UNIVERSITY OF PITTSBURGH LAW REVIEW
Vol. 84 ● Summer 2023

NOTES

CRIMINAL JUSTICE TECHNOLOGY AND THE REGULATORY SANDBOX: TOWARD BALANCING JUSTICE, ACCOUNTABILITY, AND INNOVATION

Matthew C. Christoph

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

NOTES

CRIMINAL JUSTICE TECHNOLOGY AND THE REGULATORY SANDBOX: TOWARD BALANCING JUSTICE, ACCOUNTABILITY, AND INNOVATION

Matthew C. Christoph*

Table of Contents

* J.D., 2023, University of Pittsburgh School of Law. My deepest gratitude to my wife, Kristi, for her encouragement and unending support. Many thanks to Alec Bosnic, Kaitlin Kramer Tear, Gaurav Gupte, Elliot DiGioia, Desiree Bsales, and all of the *Pitt Law Review* staff members whose hard work and keen insights improved this Note tremendously.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

INTRODUCTION

The increasing use of technology, data, and artificial intelligence in the public sector brings potential for both great risk and great reward.[1] This trend carries significant implications for public interests; civil and constitutional rights; local, state, and federal justice systems; private and public economic interests; scientific advancement; and technological innovation. Looking specifically at the criminal justice system, privately developed software and hardware for purposes such as surveillance and intelligence gathering, predictive policing, forensic analysis, or automated decision making are increasingly used by law enforcement agencies and courts at local, state, and federal levels.[2] But despite the risk of serious harm to civil liberties, public interests, and the integrity of our government and justice system, essential questions about these technologies—such as whether these proprietary tools are really as capable and accurate as their proponents claim—remain unanswered.[3] Americans from across the political spectrum have been calling for governmental institutions and law enforcement agencies to ensure transparency and accountability, root out biases, and otherwise fulfill the guarantee of equal justice for all under the law.[4] However, emerging technologies placed in the hands of state

[1] *See, e.g.*, Hannah Bloc-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1273–90 (2020) (discussing the growing use of algorithms in public governance, administration, and decision making with regard to public benefits, education, and criminal justice).

[2] *See* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1346 (2018).

[3] *See* Stephanie J. Lacambra et al., *Opening the Black Box: Defendants' Rights to Confront Forensic Software*, 42 CHAMPION, May 2018, at 28, 29–32; Jessica Pishko, *The Impenetrable Program Transforming How Courts Treat DNA Evidence*, WIRED (Nov. 29, 2017, 7:00 AM), http://www.wired.com/story/trueallele-software-transforming-how-courts-treat-dna-evidence.

[4] *See, e.g.*, Danielle L. Macedo, *What Kind of Justice is This? Overbroad Judicial Discretion and Implicit Bias in the American Criminal Justice System*, 24 J. GENDER, RACE & JUST. 43, 47 (2021) ("Studies show judges hold unconscious or implicit biases and that those biases can negatively influence their judgment and decision making."); Tracey L. Meares, *The Path Forward: Improving the Dynamics of Community-Police Relationships to Achieve Effective Law Enforcement Policies*, 117 COLUM. L. REV. 1355, 1363 (2017) ("[Citizens] want to trust that the motivations of the authorities are sincere and well intentioned . . . that the authority they are dealing with believes that they count and cares about them."); REPUBLICAN STAFF OF H.R. COMM. ON THE JUDICIARY, 117TH CONG., FBI WHISTLEBLOWERS: WHAT THEIR DISCLOSURES INDICATE ABOUT THE POLITICIZATION OF THE FBI AND JUSTICE DEPARTMENT 4 (2022) ("The FBI has the power, quite literally, to ruin a person's life—to invade their residence, to take their property, and even to deprive them of their liberty. The potential abuse of this power, or even the appearance of abuse, erodes the fundamental principle of equality under the law and confidence in the rule of law."); Andrew C. McCarthy, *How to Fix the FBI*, NAT'L REV. MAG., Nov. 7, 2022, at 26; Shiam Kannan, *A Conservative Approach to Police Reform*, CORNELL L. REV. (July 23, 2020), http://www.thecornellreview.org/a-conservative-approach-to-police-reform (arguing for implementation of

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

actors and the protective shroud that these tools have been afforded could be outpacing some of our most essential juridical principles and safeguards against governmental overreach and interference—at least for now.[5]

A critical point of conflict in "criminal justice tech" lies where third-party software or hardware systems become involved in court proceedings, yet nondisclosure agreements, intellectual property protections, and other impediments to scrutiny have been invoked to block discovery requests or prevent the confrontation of evidence at trial.[6] Much has already been written on the potential injustices, rights violations, and ethical failures which may result if economic and proprietary interests can override critical civil and constitutional protections afforded to criminal defendants through disclosure, discovery, and confrontation.[7] But compelling policy arguments should also be made for vetting these technologies *before* they are purchased and deployed—through disinterested scientific testing, verification of methodology and results, or other means of objective examination and evaluation by qualified experts.[8]

And yet, having acknowledged the risks, the potential for significant benefits from technological innovation in the justice system should also be noted. Careful,

---

reform measures—including that the conservative view "that public sector workers shouldn't be able to unionize" should logically extend to police unions, too).

[5] *See* Lacambra et al., *supra* note 3, at 38 ("Probabilistic DNA-matching programs are only one example of a forensic technology that embodies potentially flawed assumptions that could cause the wrong person to be imprisoned or executed."); Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183, 1189 (2019) (positing that state actors' use of proprietary code is encroaching "upon our everyday lives without transparency or accountability" and becoming "an everyday reality for criminal defendants and others who are swept up by the specter of automated government decision making"); Kit Walsh, *Shining a Light on Black Box Technology Used to Send People to Jail*, ELEC. FRONTIER FOUND. (Dec. 31, 2021), https://www.eff.org/deeplinks/2021/12/shining-light-black-box-technology-used-send-people-jail-2021-year-review (citing two instances where, despite rulings ordering disclosure of forensic software, "the prosecution decided to withdraw the evidence to avoid disclosure" or "handed over unusable and incomplete code fragments").

[6] *See, e.g.*, Natalie Ram, *Innovating Criminal Justice*, 112 NW. U. L. REV. 659, 665–71 (2018) (describing nondisclosure agreements between police departments and a surveillance device manufacturer); Edward J. Imwinkelried, *Computer Source Code: A Source of the Growing Controversy over the Reliability of Automated Forensic Techniques*, 66 DEPAUL L. REV. 97, 111, 124–25 (2016) (discussing denials of discovery requests for breath-testing devices and genotyping software source code). *See generally* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 1979, 2022–53 (2017) (proposing an evidentiary framework for proprietary "machine conveyances" when used in court as "credibility-dependent proof").

[7] In addition to the articles mentioned in the previous footnote, see, for example, Wexler, *supra* note 2; Katyal, *supra* note 5; Lacambra et al., *supra* note 3.

[8] *See infra* Part II.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

results-focused implementation of reliable and accurate systems could counteract human biases, improve the quality of evidentiary analysis, increase administrative efficiency, improve judicial decision making, or otherwise serve the interests of good governance and justice.[9] Mandatory disclosure of source code and development data under a strict transparency regime may cause a resulting loss of economic incentives, whereby progress and innovation (at least from the private sector) might decline or even disappear.[10] Thus, the development and implementation of new technology for law enforcement agencies or the courts should neither be roundly rejected nor necessarily conditioned on the sort of full transparency and public disclosure that could potentially amount to the forfeiture of valuable property rights.

Still, any purported advancement in this space should be carefully considered, as it could be a double-edged sword. For state actors, the acquisition and deployment of criminal justice tech should be transparent and carefully structured so as to reap any possible rewards while minimizing risks and avoiding damage to the integrity of the criminal justice system and harm to the people it exists to serve and protect. Issues presented by technology in criminal justice are complex and far-reaching—and, therefore, will require a novel, adaptable, and cooperative approach to realize benefits and minimize harm. This Note proposes that a responsible framework for the authentication and implementation of criminal justice tech may best be achieved through the establishment of a federal regulatory sandbox program specifically designed for that purpose.

A regulatory sandbox is a controlled regulatory environment where the regulated entities can bring innovations to market with "fewer regulatory constraints, real customers, less risk of enforcement action, and ongoing guidance from regulators[.]"[11] As part of a measured and careful rollout of new products or services, program participants agree to share information with regulators regarding the product's design and performance and all involved can carefully monitor impacts on

[9] Arthur Rizer & Caleb Watney, *Artificial Intelligence Can Make Our Jail System More Efficient, Equitable, and Just*, 23 TEX. REV. L. & POL. 181, 183 (2018); *see also* Mirko Bagaric et al., *Erasing the Bias Against Using Artificial Intelligence to Predict Future Criminality: Algorithms Are Color Blind and Never Tire*, 88 U. CIN. L. REV. 1037 (2020).

[10] *Cf.* Elizabeth A. Rowe, *Striking a Balance: When Should Trade-Secret Law Shield Disclosures to the Government?*, 96 IOWA L. REV. 791, 800–01 (2011) ("If a company submitted trade-secret . . . was disclosed by the government to the public, it is the trade-secret owner who would ultimately bear the cost of the government's misguided action. This is in part because when a trade secret is revealed, it loses all of its value, the loss is irreparable, and the company may not be made whole by monetary damages.").

[11] Hilary J. Allen, *Regulatory Sandboxes*, 87 GEO. WASH. L. REV. 579, 580 (2019).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

consumers, industries, and other stakeholders.[12] Like regulatory sandbox programs in numerous jurisdictions that have recently been adopted for emerging technology in the areas of tech-based financial services ("fintech")[13] or legal services,[14] a sandbox for criminal justice tech—when properly designed and executed—could be a major step toward balancing interests of private enterprise and innovation with law and order, civil rights, and the public good.

Part I of this Note discusses some of the major concerns regarding private technology as used by law enforcement and the criminal court system. In Part II, public interests and ethical implications are briefly considered. Part III examines some of the arguments supporting the implementation of criminal justice tech often put forth by developers or other proponents, as well as arguments in support of the trade secret protection afforded to these technologies. Part IV will then make the case for a regulatory solution in this space. But, as opposed to more typical administrative agency procedures, the solution proposed is arguably more responsive and collaborative, and therefore will perhaps be more appealing to regulators and regulated entities alike. This proposed solution is a regulatory sandbox for criminal justice technology.

---

[12] Brian R. Knight & Trace E. Mitchell, *The Sandbox Paradox: Balancing the Need for Innovation with the Risk of Regulatory Privilege*, 72 S.C. L. REV. 445, 449 (2020).

[13] Although initiatives in the United States thus far have been more exploratory in nature, fintech sandboxes have already been adopted in a number of global financial centers, most notably London, but also in Canada, Australia, Hong Kong, Singapore, the Netherlands, Switzerland, and the United Arab Emirates. Allen, *supra* note 11, at 592.

[14] For tech-based legal services, a number of states including California, Washington, Illinois, Florida, and North Carolina have at least explored the concept of regulatory sandboxes or similar laboratory programs to facilitate innovation and regulatory reform in the legal industry. *See* Zacharia DeMeola, *Justice Gap Demands Look at New Legal Service Models*, LAW360 (Sept. 17, 2021, 5:14 PM), https://www.law360.com/articles/1422816/justice-gap-demands-look-at-new-legal-service-models; *see also* Sam Skolnik, *Florida Joins States in Testing Law Firm Ownership Models*, BLOOMBERG L. (June 29, 2021, 3:44 PM), https://news.bloomberglaw.com/us-law-week/florida-joins-states-in-testing-new-law-firm-ownership-models (discussing Florida's proposed Law Practice Innovation Laboratory Program, designed to "collect data on non-traditional legal services providers as the program goes forward to determine which types of models work—and to make sure each company is safe for legal consumers to use."). However, at the time of this writing, the proposed program appears to be going nowhere; although initially included among a number of recommendations made by the Florida Bar's Special Committee to Improve the Delivery of Legal Services, adoption of the program was later declined by the Florida Supreme Court. *See* Letter from John A. Tomasino, Clerk of Ct., Sup. Ct. of Fla., to Joshua E. Doyle, Exec. Dir., Fla. Bar (Mar. 3, 2022), https://www.abajournal.com/files/Florida_Supreme_Court_letter.pdf.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

I. ISSUES RELATING TO JUSTICE AND SYSTEMIC INTEGRITY

New technologies for the automation of data analysis and decision making are increasingly prevalent throughout the public sector.[15] While there may be operational and administrative benefits in the automation of some governmental functions, serious concerns exist in areas where civil liberties and individual rights are at stake, and where the transparency, reliability, or accountability of these technologies may be lacking.[16] Without deliberate efforts to the contrary, data analysis and decision-making technologies may reinforce biases, foster inequality, or otherwise lead to improper outcomes in critical areas of public concern such as housing, employment, or education.[17]

The trend toward automation of the criminal justice system has especially serious implications.[18] Experts have pointed to biases,[19] inaccuracies,[20] and unconfirmed or undisclosed methods inherent in many technologies that have already been, and continue to be, implemented across the country.[21] Law enforcement entities use algorithms and machine learning systems to predict crime,

---

[15] *E.g.*, Noah Bunnell, *Remedying Public-Sector Algorithmic Harms: The Case for Local and State Regulation via Independent Agency*, 54 COLUM. J.L. & SOC. PROBS. 261, 269 (2021).

[16] *Id.* at 270–71.

[17] Dominique Harrison, *Civil Rights Violations in the Face of Technological Change*, ASPEN INST. (Oct. 22, 2020), https://www.aspeninstitute.org/blog-posts/civil-rights-violations-in-the-face-of-technological-change.

[18] KEVIN STROM, RTI INT'L, RESEARCH ON THE IMPACT OF TECHNOLOGY ON POLICING STRATEGY IN THE 21ST CENTURY 2-2–2-3 (2016), Nat'l Crim. Just. Reference Serv. 251140 [hereinafter STROM, IMPACT OF TECHNOLOGY ON POLICING STRATEGY], https://www.ojp.gov/pdffiles1/nij/grants/251140.pdf (finding that "state and local [law enforcement agencies] are heavily involved in technology[,]" and "technology use is expected to increase not only among the largest agencies but across most U.S. [law enforcement agencies.]"); Wexler, *supra* note 2, at 1346 ("At every stage—policing and investigations, pretrial incarceration, assessing evidence of guilt at trial, sentencing, and parole—machine learning systems and other software programs increasingly guide criminal justice outcomes."); *see also* Bernard Marr, *The 5 Biggest Tech Trends in Policing and Law Enforcement*, FORBES (Mar. 8, 2022, 2:09 AM), https://www.forbes.com/sites/bernardmarr/2022/03/08/the-5-biggest-tech-trends-in-policing-and-law-enforcement (listing smart device data, computer vision, robotics, digital twins, and virtual reality and augmented reality as the five biggest tech trends in policing and law enforcement).

[19] *See* Harrison, *supra* note 17 (discussing how predictive policing algorithms disproportionately focused police activity on poor communities and people of color).

[20] Fabbio Bacchini, *Race Again: How Face Recognition Technology Reinforces Racial Discrimination*, 17 J. INFO., COMMC'N & ETHICS SOC'Y 321, 324 (2019) (citing significant rates of error in facial recognition technology for African Americans, females, and individuals eighteen to thirty years of age).

[21] Lacambra et al., *supra* note 3, at 32.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

identify suspects, or otherwise direct investigation or enforcement activity.[22] Similar technologies are being used by courts in determining an individual's sentence or assessing whether to grant them bail or parole.[23] Forensic analysis of evidence is becoming increasingly automated, particularly with the analysis of DNA samples, fingerprints, and ballistics.[24] If these trends persist without objective examination and sufficient safeguards in place to verify that these tools are reliable and accurate—both in design and in application—the automation of criminal justice could have seriously detrimental implications for individual rights, the integrity of our justice system, and fundamental values of the system itself.[25]

Any technology has the potential for bugs, flawed methodology, or otherwise unsound programming or manufacturing, leading to undesirable outcomes which could range from inaccurate results to total system failures.[26] Human error may also skew results or misinterpret them, especially if operators lack necessary training, direction, or oversight when using these systems.[27] And there could always be the potential for manipulation or abuse by bad actors. These undesirable outcomes could be hugely impactful, especially when technologies are instituted on a large scale or are used in particularly sensitive contexts.[28]

---

[22] Wexler, *supra* note 2, at 1346–48.

[23] *Id.*

[24] *Id.*

[25] *See, e.g.*, Wexler, *supra* note 2, at 1364–67 ("[L]aw enforcement agencies and third-party developers will try to use intellectual property law as a shield against judicial scrutiny [of] the constitutionality and lawfulness of new investigative technologies.").

[26] Lacambra et al., *supra* note 3, at 28–29.

[27] Bacchini, *supra* note 20, at 325.

[28] *See* Lacambra et al., *supra* note 3, at 30 (citing examples of major software flaws at NASA, an Irish medical imaging system, and a major Australian bank). Elsewhere, a Texas company's IT system developed for the United Kingdom's Child Support Agency, at an overall cost of over £1.1 billion, caused "enormous operational difficulties" and "genuine hardship and distress to many parents and their children" and was described as one of the "worst public administration scandals in modern times." Andy McCue, *Child Support IT Failures Savaged*, ZDNET (July 3, 2006), https://www.zdnet.com/article/child-support-it-failures-savaged. A financial services firm lost upwards of $440 million in less than one hour when a software glitch rapidly bought and sold millions of shares of stock. Nathaniel Popper, *Knight Capital Says Trading Glitch Cost it $440 Million*, N.Y. TIMES: DEALBOOK (Aug. 2, 2012, 4:01 PM), https://archive.nytimes.com/dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million. *See generally* Simson Garfinkel, *History's Worst Software Bugs*, WIRED (Nov. 8, 2005, 2:00 AM), https://www.wired.com/2005/11/historys-worst-software-bugs.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

Systems based on data analysis, machine learning, or artificial intelligence are equally fallible in comparison to coded software, as they are trained on historical data sets or examples curated and fed into that system by programmers.[29] These data sets may be incomplete, inaccurate, biased, or otherwise flawed.[30] Facial recognition software, for example, has shown substantially diminished accuracy in identifying people with dark skin tones, women, and individuals between eighteen to thirty years of age; studies have shown that skewed data sets are at least part of the problem.[31] Algorithm-based predictive policing programs and criminal databases in Chicago and Los Angeles were shown, even by internal reports, to be subject to numerous flaws and inaccuracies.[32] For example, when a predictive policing system used by Chicago police was trained on "dirty data," including false reports, targeted stops, and unconstitutional searches, it produced a skewed forecast of criminal activity which reinforced and perpetuated a disproportionate concentration of police in minority communities.[33]

Algorithms and machine learning programs are utilized in the courts, as well. Given the high stakes involved in a criminal proceeding, one might expect robust scrutiny to be the norm wherever private technology is implicated in connection with a given defendant's innocence or lack thereof. Disturbingly, the opportunity to evaluate or independently verify the reliability of such systems may be routinely denied to those who need it most.[34] Defense counsel have been deprived of fundamental information about these technologies, their methodology, and the underlying source code or algorithms, even where such denials were directly impeding counsel's ability to mount adequate defenses.[35] Independent review and

[29] Lacambra et al., *supra* note 3, at 33.

[30] *Id.*

[31] Bacchini, *supra* note 20, at 324.

[32] CHI. OFF. OF INSPECTOR GEN., REVIEW OF THE CHICAGO POLICE DEPARTMENTS GANG DATABASE 43–47 (2019), https://igchicago.org/wp-content/uploads/2019/04/OIG-CPD-Gang-Database-Review.pdf (finding a lack of "sufficient controls in generating, maintaining, and sharing" data, and that "information practices lack procedural fairness protections" and "raise significant data quality concerns"); L.A. POLICE COMM'N, REVIEW OF SELECTED LOS ANGELES POLICE DEPARTMENT DATA-DRIVEN POLICING STRATEGIES 1, 16 (2019), http://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf (finding "data anomalies" and "significant inconsistencies" in its Chronic Offender Program data).

[33] Rashida Richardson et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. ONLINE 16, 28–34 (2020).

[34] Lacambra et al., *supra* note 3, at 29.

[35] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

testing is often vehemently resisted by developers and vendors, denying defense experts the opportunity to examine the designs and inner workings of these systems or to independently authenticate the results.[36] Without inspecting and objectively testing these systems and verifying the soundness of each system's methodology, source code, and development or training data, the soundness of the analysis conducted or results rendered by these systems cannot be ensured.[37]

For the sake of comparison, consider the applicable rules for admitting expert testimony in federal court. Federal Rule of Evidence 702 requires thorough scrutiny in determining whether to allow an expert witness to offer their testimony.[38] If an expert is "qualified" to do so, meaning they possess "scientific, technical, or other specialized knowledge," an expert may testify so long as the testimony is "based on sufficient facts or data" that is "the product of reliable principles and methods . . . reliably applied . . . to the facts of the case."[39] In other words, a court must ensure the reliability of the theory, methodology, and procedure used to reach any expert opinion that is offered at trial.[40] And even though an expert—if their testimony is first deemed admissible—is not necessarily required to testify to underlying facts or data before testifying as to their opinion, "the expert may be required to disclose those facts or data on cross-examination."[41] Therefore, it would not be permissible for an expert to testify, for example, that a defendant's DNA matched evidence from a crime scene, yet refuse to explain on cross-examination the methodology used to

[36] *Id.*; *see also* Wexler, *supra* note 2, *passim*.

[37] Lacambra et al., *supra* note 3, at 38.

[38] FED. R. EVID. 702(a)–(d).

[39] *Id.* The rules govern in federal courts and most states follow a similar approach in accord with their own similar, if not identical, rules of evidence, as well as the standard from *Daubert v. Merrell Dow Pharmaceuticals*. Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 592–94 (1993) (holding trial courts must examine whether the testimony's underlying "reasoning or methodology . . . is scientifically valid and . . . properly can be applied to the facts" by considering (1) whether the theory or technique in question can be (and has been) tested; (2) whether it has been subjected to peer review and publication; (3) its known or potential error rate and the existence and maintenance of standards controlling its operation; (4) and whether it has attracted widespread acceptance within a relevant scientific community). However, some jurisdictions may still follow the "general acceptance" test of *Frye v. United States*, whereby the validity of the basis for any scientific testimony requires that it be "sufficiently established to have gained general acceptance in the particular field in which it belongs." 293 F. 1013, 1014 (D.C. Cir. 1923).

[40] *See, e.g.*, *In re* Paoli R.R. Yard PCB Litig., 35 F.3d 717, 745 (3d Cir. 1994) ("*[A]ny* step that renders the analysis unreliable . . . renders the expert's testimony inadmissible. This is true whether the step completely changes a reliable methodology or merely misapplies that methodology.").

[41] FED. R. EVID. 705.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

make that determination and deny the defense access to any underlying analytical data.[42] Similarly, the soundness of the underlying methodologies of third-party technology should not be allowed to evade scrutiny, either.

Another relevant point of comparison is the manual analysis of forensic evidence. Despite its prevalence in pop culture portrayals of police work or court proceedings and frequent coverage in the news,[43] forensic science has long been recognized as inconsistent and potentially problematic, if not entirely dubious in some instances.[44] The Supreme Court previously indicated the importance of ensuring that forensic evidence does not escape inquiry and confrontation at trial.[45] The Court stated in *Melendez-Diaz v. Massachusetts* that confrontation of forensic evidence and the analysts who offer it "is designed to weed out not only the fraudulent analyst, but the incompetent one as well."[46] Likewise, any technology used to produce evidence against a defendant should be subject to discovery, scrutiny, and confrontation. Ideally, methods and results should be thoroughly vetted and authenticated before the purchase and implementation of any such system but especially before giving technology an outsized effect upon any individual's due process rights and civil liberties.

A foundational tenet of our society is that the people are guaranteed an open and fair criminal justice system.[47] Yet some courts have seemingly allowed the intellectual property rights of private companies to override individuals' due process

---

[42] *See id.*

[43] DAVID A. HARRIS, FAILED EVIDENCE: WHY LAW ENFORCEMENT RESISTS SCIENCE 1–3 (2012) (and accompanying notes); Kimberlianne Podlas, *The "CSI Effect" and Other Forensic Fictions*, 27 LOY. L.A. ENT. L. REV. 87, 89 (2006); Tom. R. Tyler, *Viewing CSI and the Threshold of Guilt: Managing Truth and Justice in Reality and Fiction*, 115 YALE L.J. 1050 (2006).

[44] *See* NAT'L RSCH. COUNCIL, STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD (2009) (finding substantial reasons to doubt the methodology or reliability of many forensic "disciplines" and calling for independent regulation); Jennifer E. Laurin, *Remapping the Path Forward: Toward a Systemic View of Forensic Science Reform and Oversight*, 91 TEX. L. REV. 1051, 1059–64 (2013) (pointing to systemic issues including "a history of competition with other police divisions for limited resources; failure to hire, train, and retain qualified analysts; and caseload pressures that exacerbated other organizational deficiencies to further cause slipshod work and enhance analysts' vulnerability to pressure from police and prosecutors"); Michael J. Saks & Jonathan J. Koehler, *What DNA "Fingerprinting" Can Teach the Law About the Rest of Forensic Science*, 13 CARDOZO L. REV. 361, 372 (1991) ("[M]ost forensic sciences . . . have not yet been verified by empirical testing.").

[45] Melendez-Diaz v. Massachusetts, 557 U.S. 305, 327 (2009).

[46] *Id.*

[47] *E.g.*, U.S. CONST. amends. VI, XIV, § 1.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

rights.[48] There have, of course, been some favorable rulings for defendants,[49] but courts of various jurisdictions continue to reach disparate results, which, even within the same state, may be inconsistent and unpredictable.[50] Examples of patently unfair outcomes allowing intellectual property and underlying economic concerns to prevail over defendants' constitutional rights are not difficult to find. At one New York hearing, an inmate was denied parole, despite being able to prove that inaccurate information about him had been fed into the risk assessment algorithm.[51] Because the developer invoked trade secret protection and would not disclose how this demonstrably false data was weighted as an input of the algorithm, the individual could not prove that the false data had been significant enough to invalidate that algorithm's decision to deny parole.[52]

Adding insult to injury in such cases, the discovery of trade secrets that is often denied to criminal defendants has been granted in civil cases where only financial interests are at stake.[53] One scholar argues, in a thorough and detailed recounting of its development, that a so-called "trade secret privilege" to withhold information in a criminal trial—even from review under protective order—has been supported by authority seemingly manufactured out of whole cloth within the past few decades.[54] Others have argued that withholding this information is antithetical to the

[48] Wexler, *supra* note 2, at 1355.

[49] United States v. Ellis, No. 19-369 (W.D. Pa. Feb. 26, 2021) (memorandum order denying motion to quash the defense's subpoena of forensic software source code and ordering disclosure under protective order) (quoting, as persuasive authority, State v. Pickett, 246 A.3d 279, 284 (N.J. Super. Ct. App. Div. 2021), which stated in part, "[i]n appropriate circumstances, especially where civil liberties are on the line, independent source-code review is critical when determining reliability . . . . Fundamental due process and fairness demand access.").

[50] *Compare* the order in *Ellis*, slip op. at 1, requiring the forensic software developer to disclose proprietary source code and finding it "central to the case against Defendant," *with* Commonwealth v. Robinson, No. CC 201307777, 2016 Pa. Dist. & Cnty. Dec. LEXIS 21764, at *2–3 (Ct. Com. Pl. Feb. 4, 2016) (memorandum order), finding that the same forensic software's source code was "not material to the defendant's ability to pursue a defense" and that ordering disclosure "would be unreasonable, as release would have the potential to cause great harm to [the developer]." Curiously, after dismissing the source code as "not material" to the defense, the court points out that, rather than disclose the code, the developer could just "decline to act as a Commonwealth expert, thereby seriously handicapping the Commonwealth's case." *Id.*

[51] Rebecca Wexler, *Code of Silence*, WASH. MONTHLY (June 11, 2017), https://washingtonmonthly.com/2017/06/11/code-of-silence.

[52] *Id.*

[53] Wexler, *supra* note 2, at 1401.

[54] *Id.* at 1377–96.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

fundamental values of due process and individual civil rights.[55] Furthermore, critics say that depriving defendants of the ability to confront "secret" evidence used against them may signal that the justice system values private economic interests more than ensuring just and fair outcomes for defendants and adhering to the tenets on which our courts are founded.[56]

II. PUBLIC INTERESTS AND ETHICAL CONSIDERATIONS

Of primary concern is the legitimacy of the criminal justice system. It is critical that the people the system serves perceive it, on balance, to be fair, accountable, and in keeping with the ethical and legal principles to which our system of government has always aspired. The Constitution guarantees each individual's rights to life, liberty, and property.[57] It has been said that the order in which these rights are listed is by no means arbitrary or accidental; these rights are listed in a ranked hierarchy of importance, with life as the most essential, liberty the second-most, and property rights as the least important of the three.[58] Where there is conflict with property rights, the right to life or liberty should always prevail over property.[59] In other words, where there is conflict, one's property rights must succumb to the other, superior rights.[60] For centuries, moral and political philosophy[61] and the common

[55] *Id.*; *see also* Katyal, *supra* note 5; Lacambra et al., *supra* note 3; Steven M. Bellovin et al., *Seeking the Source: Criminal Defendants' Constitutional Right to Source Code*, 17 OHIO ST. TECH. L.J. 1 (2021); Vera Eidelman, *The First Amendment Case for Public Access to Secret Algorithms Used in Criminal Trials*, 34 GA. ST. U. L. REV. 915 (2018).

[56] Wexler, *supra* note 2, at 1395.

[57] U.S. CONST. amends. V, XIV.

[58] *See, e.g.*, John William Draper, *Preserving Life by Ranking Rights*, 82 ALB. L. REV. 157, 182 (2018).

[59] *Id.*

[60] *Id.*

[61] *E.g.*, JOHN LOCKE, TWO TREATISES OF GOVERNMENT 188 (Peter Laslett ed., Cambridge Univ. Press 1970) (1690) ("As *Justice* gives every Man a Title to the product of his honest Industry, and the fair Acquisitions of his Ancestors descended to him; so *Charity* gives every Man a Title to so much out of another's Plenty, as will keep him from extream want, where he has no means to subsist otherwise: and a Man can no more justly make use of another's necessity, to force him to become his Vassal, by with-holding that Relief, God requires him to afford to the wants of his Brother, than he that has more strength can seize upon a weaker, master him to his Obedience, and with a Dagger at his Throat offer him Death or Slavery.").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

law[62] have firmly recognized this hierarchy of life and liberty over property rights.[63] It follows that intellectual property rights should not be allowed to supersede due process rights, especially in a capital case.

Second, from a public policy standpoint, proper oversight and vetting of proprietary, for-profit technology vendors is necessary to serve the people's interest in the fiscally responsible and accountable use of public funds.[64] As these technologies are purchased by public sector institutions and are then used by civil servants to investigate or prosecute members of the public, all at the taxpayers' expense, society should—as of right—expect that these systems be scientifically proven to produce accurate and reliable results before they are purchased and used.

Like most advanced systems, these technologies are not cheap. For example, although pricing information is not generally available to the public, TrueAllele, a forensic analysis software used in crime labs around the country, was estimated by one source in 2017 to cost roughly $60,000 per individual license.[65] Dating from 2012, an internal procurement document from the California Department of Justice, obtained through a Freedom of Information Act request by the Electronic Privacy Information Center, lists a four-station TrueAllele system and two "Long Distance Training" sessions as costing over $220,000.[66] Cybergenetics, the company that developed TrueAllele, has asserted that disclosure and independent testing is not necessary because its own internal validation studies have proven that the software is accurate.[67] The obvious counterargument is that unpublished studies performed or

[62] *See, e.g.*, Ploof v. Putnam, 71 A. 188 (Vt. 1908) ("This doctrine of necessity applies with special force to the preservation of human life. One assaulted and in peril of his life may run through the close of another to escape from his assailant. One may sacrifice the personal property of another to save his life or the lives of his fellows.") (citation omitted).

[63] Draper, *supra* note 58, at 182–86.

[64] *See* STROM, IMPACT OF TECHNOLOGY ON POLICING STRATEGY, *supra* note 18, at 2–3 (noting that "law enforcement technology adoption is often ad hoc and not based on longer-term planning" and shows a "tendency to purchase technology without a clear, strategic plan").

[65] Pishko, *supra* note 3.

[66] Cal. Dep't of Just., *Cybergenetics: TrueAllele DNA Casework System Justification for Non-competitive Procurement*, EPIC.ORG (Mar. 12, 2012), https://archive.epic.org/state-policy/foia/dna-software/EPIC-16-02-02-CalDOJ-FOIA-20160219-Procurement-Justification-TrueAllele.pdf.

[67] Pishko, *supra* note 3.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

funded by the same company producing and selling the technology in question do not suffice as objective proof that the software renders accurate, reliable results.[68]

A tool should satisfy a need, bestow some sort of benefit, or both. A basic cost-benefit analysis would dictate that a tool is only worth buying if it does what it says it does and is expected to do. If a tool turns out to be defective, the cost of acquiring it is only the beginning—the additional cost of any harms caused by its failings will compound the loss.

In one such instance, a proprietary forensic software was developed at substantial expense and used in the lab of New York City's Office of the Chief Medical Examiner for years.[69] The office consistently and successfully (and at additional expense to taxpayers) fought against any independent examination of the software code, even if under protective order.[70] Although the lab had been heralded as pioneering the analysis of complex DNA evidence, significant doubts about its reliability grew over time.[71] After a court order finally made the software available for objective review and testing, it was shown to be seriously flawed, casting doubt over thousands of verdicts; ultimately, the software was abandoned.[72] The Office of the Chief Medical Examiner reportedly then replaced its proprietary software with STRmix.[73]

STRmix is a DNA sequencing software. After widespread use, independent testing found STRmix to have produced false results in at least sixty out of some 4,500 court cases that were retrospectively examined.[74] In addition to the bare injustice done to those sixty individuals, consider the implications for the court system and the taxpayers if hundreds or thousands of defendants suddenly had

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] 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.

[72] Pishko, *supra* note 3; *see also* Lauren Kirchner, *Federal Judge Unseals New York Crime Lab's Software for Analyzing DNA Evidence*, PROPUBLICA (Oct. 20, 2017, 8:00 AM), https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence.

[73] Lauren Kirchner, *Powerful DNA Software Used in Hundreds of Criminal Cases Faces New Scrutiny*, THE MARKUP (Mar. 9, 2021, 8:00 AM), https://themarkup.org/news/2021/03/09/powerful-dna-software-used-in-hundreds-of-criminal-cases-faces-new-scrutiny.

[74] Lacambra et al., *supra* note 3, at 32.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

grounds to appeal or to retry their cases due to a commercial software's inaccurate results. Extrapolated out to numerous court systems across the country, the cost could be staggering. Worse still, it might have been avoided if proper proof of concept had been made a prerequisite to the acquisition of high-cost, high-risk technology.

To prevent societal harm and systemic injustice, there is a strong case to be made that thorough, unfettered examination is needed to pre-screen criminal justice tech before it is purchased and implemented. User-level access to software and algorithms would at least allow for the running of test cases and the comparing of results to control samples. This form of screening, however, would still constitute a relatively limited review and may not detect latent bugs or inherent errors.[75] A deeper dive into the programming and source code of these programs could examine the underlying instructions or data sets that generate the final results.[76] Examiners may discover bugs in the programming that simple, user-level interactions with the software may not detect and might identify where and how the software encounters an error or reaches a result that is less than optimal.[77] But without systemic changes to the current status quo of private-public tech relationships and bureaucratic purchasing behavior,[78] we may never be certain that technology is reliable and accurate enough to be worth the high costs associated with its acquisition and use, let alone the even higher costs implicated if potential flaws become manifest. For that sort of assurance, the cooperation of developers and rightsholders is essential.

[75] *Id.* at 29–30.

[76] *Id.* at 30.

[77] *Id.*

[78] *See* STROM, IMPACT OF TECHNOLOGY ON POLICING STRATEGY, *supra* note 18, at 2–3 ("As a whole, our findings demonstrate that law enforcement technology adoption is often ad hoc and not based on longer-term planning. The tendency to purchase technology without a clear, strategic plan can result in limited integration within the agency and a failure to recognize the primary or secondary benefits of the technology. These factors can lead to disillusionment and a lack of continuation funding for maintaining or updating particular types of technology."). Although the report made this general assessment in its executive summary, there were bright spots in the body of the report. In particular, a distinction was made between "high-impact" and "mixed-impact" agencies, where high-impact agencies "formed working groups[,] . . . conducted pilot studies[,] test[ed] in the field[,]" and "emphasized the importance of researching or vetting different vendors[,]" while mixed-impact agencies "often qualified their acquisition and implementation processes as 'opportunistic' or 'reactive.'" *Id.* at 6–32. Additionally, the report noted that "[o]ne mixed-impact agency described its technology implementation strategy as a 'solution looking for a problem.'" *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

III. ARGUMENTS IN SUPPORT OF TECH AND TRADE SECRECY

Proponents of technological innovation in criminal justice often point to the many shortcomings of the justice system and emphasize the improvements that technology may be able to bring.[79] Human beings, undoubtedly not "perfect arbiters of truth and reason," are the original source of bias, error in judgement, corruption, and any other number of evils in our undeniably imperfect system of justice.[80] Technology, done right, could be a path to making the criminal justice system more efficient, equitable, and just.[81] After all, if artificial intelligence and algorithms are merely tools—just as surely as they can do harm if imperfectly built or improperly used—they may instead be implemented in ways that could reduce human error or bias, increase access to information, and facilitate better decisions and more just outcomes, which may thereby decrease unnecessary jailing, reduce crime, avoid injustice, and save taxpayer money.[82]

However, even strong proponents of criminal justice technology recognize the dangerous implications for due process and civil rights that such technology may pose. As Arthur Rizer and Caleb Watney put it, "due process is not furthered by blind trust in the results of an algorithm whose assumptions cannot be challenged; there is a critical need for process checks—including transparency and discoverability—when the results of a machine weigh so heavily on guilt and innocence."[83] On the subject of sentencing algorithms, for instance, proponents acknowledge that the key to incorporating fair and accurate systems into the sentencing process is to understand how various inputs may serve as proxies for bias or inequity and to adjust the data sets and operations of the algorithms accordingly.[84] The same experts who describe "algorithmic aversion" as an unfounded bias against the use of artificial intelligence also freely admit that to best implement such technology requires that it

[79] *See, e.g.*, Rizer & Watney, *supra* note 9, *passim*; *see also* Mirko Bagaric et al., *Erasing the Bias Against Using Artificial Intelligence to Predict Future Criminality: Algorithms are Color Blind and Never Tire*, 88 U. CIN. L. REV. 1037 *passim* (2020).

[80] Bagaric et al., *supra* note 79, at 1064–66 (2020); *see also, e.g.*, Ozkan Eren & Naci Mocan, *Emotional Judges and Unlucky Juveniles*, 10 AM. ECON. J.: APPLIED ECON. 171, 187–95 (2018) (asserting findings of a direct correlation between unexpected losses by the LSU Tigers football team and harsher sentences handed down to juvenile defendants by Louisiana judges).

[81] Rizer & Watney, *supra* note 9, at 183.

[82] *Id.* at 194–97.

[83] *Id.* at 198.

[84] Bagaric et al., *supra* note 79, at 1040.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

"must be transparent and publicly available" to "provide the opportunity for ongoing testing, evaluation, refinement, and improvement[.]"[85]

But herein lies the fundamental problem: these systems are not within the public view, nor widely understood, nor freely accessible for independent study and further development. The design and creation of proprietary systems is done behind closed doors by private, for-profit entities, who, under current market realities, have no incentive to make the inner workings of their products available for review or criticism.[86] In fact, the opposite is true; current market incentives would most likely drive a private entity to minimize or dismiss the risk of shortcomings, errors, or inaccuracies in order to avoid liability and continue selling their product to municipal or governmental buyers.[87]

Software developers typically safeguard valuable, intangible property interests in hardware or software through trade secret protection.[88] Since trade secret protection in turn depends on vigorous enforcement and avoidance of any disclosure, efforts toward public accountability, harm prevention, and open and cooperative development and testing will all be severely hampered, if not defeated entirely.[89] Trade secret holders routinely and necessarily "engage in self-help measures to deter

[85] *Id.*

[86] For example, see Ram, *supra* note 6, at 668–70, for discussion of the Stingray, a device used by law enforcement agencies across the country to track and surveille mobile phones. When applying for Federal Communications Commission's ("FCC") approval to expand sales from federal agencies to state and local law enforcement agencies, Harris Corporation, the manufacturer of the Stingray, requested that any information about its devices "be withheld from public disclosure until and unless Harris notifies the Commission that such information may be publicly released." *Id.* Harris justified its request for blanket confidentiality mostly by asserting that disclosure would substantially harm its competitive interests and would divulge trade secrets to its competitors. *Id.* at 669. The FCC granted the confidentiality request and approved the expanded sales. *Id.* Police departments across the country could then acquire Stingrays from Harris, but only after coordinating acquisition through the FBI and entering nondisclosure agreements to bar purchasers from revealing any information about the devices, even to courts or other government entities. *Id.*

[87] *See, e.g.*, *id.* at 673–75 (discussing the Intoxilyzer, a breathalyzer device whose manufacturer "repeatedly refused to disclose the source code for its devices on trade secret grounds"). In the limited number of cases where disclosure did occur, serious flaws in its programming, false positives, and incorrect results were discovered, leading at least two states to abandon use of the devices and several courts to deem its results inadmissible. *Id.*

[88] *See* Kaytal, *supra* note 5, at 1216.

[89] *Id.* at 1215.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

discovery, physically protect the trade secret, and administer a maze of nondisclosure and employee confidentiality agreements."[90]

For information to qualify as an enforceable trade secret, its economic or commercial value must be derived, at least in part, from its undisclosed nature and the secret must be subject to continued efforts to keep it from being disclosed or otherwise becoming known or discovered.[91] In theory, secrecy should not be surrendered if disclosed "under adequate confidentiality safeguards," such as under protective order incident to litigation.[92] Nevertheless, trade secret holders often fight vehemently against any disclosure or discovery of protected information to avoid the risk that the information might be misappropriated, leaked, or would otherwise lose its protected status.[93]

To balance the widely acknowledged need to ensure open and fair proceedings with the upside potential of more perfect justice through technological innovation, a neutral, controlled environment enabling both rigorous third-party review and continuing property protections would be ideal. This would function something like intellectual property escrow, a temporary middle ground between the interests requiring proof that a technology works and those with justifiable concerns about protecting property rights and commercial viability.[94] Just as the Food and Drug Administration keeps a secret formula confidential and exempt from public disclosure while reviewing it for safety and efficacy,[95] a similar process could allow confidential review by experts to make certain that criminal justice tech is verifiably accurate and demonstratively reliable enough to be worth the taxpayer's money and

[90] *Id.*

[91] UNIF. TR. SECRETS ACT § 1(4) (UNIF. L. COMM'N 1985).

[92] 1 ROGER M. MILGRIM & ERIC E. BENSEN, MILGRIM ON TRADE SECRETS § 1.03 (2023), Lexis.

[93] *Id.* § 14.02.01(2).

[94] Albeit for different reasons, software developers, especially those providing enterprise-level, software-as-a-service products, have long used "source code escrow" to alleviate buyers' concerns that a developer might suddenly shutter its business or otherwise abruptly stop supporting mission-critical software products. *See, e.g.*, Jonathan L. Mezrich, *Source Code Escrow: An Exercise in Futility?*, 5 MARQ. INTELL. PROP. L. REV. 117, 119 (2001); Mark Kesslen & Leah Satlin, *Source Code Escrow Agreements Are Reaching For The Cloud*, LAW360 (Feb. 28, 2020), https://www.law360.com/articles/1248285/source-code-escrow-agreements-are-reaching-for-the-cloud. A key difference here, however, is the purpose of the escrow; developers may be far less amenable to surrendering source code for the purpose of pre-sale scrutiny.

[95] 21 C.F.R. § 20.61(d) (2023); 3 MILGRIM & BENSEN, *supra* note 92, § 12.02(1).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

worthy of admission into evidence in a court of law. A regulatory sandbox may be able to achieve this.

IV. THE REGULATORY SANDBOX: A BALANCED SOLUTION

A regulatory sandbox is an administrative construct for the controlled testing of new products or services under the supervision of regulators and in cooperation with the regulated entities themselves.[96] Zacharia Demeola of the Institute for the Advancement of the American Legal System defines a regulatory sandbox as "a limited regulatory space that allows for measured delivery of new models and services under careful oversight, in order to test interest, marketability, and consumer impact, and to inform policy development."[97] More in line with principles-based regulation and other regulatory reform ideas like the broader "new governance" movement,[98] a regulatory sandbox could be a cooperative, adaptive, and less onerous approach to facilitating beneficial economic activity and innovation while minimizing potential harm. Ideally, such a collaborative framework—provided it has sufficient "teeth" to enforce its own rules—might even foster a "private-sector culture of compliance" requiring less aggressive oversight and enforcement.[99]

In comparison, traditional regulatory agency regimes often operate via centralized rulemaking, compliance monitoring and assessment, and coercive, sanction-based enforcement.[100] Administrative agencies have been characterized by some critics as rigid, top-down control structures which issue and enforce a litany of rules, arguably without, or perhaps in spite of, feedback from regulated entities themselves.[101] On the private industry side, it is often said that regulation stifles competition and innovation.[102] Resources which could have been directed to ongoing

[96] Knight & Mitchell, *supra* note 12, at 449.

[97] DeMeola, *supra* note 14.

[98] *See* Allen, *supra* note 11, at 600. Allen describes new governance as "a paradigm that 'views regulation as a reflexive, iterative, and dialogical process and identifies ongoing deliberation as the most legitimate and most effective mechanism for making decisions in complex organizational structures.'" *Id.* (quoting Cristie L. Ford, *New Governance, Compliance, and Principles-Based Securities Regulation*, 45 AM. BUS. L.J. 27–28 (2008)). "Instead of forcing regulated entities to act in the public interest against their will, the new governance paradigm seeks to involve and harness regulated entities in a public-private partnership for a defined public good." *Id.* at 600–01.

[99] *Id.* at 601.

[100] Sharon Yadin, *E-Regulation*, 38 CARDOZO ARTS & ENT. L.J. 101, 124–25 (2020).

[101] *See, e.g.*, Allen, *supra* note 11, at 600.

[102] *Id.* at 591.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

improvement of concept or development of new economic activity go instead toward costs of compliance—and perhaps disproportionately so for smaller firms or startups.[103]

Many of the criticisms lodged against standard regulatory agency models may become especially acute in regard to tech-based industries, given the dynamic and persistent nature of technological change and innovation. Because of this, some scholars have called for "new governance" or novel regulatory approaches "in policy areas 'in which technological and economic change has outstripped the capacities of established market and bureaucratic safeguards to protect key public interests.'"[104] Arguably, that is precisely what is happening in the area of criminal justice technology and precisely why a regulatory sandbox could be a fitting solution.

From the regulated entities' perspective, a major advantage of a sandbox is that it permits a firm to test new offerings with actual consumers while receiving real-time guidance and oversight from regulators and experts.[105] The firm can do this while not yet being subject to the full scope of rules and compliance requirements that would normally apply to industry participants.[106] Additionally, a sandbox could be beneficial for regulated entities because of its increased flexibility, lower compliance costs, and direct lines of communication with regulators.[107] One author on the subject noted that acceptance into a regulatory sandbox program may actually be a selling point for a firm to attract customers or funding, as involvement in such a program could give a firm, especially a startup, increased credibility.[108] For private companies in the criminal justice space, participation in a regulatory sandbox could be seen by observers as showing a good faith belief in the reliability of their product and a willingness to root out and improve on any flaws.

The sandbox approach may especially appeal to tech companies since it might be a familiar concept. In the computer science context, a sandbox can serve as a controlled space to separate and run programs in parallel while preventing errors or

[103] *Id.*

[104] *E.g.*, Christopher G. Bradley, *FinTech's Double Edges*, 93 CHI.-KENT L. REV. 61, 86 (2018) (quoting Charles F. Sabel & William H. Simon, *Minimalism & Experimentalism in the Administrative State*, 100 GEO. L.J. 53, 78–92 (2011)).

[105] Allen, *supra* note 11, at 592.

[106] *Id.*

[107] *Id.* at 601.

[108] *Id.* at 587.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

vulnerabilities from spreading system-wide.[109] Sandboxes may also be used in software development to allow controlled access and implementation while experimenting with new ideas.[110] The overall impact of a new function or a change in source code can be studied and tweaked before either being fully adopted or rejected.[111] Likewise, a sort of scaled, iterative framework for regulation may seem more agreeable to those in the software or tech industries than a traditional, rule-and-sanction-based, command-and-control regulatory framework.

A sandbox program could reap significant benefits for regulators, as well. It can offer regulators insight into cutting-edge innovation and developing technologies, especially ideal "when complex innovations defy regulators' understanding."[112] It is important that emerging technology not overtake the capacity of the regulatory state to safeguard values such as "public safety, universal access, competition, and consumer protection."[113] Better informed regulators may then keep up with or anticipate changes among participants in the regulated markets.[114] The FCC, for instance, used the sandbox approach to study experimental licensing practices as well as processes and policies for updating decades-old telecommunications networks to better suit mobile technology and internet protocols.[115] The regulatory sandbox may then be adapted as needed—for example, issuing looser, principle-based guidance for startup entities or in regard to an emerging technology and then observing and revising guidance over time toward a more definite, rule-based regulatory scheme.[116]

Sandboxes may also be an easier sell politically. Awareness and interest has grown considerably in recent years, and regulatory sandboxes have already been

---

[109] Jiang Jiaying, *Technology-Enabled Co-Regulation for Blockchain Implementation*, 83 U. PITT. L. REV. 829, 858 (2022) (citing Ian Goldberg et al., *A Secure Environment for Untrusted Helper Applications* (Confining the Wily Hacker), *in* SAN JOSE, PROCEEDINGS OF THE SIXTH USENIX UNIX SECURITY SYMPOSIUM 2 (1996)).

[110] Jessica Rosenworcel, *Sandbox Thinking*, DEMOCRACY, Fall 2014, https://democracyjournal.org/magazine/34/sandbox-thinking/. At the time of writing the article, Jessica Rosenworcel was the acting chair of the FCC. She was sworn in as commissioner in 2017.

[111] *Id.*

[112] Allen, *supra* note 11, at 601.

[113] Rosenworcel, *supra* note 110.

[114] *Id.*

[115] *Id.*

[116] Allen, *supra* note 11, at 604.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

implemented in a number of regulated industries around the world and in the United States.[117] Current or former sandbox programs have been initiated at the federal level by agencies like the Consumer Financial Protection Bureau ("CFPB")[118] and the FCC[119] and have been considered, if not implemented, in several states, including Arizona, Utah, California, Washington, Illinois, Florida, and North Carolina.[120] Republican Congressman Patrick McHenry of North Carolina introduced legislation, the Financial Services Innovation Act of 2016, which would have established a framework for regulatory relief in conjunction with a financial services technology ("fintech") sandbox.[121] The bill would have granted broad relief from standard regulatory compliance and enforcement measures for the makers of a fintech product that (A) "would serve the public interest; (B) improves access to financial products or services; and (C) does not present systemic risk to the United States financial system and promotes consumer protection."[122] Unfortunately, the bill appears to have gone nowhere.[123] In the future, however, the balanced, measured approach which sandboxes offer could potentially have a wider appeal than traditional regulation, even to those "in risk-averse Washington."[124]

The regulatory sandbox program implemented in Utah for tech-based legal services[125] is particularly illustrative of how a criminal justice tech sandbox could be formulated. More than two dozen non-traditional legal service providers have been

[117] *See supra* notes 13–14.

[118] *CFPB Issues Policies to Facilitate Compliance and Promote Innovation*, CONSUMER FIN. PROT. BUREAU (Sept. 10, 2019), https://www.consumerfinance.gov/about-us/newsroom/bureau-issues-policies-facilitate-compliance-promote-innovation/.

[119] Rosenworcel, *supra* note 110.

[120] *See* sources cited *supra* note 14 and accompanying text.

[121] H.R. 6118, 114th Cong. (2016).

[122] *Id.* § 6(b)(2).

[123] *Summary: H.R. 6118—114th Congress (2015–2016)*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/6118 (last visited Apr. 19, 2023) ("Latest Action: House—10/19/2016 Referred to the Subcommittee on Commodity Exchanges, Energy, and Credit.").

[124] Rosenworcel, *supra* note 110.

[125] UTAH CODE ANN. §§ 13-55-101–13-55-108 (LEXIS through 2022 Third Special Sess. of the 64th Legis.). Initially approved in August of 2020, Utah's Supreme Court voted unanimously in April of 2021 to extend the original two-year duration of the program to seven years. *Utah Supreme Court to Extend Regulatory Sandbox to Seven Years*, UTAH CTS. RECENT PRESS NOTIFICATIONS (May 3, 2021), https://www.utcourts.gov/utc/news/2021/05/03/utah-supreme-court-to-extend-regulatory-sandbox-to-seven-years.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

approved through the Utah program.[126] Each provider is subject to requirements of regular reporting and submission of operational data, with continued authorization "contingent upon data showing no evidence of significant consumer harm."[127]

Several key features of the Utah program further demonstrate why a similarly structured program might be able to reconcile key interests otherwise at odds regarding criminal justice technology. First, Utah established the Office of Legal Services Innovation, an independent regulator answerable to the Utah Supreme Court that determines whether to admit potential service providers to the sandbox through an application process involving review by legal professionals and experts in "data analysis, business, and sociology."[128] Second, the goal of the Utah program is to enact evidence and risk-based regulation, while seeking to ensure that consumers or others interacting with the regulated entities are not negatively impacted by "achieving an inaccurate or inappropriate legal result, failing to exercise legal rights through ignorance or bad advice, or purchasing an unnecessary or inappropriate legal service."[129] Third, regulated entities must consent to providing data to the regulatory authority as a condition for admittance to the sandbox and access to the legal services market.[130]

A criminal justice technology sandbox could be established in a similar way. Some have already advocated for an independent federal agency to be established with authority to regulate criminal justice technology.[131] Congress or a state legislature could enact enabling legislation to create such an agency while expressly providing that the utilization of one or more regulatory sandboxes is within said agency's fundamental purposes. Going forward, the use of criminal justice tech by any state actor would have to be restricted to those technologies which the agency has evaluated and approved for sale. To minimize disruption to current producers and institutional users of these technologies, a fast-track protocol could be established to quickly—yet rigorously—examine existing technologies and either grant or deny approval, depending on whether they adequately perform their intended functions while meeting all other requisite criteria for access to the criminal

[126] DeMeola, *supra* note 14.

[127] UTAH CTS. RECENT PRESS NOTIFICATIONS, *supra* note 125.

[128] DeMeola, *supra* note 14.

[129] *Id.*

[130] *Id.*

[131] Bunnell, *supra* note 15, at 299–303.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

justice tech market. Over time and as more existing technologies have been screened through the fast-track program, the agency's focus could shift more toward longer-term sandbox programs for new and emerging technologies.

Similar to the Utah program, experts in the relevant fields—here, science, technology, law enforcement, and criminal law—should work directly with the regulated entities to ensure informed, scientifically rigorous, and objective evaluations are completed under conditions which best protect the sensitive and confidential nature of the proprietary technologies involved. Through "evidence- and risk-based regulation,"[132] the agency can ensure that any technologies approved for use in police work or judicial proceedings are scientifically accurate enough that neither individual civil rights nor the public interest are negatively impacted. The entire criminal justice system—and those whose lives and liberty hang in the balance—will benefit greatly from safeguarding against "inaccurate or inappropriate legal result[s]," and society will benefit where its institutions are not wasting public funds on the acquisition of any "unnecessary or inappropriate," privately developed criminal justice tech that does not function, as it should, in the interest of truth and justice.[133]

Although under this framework, participation of the regulated entities would be compelled by prohibition of the sale of any criminal justice tech lacking preapproval, the regulated entities would ultimately benefit in several ways. Like The Financial Services Innovation Act envisioned,[134] broad relief from standard regulatory compliance and enforcement measures could be granted. Participation might also result in a reduction in the amount of legal and compliance costs, including expensive and time-consuming litigation that these companies are engaged in over issues of discoverability and confrontation of evidence. Timely feedback from experts and regulators can help guide companies toward improved products, lower costs of compliance, and better relations with their customers and with the public. And wherever the regulatory screening process might "weed out not only the fraudulent analyst, but the incompetent one as well[,]"[135] those firms offering sound, reliable, accurately performing products would benefit from not having to compete with unscrupulous sellers or inferior products hiding behind trade secrecy or nondisclosure to obscure the flaws or failings of their technology.

---

[132] DeMeola, *supra* note 14.

[133] *Id.*

[134] *See supra* notes 120–22 and accompanying text.

[135] Melendez-Diaz v. Massachusetts, 557 U.S. 305, 327 (2009).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu

CONCLUSION

The criminal justice system has never been perfect. But the lofty ideals of truth and equal justice on which the system is founded are worth striving for. The current lack of regulation to bring coherence and discipline to the use of new technology in law enforcement and criminal proceedings has led to uncertainty, inconsistency, and the danger of manifest injustice within local, state, and federal justice systems. In all likelihood, technological innovation and private enterprise will continue to further implicate itself within the public sector. Given any particular set of circumstances, these private-public partnerships could either bring great benefit or inflict great harm upon society. Because of this duality, proper safeguards and oversight are needed. A thoughtfully designed and properly instituted regulatory sandbox may be the best approach toward balancing the civil rights of defendants and the public interest in open justice and governmental accountability with legitimate economic interests, intellectual property protections, and the need for continuing innovation.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.959
http://lawreview.law.pitt.edu