Although courts cannot command optimal disclosure or institute alternative innovation policies directly, they have a crucial role to play in bringing about appropriate and effective innovation policy. To date, courts have largely been content to defer to assertions of trade secret protection, and government entities have been keen to defend those assertions.[390] But that deference is not unalterable. Adjudicating an assertion of trade secret privilege calls for a court to balance a defendant's need for the privileged information against the likely harm from disclosure.[391] In making that determination, a court may consider whether alternative innovation incentives mitigate the risks of disclosure.[392] As set forth above, many alternative incentives already exist in the field of criminal justice algorithms.[393] If those alternative measures still come up short, they offer a ready roadmap for adapting incentives to achieve innovation without incurring the harms of secrecy.[394] Accordingly, courts need not wait for legislatures to act before ordering source code disclosure. To the contrary, courts should be emboldened by the existence of alternative innovation policy levers to reject trade secrecy in the first instance.

Indeed, there is good reason to believe that courts are the best-situated institution to initiate source code disclosure. That is so because, in many cases, the government entities responsible for supporting and procuring criminal justice technologies are not interested in disclosing those technologies to anyone. Police departments have obfuscated their use of

---

389 *See infra* Section IV.C.

390 *See supra* Part I.

391 *See* 1 JAGER, *supra* note 379, § 5:33.

392 *See id.* § 27:13; *see also* Wexler, *supra* note 10, at 43–44.

393 *See supra* Section IV.A.

394 *See id.*

technologies like stingrays.[395] The Baltimore police department declined to inform even other Baltimore public officials—including the mayor—about its use of persistent aerial surveillance and photography of the city to track and solve crimes.[396] And some state procurement offices have declined to negotiate for any access to source code in purchasing criminal justice technology like alcohol breath test devices.[397] At a minimum, courts are likely to be more interested in disclosure and constitutional assessment of these programs than are the government entities already invested in their success. Even if these entities evaluate these technologies in good faith, they will have "already deemed them valid and reliable according to whatever procurement standards apply, and will have weak incentives to identify information that could prove otherwise."[398] A court's refusal to defer to an assertion of trade secrecy enables scrutiny of criminal justice technology by the institutional participant most motivated to uncover its flaws—the defendant.

Jettisoning trade secrecy nondisclosure in a court proceeding in the first instance may yield other benefits as well. In some instances, independent bases for continued secrecy may exist. Thus, the government might seek to preserve source code secrecy not for trade secret reasons but for security reasons. Harris prevailed upon this reasoning in seeking nondisclosure about stingray devices from the FTC.[399] Law enforcement may be concerned that disclosure could enable law breakers or criminal defendants to "game" the system or circumvent surveillance technology.[400] Insofar as there are legitimate alternative bases for nondisclosure, a court-initiated process would enable those alternative bases to be litigated on their own terms.[401]

---

[395] *See* State v. Andrews, 134 A.3d 324, 327 (Md. Ct. Spec. App. 2016) (describing the state's failure to disclose the use of stingray to locate criminal defendant); *see generally* Section I.A (discussing nondisclosure of stingray use in criminal investigations).

[396] *See* Tom Dart, *Eye in the Sky: The Billionaires Funding a Surveillance Project Above Baltimore*, GUARDIAN (Oct. 15, 2016), https://www.theguardian.com/world/2016/oct/15/baltimore-surveillance-john-laura-arnold-billionaires [https://perma.cc/W8JD-PN6G] (describing the privately-funded aerial surveillance program in Baltimore).

[397] *See* Short, *supra* note 11, at 195.

[398] Wexler, *supra* note 10, at 63.

[399] *See* Harris Letter, *supra* note 13, at 1 (stating that disclosure "could cause significant harm to federal, state, and local law enforcement surveillance activities").

[400] *See* Kroll et al., *supra* note 180, at 634.

[401] It is far from clear that these alternative arguments for nondisclosure would be successful. For one thing, the pedigree of the law enforcement privilege may not be as pristine as modern cases suggest. *See* Smith, *supra* note 40, at 242–46. For another, concerns that disclosure will imperil investigative methods frequently appear overstated. Such concerns are decidedly misplaced with respect to probabilistic genotyping software because criminals are (at present) unable to alter their DNA to evade identification. Disclosure of source code for alcohol breath test devices also has not hampered their use

Finally, a court-initiated disclosure requirement is not a second best solution; rather, it is likely to be an essential first step to improved innovation policy. If courts stop deferring to assertions of trade secret protection, other government entities will need to determine whether recalibrating innovation incentives is necessary to sustain innovation in this field. In so doing, these policymakers and purchasers may conclude that broader and earlier disclosure is better, both as a matter of innovation policy and as a matter of justice.[402] After all, source code secrecy imposes harms not only on criminal defendants and the judiciary in whose courtrooms justice is meted out;[403] it also imposes harms on innovation itself, inhibiting innovation of better software and other criminal justice tools.[404] Earlier and broader disclosure may help to ensure that technologies in which the government invests considerable sums of public money is legitimate, reliable, and accurate—the better to ensure its future acceptance in individual criminal prosecutions.

Recalling the recent experience with New York City's own probabilistic genotyping software, FST, reinforces the importance of judicial decisionmaking in this arena. Although FST is a government-developed tool,[405] the city crime lab repeatedly resisted efforts to examine FST's source code in criminal cases, describing the code as "proprietary."[406] But in July 2016, a federal district court ordered the laboratory to turn FST's source code over to a defense expert for analysis, subject to a strict protective order.[407] After reviewing FST's source code, the expert concluded, "the correctness of the behavior of the FST software should be seriously questioned."[408] Not long after, the New York City crime

---

or effectiveness. *See In re* Source Code Evidentiary Hearings in Implied Consent Matters, 816 N.W.2d 525, 542 (Minn. 2012); State v. Chun, 943 A.2d 114, 159 (N.J. 2008). And the content of certain nondisclosure agreements between the FBI and law enforcement entities belies Harris's assertion of significant law enforcement secrecy concerns. *See supra* notes 54–55 and accompanying text (discussing Tucson's nondisclosure agreement, which allocates the power to determine disclosure to Harris, thus attenuating any relationship between nondisclosure and legitimate law enforcement concerns).

[402] On the importance of broad and early access to source code, see *supra* Part II and Section IV.B.

[403] *See supra* Sections II.A–B.

[404] *See* Strandburg, *supra* note 202 at 113; text accompanying notes 201–203 (discussing the relationship between disclosure and follow-on innovation).

[405] *See* ProPublica Memorandum, *supra* note 108.

[406] Kirchner, *supra* note 112 ("The office has long kept the source code secret, successfully opposing requests in court by defense attorneys to examine it."); Kirchner, *Traces of Crime*, *supra* note 91.

[407] *See* Order at 1–2, United States v. Johnson, No. 1:15-cr-00565 (S.D.N.Y. July 6, 2016); ProPublica Memorandum, *supra* note 108, at 7.

[408] Kirchner, *supra* note 112.

lab announced that it was discontinuing use of that software.[409] ProPublica subsequently sought to intervene in the case, requesting that the court lift the protective order on FST's source code and the expert analysis.[410] On October 16, 2017, the district court granted ProPublica's request.[411]

There was another significant consequence of the litigation surrounding FST: In August 2017, as ProPublica sought to unmask FST more fully, members of the New York City Council introduced a bill designed to bring greater transparency to the algorithms and other automated processing systems upon which city agencies frequently rely.[412] In December 2017, the Council passed an amended version of that bill, becoming the first U.S. jurisdiction to begin to tackle the risks arising from secrecy surrounding algorithmic decisionmaking in public life.[413]

Thus, court-initiated disclosure under a protective order was the first step in a process that culminated in the publication of the source code of an advanced criminal justice algorithm—and that spurred legislative interest in greater transparency earlier and more broadly than a court could require. The final bill that New York City approved, however, leaves much undone. Most significantly, it states that "[n]othing herein shall require . . . disclosure of any information where that disclosure would . . . result in the disclosure of proprietary information."[414] The New York City Council bill

---

[409] Kirchner, *Traces of Crime*, *supra* note 91. OCME also announced that, in place of FST, it would use the privately developed and proprietary STRmix. *Id.*

[410] ProPublica Memorandum, *supra* note 108, at 8–9.

[411] Order at 2, United States v. Johnson, No. 1:15-cr-00565 (S.D.N.Y. Oct. 16, 2017). Lauren Kirchner, *Federal Judge Unseals New York Crime Lab's Software for Analyzing DNA Evidence*, PROPUBLICA (Oct. 20, 2017), https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence [https://perma.cc/J9SF-4AVJ].

[412] N.Y.C. COUNCIL, INT. NO. 1696-2017 (N.Y. Aug. 24, 2017), http://legistar.council.nyc.gov/View.ashx?M=F&ID=5386249&GUID=24719B50-305D-486F-ACA7-3178E9F32D8B [https://perma.cc/M3D2-5N3R].

[413] *See* N.Y.C. COUNCIL, INT. NO. 1696-2017 (N.Y. Dec. 11, 2017), http://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0 [https://perma.cc/389L-972M]; *see also* Rashida Richardson, *New York City Takes on Algorithmic Discrimination*, ACLU (Dec. 12, 2017), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/new-york-city-takes-algorithmic-discrimination [https://perma.cc/L468-CF95] ("A first-in-the-nation bill, passed yesterday in New York City, offers a way to help ensure the computer codes that governments use to make decisions are serving justice rather than inequality.").

[414] *See* N.Y.C. COUNCIL, PROPOSED INT. NO. 1696-A, ¶ 6 (N.Y. Dec. 1, 2017), http://legistar.council.nyc.gov/View.ashx?M=F&ID=5678638&GUID=2E9A800E-958D-4038-A38B-4A101B740FFE [https://perma.cc/DEJ7-E5X6]. The bill as amended would do much less to further the goal of public transparency in other ways as well. In place of a requirement to publish algorithms in a publicly-accessible manner, the amended bill calls instead for the formation of a task force to consider which "agency automated decision systems" ought to be subject to transparency and disclosure requirements and to make recommendations about whether and in what form transparency and disclosure might be achieved. *Id.*

thus reaffirms the significant role that courts may play in this arena in compelling disclosure. Even though optimal innovation policy for criminal justice algorithms requires the participation of policymakers, the impetus for change may—and perhaps must—begin with courts.

CONCLUSION

The criminal justice system has experienced an explosion in the number, complexity, and use of privately developed software tools throughout the criminal justice process.[415] Police employ privately developed investigative tools to perform crucial law enforcement functions, prosecutors rely on evidence produced by complex software algorithms to win convictions, and judges trust privately developed algorithms to accurately identify the likelihood that a defendant will commit another crime in the future. Yet, frequently, the source code of these tools—their "lifeblood"[416]—and, sometimes, their very existence and use by law enforcement are shielded from scrutiny. The developers of these tools persistently and stridently assert that disclosure will injure their competitive interests. And courts have largely acquiesced, despite the significant practical and potentially constitutional costs of such secrecy to individual defendants, the criminal justice system, and the development of well-designed criminal justice algorithms more broadly.

That is the law as it is; but that acquiescence is not inevitable. The government has at its disposal a multitude of alternative policy mechanisms to spur innovation, none of which mandate secrecy and most of which will easily accommodate a robust disclosure requirement. Several of these mechanisms are already in use, encouraging innovation through research and development grants and exclusive procurement contracts. Recalibrating the non-trade-secret rewards for innovation is likely to be particularly efficient and effective in this field, where government is both a funder of research and the primary purchaser of criminal justice algorithms. In sum, innovation does not require secrecy. Where, as here, secrecy imposes significant systemic costs, secrecy must go.

---

[415] *See* Roth, *supra* note 20, at 1975.

[416] Imwinkelried, *supra* note 8, at 98–99.