Fordham Urban Law Journal

Volume 46
Number 2 *Artificial Intelligence and Predictive Algorithms: Why Big Data Can Lead To Big Problems*
Article 4

2019

Impoverished Algorithms: Misguided Governments, Flawed Technologies, and Social Control

Sarah Valentine

IMPOVERISHED ALGORITHMS: MISGUIDED GOVERNMENTS, FLAWED TECHNOLOGIES, AND SOCIAL CONTROL

Sarah Valentine[*]

ABSTRACT

This Article posits that governments deploy algorithms as social control mechanisms to contain and criminalize marginalized populations. Though recognition of the dangers inherent in misuse of big data and predictive analytics is growing, governments and scholars alike have not paid sufficient attention to how these systems inevitably target the poor, the disabled, and communities of color. As the criminal justice and social welfare systems have become fused, big data analytics increases the breadth of government control over those caught within these overlapping systems. Challenging governmental use of algorithms as instruments of social control requires understanding the fallibility of the technology, the historical and political forces driving adoption of the technology, and the strategies that have been most effective in advocating against it. It also requires recognizing that the technological capacity to control and punish includes, but also expands far beyond, uses by law enforcement.

This Article discusses the most problematic aspects of governmental use of big data and artificial intelligence. These include issues of governmental malfeasance, system capacity for masking encoded bias, technological alteration of policy, the ceding of political decisions to private developers, and systemic data error. It then examines the social and political forces driving governmental deployment of data analytics. It concludes by examining litigation,

---

[*] Professor of Law, City University of New York School of Law. The author would like to thank Ruthann Robson for her critique and feedback. Additional thanks to both CUNY School of Law and Stetson University College of Law for their institutional support.

regulatory, and organizing strategies that can be used to challenge governmental employment of algorithmic social control mechanisms.

TABLE OF CONTENTS

INTRODUCTION

Governments at all levels, from the local to the federal, are increasing their reliance on algorithmic decision-making technologies.[1] Helpful as algorithms may be, they inevitably target marginalized populations and exacerbate the social stratification and vast inequality that already exists in our society. Simply put, algorithms are mathematical processes for solving defined problems.[2] Algorithmic decision-making technologies encompass a wide variety

1. Algorithmic decision-making is the use of algorithms to either assist human decision-making or, now more commonly, to make decisions without human intervention. *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1252 (2008).

2. While "algorithm" is a term with a highly technical definition, scholars have generalized the definition as a computational procedure for solving a specifically defined task or problem. *See* Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 640 n.14 (2017) (detailing observations by a host of well-known scholars in the field of technology and the law, including Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, and Harlan Yu).

of big-data analytic systems,[3] including predictive analytics[4] and machine learning.[5] As these technologies grow more and more sophisticated, human decision-making in the areas of criminal justice, public benefits, and child welfare is rapidly being replaced by technologies that few understand and many in positions of power mistakenly believe are infallible.[6] When deployed to control and contain vulnerable populations, these systems dehumanize the people they target and impoverish standards of due process and justice.

Public awareness of the potential dangers that arise from misuse of big data is increasing,[7] and legal academia has begun to grapple with how this technology upends civil rights and privacy.[8] However, current discussions tend to elide how these algorithmic technologies

---

3. Big data analytics is the increased computational analysis possible from the application of advanced algorithms to increasingly large data sets. *See* David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. DAVIS L. REV. 653, 669 (2017).

4. Predictive analytics is the use of complex algorithms to predict future behavior through analyzing large data sets. *See* I. Glenn Cohen & Harry S. Graver, *Cops, Docs, and Code: A Dialogue Between Big Data in Health Care and Predictive Policing*, 51 U.C. DAVIS L. REV. 437, 438 (2017).

5. Machine learning algorithms are not programmed to complete a specifically defined task, but rather to learn to solve more indeterminate problems — to develop additional algorithms without additional programming. *See* Andrew Tutt, *An FDA for Algorithms*, 69 ADMIN. L. REV. 83, 85 (2017); *see also* Robert D. Helfand, *Big Data and Insurance: What Lawyers Need to Know and Understand*, 21 J. INTERNET L. 1, 6 (2017) (explaining that machine learning programs revise their instructions based on correlations that human programmers may not have considered).

6. *See generally* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017) [hereinafter THE RISE OF BIG DATA POLICING] (discussing predictive policing technology in the criminal justice system); VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2017) (detailing technologically enhanced governmental control over the poor in social and family services).

7. *See generally* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION, HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016). Even with increased attention, much of the public remains unaware of the capacity for surveillance and manipulation big data analytics provides. *See* SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 51–54 (2018).

8. *See, e.g.*, Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016) (discussing Title VII's inability to address discrimination arising from employer's data mining enhanced decision making); Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871 (2016) (arguing that machine learning to predict individual criminality may shift reasonable suspicion determinations to predictive algorithms); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93 (2014) (arguing existing privacy protections are inadequate to address big data's harms).

increasingly become tools of social control, used to maintain rigid and historical demarcations of class and race. For example, while police officers have long had the ability to use their own judgment to decide if there is the articulable suspicion necessary to stop and frisk someone,[9] today that articulable suspicion may be guided by an algorithm that neither the police officer nor anyone else in the police department understands or can explain.[10] Similarly, while caseworkers have always had to make decisions about whether or not a family qualifies for public benefits or whether there is sufficient risk of harm to remove a child,[11] now those decisions are guided and sometimes determined by opaque and inexplicable predictive analytics.[12]

Although individual decisions made by police officers or caseworkers can be biased or wrong, those decisions are traceable to an individual actor in particular circumstances. Individual decisions can be disputed in court, with those affected able to challenge the circumstances or evidence the police officer or caseworker relied on. Big data analytics is altering how these kinds of governmental decisions are made and this, in turn, weakens the ability for those harmed to effectively challenge those decisions. Big data systems are often touted as more cost efficient and objective methods of governmental decision-making concerning vulnerable populations.[13] However, this focus on efficiency only glorifies savings over proper services, and the belief that hyper-surveillance and predictive analytics can solve deep issues of bias and discrimination is misguided at best.

We live in a country that consigns a large part of its population to an underclass, a permanently marginalized group contained, controlled, and criminalized purportedly for the protection of everyone else.[14] Over the past several decades, government has

---

9. *See* Terry v. Ohio, 392 U.S. 1, 21 (1968).

10. *See infra* Section I.B.

11. *See, e.g.*, Lauren Huber Martin, Comment, *Caseworker Liability for the Negligent Handling of Child Abuse Reports*, 60 U. CIN. L. REV. 191, 195–96 (1991) (describing typical responsibility of child protection case worker investigating an allegation of neglect or abuse).

12. *See infra* Section I.B.

13. Citron, *supra* note 1, at 1252–53 (discussing how the automation of benefits decision-making systems are seen as more efficient and consistent); EUBANKS, *supra* note 6, at 33 (discussing how the computerization of benefits systems as neutral tools can reduce public spending).

14. *See* Malcolm M. Feeley & Jonathan Simon, *The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications*, 30 CRIMINOLOGY 449, 467–68 (1992).

coercively leveraged the welfare, foster care, prison, and deportation systems to control residents of neighborhoods devastated by the systemic withdrawal of public resources.[15] When these vulnerable populations seek assistance, the state they encounter not only often fails to support them, but it also actively targets them with punitive social control mechanisms.[16] The criminal justice and social welfare systems are now fused to better control and contain marginalized populations such as the poor, the disabled, and communities of color.[17]

What happens when government introduces algorithmic decision-making systems into an already repressive environment? It increases its capacity to dominate vulnerable communities by making it almost impossible to challenge system errors.[18] It reinforces historical discrimination by relying on inaccurate and biased data.[19] It further destroys our country's already meager social safety net by ceding more regulatory power to private companies whose focus is profit.[20] Most dangerously, it allows governments to hide these negative effects behind the veneer of technological infallibility.

Technology is not neutral, and governmental reliance on big data analytics has the capacity to further erode fundamental relationships between the governing and the governed.[21] Unchecked governmental use of algorithms as social control mechanisms[22] is

---

15. Dorothy Roberts, *Prison, Foster Care, and the Systemic Punishment of Black Mothers*, 59 UCLA L. REV. 1474, 1477–78 (2012). The criminalization of poverty extends further into communities as the collateral consequences of mass incarceration effect entire neighborhoods. *See* Ann Cammett, *Shadow Citizens: Felony Disenfranchisement and the Criminalization of Debt*, 117 PENN ST. L. REV. 349, 366 (2012) (noting that disenfranchisement affects communities through vote dilution and economic displacement from the redistribution of federal resources).

16. Wendy A. Bach, *The Hyperregulatory State: Women, Race, Poverty, and Support*, 25 YALE J.L. & FEMINISM 317, 318–19 (2014).

17. *Id.* at 334–36 (describing the state's targeting of poor, urban, communities of color as intentional).

18. *See infra* Sections I.B. and II.A.

19. *See infra* Section I.C.

20. *See infra* Section II.C.

21. Torin Monahan, *Questioning Surveillance and Security*, *in* SURVEILLANCE AND SECURITY: TECHNOLOGICAL POLITICS AND POWER IN EVERYDAY LIFE 10 (2006) ("Technologies are neither separate from society nor are they neutral tools . . . [i]nstead [they] are part of the social problems they are intended to correct."); *see also* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1953–54 (2013) (discussing how state surveillance affects the power dynamic between "the watcher and the watched").

22. Advanced algorithms and AI systems can, of course, be greatly beneficial. It is governmental deployment of these technologies as social control mechanisms this Article critiques. Technologically similar systems can be used for vastly different

dangerous to many of our core democratic beliefs about due process and equality, especially when the technology is used to target already marginalized populations. Governmental adoption of these technologies is inherently political, not only because it impacts the use of governmental resources, but also because it reinforces some of the worst aspects of our current justice system. Big data analytics provides the state a degree of control over marginalized populations that is unrivaled in American history.[23] To confront the increasingly authoritarian application of big data analytics, progressive lawyers, policymakers, and advocates must not only understand the technology and how it reinforces oppression, but also must engage with the socioeconomic forces that drive governments to adopt technological systems of social control.

The layering of algorithms on top of the already complex social structures underpinning our problematic justice system may seem like a significant shift in practice to those of us not steeped in technology. However, no matter how complex the mathematics, these systems are less revolutionary than they are the logical evolution of past strategies that governments have used to control marginalized people.[24] Thus, many of the tools used to challenge governmental overreach in the past provide the foundations with which to oppose big data analytics — algorithms of social control themselves, both impoverished and impoverishing.

This Article discusses various aspects of how and why governments use algorithmic decision-making systems as a mechanism of social control. It also explores potential avenues of resistance before government reliance on these systems becomes unassailable. Part I addresses issues of governmental malfeasance in implementing big data technologies and discusses how the systemic flaws in the deployment of seemingly "objective" tools can do harm to vulnerable populations. Part II discusses some of the prominent sociopolitical factors driving governmental adoption of big data technologies.

---

purposes. *See, e.g.*, Allison J. Pugh, *Automated Health Care Offers Freedom from Shame, but Is It What Patients Need?*, NEW YORKER (May 22, 2018), https://www.newyorker.com/tech/elements/automated-health-care-offers-freedom-from-shame-but-is-it-what-patients-need/amp [https://perma.cc/RM6A-PW7K] (describing similar systems where individuals interact with artificial intelligence, one developed to provide low income patients assistance returning home from the hospital and another developed to assist Homeland Security in interrogations).

23. EUBANKS, *supra* note 6, at 200.

24. *Id.* at 37 (describing data analytics targeting the poor and working class as an "expansion and continuation of moralistic and punitive poverty management strategies existing since the 1820's").

Finally, Part III considers how litigation, regulation, and political activism can be combined to address the harms caused by governmental deployment of these systems.

I. NEW TOOLS BUILT ON PAST PREJUDICE

Governments have always relied on the surveillance technology of the day.[25] Historically, the burdens of surveillance have fallen hardest on poor and marginalized populations.[26] Still, the wholesale adoption of big data analytics is unique,[27] even as it shares troubling historical roots with government use of other technologies. Unprecedented levels of public and private surveillance[28] have created what is commonly called "big data,"[29] an almost unfathomable amount of searchable and sharable data on every individual and community in the country.

The sheer amount of collected data from hyper-surveillance is stunning, but it is the analytics that weaponizes this information, allowing governments to "profile, police, and punish the poor."[30]

---

25. *See generally* JEREMY BLACK, THE POWER OF KNOWLEDGE: HOW INFORMATION AND TECHNOLOGY MADE THE MODERN WORLD (2014) (reviewing historical governmental use of information and technology from the fall of the Mongolian empire through the rise of big data).

26. Kimani Paul-Emile, *Blackness as Disability?*, 106 GEO. L.J. 293, 340–42 (2018) (describing police profiling and systematic surveillance as social control mechanisms that disproportionately target black populations); *see also* Nathalie Maréchal, *First They Came for the Poor: Surveillance of Welfare Recipients as an Uncontested Practice*, 33 MEDIA & COMM. 56 (2015) (describing persistent governmental surveillance of poor and low-income Americans).

27. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (describing the amount of searchable data available to law enforcement, in this case cell-site records, as caused by "seismic shifts in digital technology").

28. Data collection is a form of surveillance, and the current scope of this surveillance is unprecedented. *See* Richards, *supra* note 21, at 1936. The level of surveillance today is so immense that it necessitates a parsing of the concept. *See* Andrew Guthrie Ferguson, *The Smart Fourth Amendment*, 102 CORNELL L. REV. 547, 551, 551 n.15 (2017) (describing "sensorveillance" as the "ever increasing ability for surveillance technologies to track individuals through the data trails they leave behind," and indicating the term was inspired by the concept of "dataveillance" used to "describe the systematic observation, collation, and dissemination that modern computing make possible").

29. There is no uniform definition of "big data," though in general it is recognized as the aggregation of massive amounts of information in digital format to increase analytic capacity to search and sort. *See, e.g.*, Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U. L. REV. 53, 64 (2017) (describing big data as "the collection, aggregation, analysis, and use of mass amounts of digital information gathered and shared about individuals").

30. EUBANKS, *supra* note 6, at 38. "Policing" is used to capture all the ways the government forcefully attempts to regulate and manage the poor, regardless of

Advances in computational science have created the ability to capture, collect, and combine everyone's digital trails and analyze them in ever-finer detail.[31] It is this merging of big data with advanced analytics that facilitates social control through algorithmic decision-making systems. As political scientist, data scholar, and activist Virginia Eubanks explains:

> Forty years ago, nearly all of the major decisions that shape our lives — whether or not we are offered employment, a mortgage, insurance, credit, or a government service — were made by human beings. They often used an actuarial process that made them think more like computers than people, but human discretion still ruled the day. Today, we have ceded much of that decision-making power to sophisticated machines. Automated eligibility systems, ranking algorithms, and predictive risk models control which neighborhoods get policed, which families attain needed resources, who is short-listed for employment, and who is investigated for fraud.[32]

But algorithmic decision-making, built on imperfect science and implemented using terribly flawed data sets, is generally hidden, opaque, and unknowable — thus often unchallengeable, making it a stealth weapon of social control governments find hard to resist.[33] Limiting the harmful effects of big data analytics requires advocates to recognize the political implications of these systems. It also requires an understanding of just how much can, and does, go wrong with algorithmic decision-making technology. From government malfeasance in adopting and implementing the technology, to the problematic analytics and inaccurate data inherent in their design, the flaws are serious, systemic, and most often ignored.

A. Government Malfeasance

This section explores the ways in which government administrators purchase and implement big data systems — often without understanding how the technology impacts policy, without providing regulatory oversight, and without accurately informing the public about whether or how the systems are functioning. Problems arise from the fact that merely implementing algorithmic decision-making is dangerous, regardless of the technology used. Translating complex

---

whether it is done explicitly by law enforcement or through threats to remove access to food, shelter, or one's children. *See id.* at 215.

31. *See* THE RISE OF BIG DATA POLICING, *supra* note 6, at 109–12 (describing data collection and data mining techniques).

32. EUBANKS, *supra* note 6, at 3.

33. *See infra* notes 62–70 and accompanying text.

policy into computer code alters the policy itself,[34] often harming the communities governed by the policy or regulations.[35] Additionally, automating complex regulatory systems by operation delegates legislative power to that system and its programmers.[36] As one commentator explained, "[t]ranslating powerful, complex ideas into the language of algorithms and machine learning protocols is the mother of all statutory drafting and interpretation problems."[37]

Even in fairly simple systems, coding errors can have disastrous effects. For example, New York City's automated benefits system was developed to guide caseworkers in determining eligibility for various benefits.[38] The system failed to list an option for the immigration status for "battered qualified alien," thereby denying benefits to an entire class of immigrant women fleeing domestic violence.[39] The errors embedded in the New York City system are not unusual, and similarly harmful errors continue to surface across the country as more states adopt algorithmic decision-making technologies.[40]

Most government administrators implementing big data systems do not have the capacity to understand them and cannot explain them. The systems remain opaque, a "mysterious 'black box' impervious to

---

34. Citron, *supra* note 1, at 1261.

35. *Id.* at 1268–71 (describing how coding failures altered regulations in the Colorado, California, and Texas public benefits systems, negatively affecting thousands of recipients).

36. *Id.* at 1295 (noting that because the defects that occur during coding of policy or rules are hidden, agencies fail to provide procedural safeguards typically applied in rulemaking).

37. Mariano-Florentino Cuéllar, *A Simpler World? On Pruning Risks and Harvesting Fruits in an Orchard of Whispering Algorithms*, 51 U.C. DAVIS L. REV. 27, 36 (2017).

38. M.K.B. v. Eggleston, 445 F. Supp. 2d 400, 412 (S.D.N.Y. 2006).

39. *Id.* at 413. New York's automated benefits system also failed to include a complete listing of the documents that could support an applicant's eligibility, and demanded documentation that was not required by law. *Id.*

40. *See, e.g.*, Citron, *supra* note 1, at 1268 ("[F]rom September 2004 to April 2007, code writers embedded over nine hundred incorrect rules into Colorado's public benefits system. With one such incorrect rule, CBMS [Colorado Benefits Management System] denied Medicaid to patients with breast and cervical cancer based on income and asset limits that were not authorized by federal or state law."). In 2016, Arkansas implemented an algorithmic assessment program for disabled Medicaid patients that included coding errors, mistakenly reducing benefits for recipients with diabetes and cerebral palsy. *See* Colin Lecher, *What Happens When An Algorithm Cuts Your Health Care*, VERGE (Mar. 21, 2018, 9:00 AM), https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy [https://perma.cc/55ZZ-RWFP].

challenge."[41] In 2011, the Houston Independent School System began using a privately developed algorithmic decision-making system to terminate teachers.[42] During litigation, the school district could not explain the algorithm's outputs and refused to provide information about the algorithm itself, arguing that it did not have "custody, control or possession" of the technology.[43] The school district also admitted that it ceded all teacher evaluations to the algorithm's developer and did not verify or audit the scores the algorithm provided.[44]

This ceding of authority to the developers is common,[45] and the results are often spectacularly awful for those governed by the system. For example, the Michigan Unemployment Insurance Agency used outside contractors to develop the Michigan Integrated Data Automated System (MiDAS).[46] A completely automated system, MiDAS made determinations of unemployment fraud algorithmically, with absolutely no human review.[47] It also had a ninety-three percent error rate.[48] MiDAS was so problematic that a federal trial court granted a non-profit legal service provider standing

---

41. Hous. Fed'n of Teachers, Local 2415 v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1179 (S.D. Tex. 2017).

42. *Id.* at 1171.

43. *Id.* at 1177 n.28.

44. *Id.* at 1177.

45. *Id.*; *see also* M.K.B. v. Eggleston, 445 F. Supp. 2d 400, 412 (S.D.N.Y. 2006) (discussing how an inaccurate code denied benefits to immigrants seeking assistance in domestic violence cases); Citron, *supra* note 1, at 1309 (describing coding errors that denied benefits to cancer patients); *infra* note 152 and accompanying text (describing a code that automatically terminated benefits for failure to provide certain documentation, regardless of fault).

46. Ryan Felton, *Criminalizing the Unemployed*, DETROIT METRO TIMES (July 1, 2015), https://www.metrotimes.com/detroit/criminalizing-the-unemployed/Content?oid=2353533 [https://perma.cc/E6YH-8Q44].

47. Robert M. Charette, *Michigan's MiDAS Unemployment System: Algorithm Alchemy Created Lead, Not Gold*, IEEE SPECTRUM (Jan. 24, 2018, 5:00 PM), https://spectrum.ieee.org/riskfactor/computing/software/michigans-midas-unemployment-system-algorithm-alchemy-that-created-lead-not-gold [https://perma.cc/9VX7-TLW9]; *see also* Zynda v. Arwood, 2016 WL 4593828, at *1–2 (E.D. Mich. Sept. 2, 2016) (denying Michigan's Motion to Dismiss, which argued that the case should be thrown out on the grounds that it implemented human review and ceased use of the MiDAS system). Training materials provided by Michigan reportedly stated: "Regardless of the manner in which the information is gathered, maintained, or processed, all UI functions are ultimately performed by MiDAS." Ted Roleofs, *Broken: The Human Toll of Michigan's Unemployment Fraud Saga*, BRIDGE (Feb. 7, 2017), https://www.bridgemi.com/public-sector/broken-human-toll-michigans-unemployment-fraud-saga [https://perma.cc/69JW-KAHE].

48. Roleofs, *supra* note 47.

to challenge the State's deployment of the algorithmic tool.[49] The court found that MiDAS's error rate was so high that it forced the law office to divert significant resources to handling the claims, which amounted to injury sufficient to grant standing.[50]

Shifting the power to determine policy to computer programmers is inherently problematic from the perspective of democratic governance. But it is also important to recognize to whom this power is shifted. Tech fields have historically excluded women, black, and Latinx individuals.[51] This exclusion practically insures that the developers building the algorithms governments will use to control marginalized communities will not include individuals from those communities.[52] In other words, the people making programming choices that alter government policy work from a perspective that lacks the cultural awareness of those the technology most directly affects. Beyond this collective problem of nonrepresentation, it is also unfortunately likely that individual programmers will eschew any responsibility for how the technology is ultimately used.[53]

Governments also fail to test the systems they purchase prior to implementation.[54] This lack of due diligence is especially troublesome as more information about system bias and fallibility

---

49. Zynda v. Arwood, 175 F. Supp. 3d 791, 804 (E.D. Mich. 2016).

50. *Id.* at 805–06 (grant of standing to nonprofit law firm because number and opaqueness of the fraud claims generated by MiDAS system).

51. NOBLE, *supra* note 7, at 64–65.

52. *Id.*

53. AARON RIEKE ET AL., UPTURN, OPEN SOC'Y FOUND., DATA BROKERS IN AN OPEN SOCIETY 43 (2016), https://www.opensocietyfoundations.org/sites/default/files/data-brokers-in-an-open-society-20161121.pdf [https://perma.cc/JAU4-56UR] ("An occupational hazard of becoming a technology expert is that one risks losing touch with the animating concerns of social justice."). This is not an overblown concern, as illustrated by this particular incident: a programmer working on technology to retroactively determine whether someone was a gang member was asked about the potential for someone being mistakenly identified as a gang member because of biased training data. *See* Matthew Hutson, *Artificial Intelligence Could Identify Gang Crimes — and Ignite an Ethical Firestorm*, SCI. MAG. (Feb. 28, 2018, 8:00 AM), http://www.sciencemag.org/news/2018/02/artificial-intelligence-could-identify-gang-crimes-and-ignite-ethical-firestorm [https://perma.cc/7YTZ-DQP6]. The programmer denied any responsibility, claiming he could not be sure how the system would be used and that he was "just an engineer." *Id.* In another instance, a developer of the algorithm used in Arkansas to assign Medicaid benefits argued that the lack of transparency in the system was not problematic, because "at some point, you're going to have to trust me that a bunch of smart people determined this is the smart way to do it." Lecher, *supra* note 40.

54. Citron, *supra* note 1, at 1272.

becomes available.[55] To make matters worse, government agencies often refuse to concede when predictive technologies are failing,[56] sometimes going so far as to threaten government employees who raise concerns about the technology.[57] In addition to these technology-specific issues, there are the more mundane ethical lapses common to public-private contracting. Predictive algorithms are expensive and the stakes for individual companies are high.[58] This leads to public procurement with little or no competitive bidding,[59] and unsavory, if not illegal, relationships between government officials and the companies from who they purchase.[60]

---

55. *See infra* Sections II.B. and II.C. Not only is there more information about issues with the technology, there are also suggested solutions that states seem determined to overlook. *See, e.g.*, Danielle Ensign et al., *Runaway Feedback Loops in Predictive Policing*, 81 PROC. MACHINE LEARNING RES. 1, 10 (2018), https://arxiv.org/pdf/1706.09847.pdf [https://perma.cc/NQD8-JWQF] (showing ease of modifying PredPol predictive policing system to minimize its asymmetrical feedback loop that continues to send police into areas based on the technology, not the actual crime rate); Elaine Angelino et al., *Learning Certifiable Optimal Rule Lists for Categorical Data*, 19 J. MACHINE LEARNING RES. 1, https://arxiv.org/pdf/1704.01701.pdf [https://perma.cc/8F5P-X88J] (developing a transparent algorithmic decision-making system for recidivism prediction that work as well as the COMPAS non-transparent and proprietary system).

56. *See* M.K.B. v. Eggleston, 445 F. Supp. 2d 400, 421 (S.D.N.Y. 2006) (noting that despite high-level awareness of the problems with the system "no meaningful corrective action was taken"); *see also* Citron, *supra* note 1, at 1269 n.133 (discussing how despite knowledge of system errors that incorrectly applied income limits to women with breast or cervical cancer, administrators delayed fixing the system "for years").

57. Paul Eagon, *Judges Feel Pressured After Blasting Michigan Jobless Agency*, DETROIT FREE PRESS (July 2, 2017, 7:14 PM), https://www.freep.com/story/news/local/michigan/2017/07/02/judges-michigan-jobless-agency/423502001/ [https://perma.cc/7ERT-GUXH] (reporting pressure placed on administrative law judges who were critical of the MiDAS system).

58. *See* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. 101, 114–16 (2017) (describing Taser's attempt to monopolize the police body camera market).

59. *See, e.g.*, David Gelles, *Taser International Dominates the Police Body Camera Market*, N.Y. TIMES (July 12, 2016), https://www.nytimes.com/2016/07/13/business/taser-international-dominates-the-police-body-camera-market.html [https://perma.cc/CDR5-PQSJ] (describing investigations into cities entering into no bid contracts with Taser).

60. *Id.* (noting the pattern of police chiefs being hired by Taser as consultants). The Director of the Illinois Department of Children and Family Services resigned amid ethical concerns which included no bid contract for a company selling a predictive analytics system. *See* Nancy Smith, *Illinois Dumps George Sheldon's 'Failed' Predictive Analytics Program*, SUNSHINE STATE NEWS (Dec. 7, 2017, 6:00 AM), http://sunshinestatenews.com/story/illinois-dumps-george-sheldons-eckerd-kids-failed-predictive-analytics-program [https://perma.cc/5XPD-RV3W].

Governments could address at least some of the concerns described above by increasing transparency and providing ample opportunities for public input prior to purchasing big data systems.[61] Unfortunately, most governments are less than forthcoming about adopting these technologies. Some jurisdictions go as far as deploying predictive algorithms in secret, especially in the policing arena. In Baltimore, the police department used data from a program that provided aerial surveillance footage for months, without ever reporting it to the mayor, the city council, prosecutors, or defense attorneys — all because the program was privately funded.[62] Keeping the program secret, especially from defense attorneys, is particularly problematic because the Baltimore police used this aerial surveillance information in criminal investigations.[63]

Government reliance on funding loopholes to evade oversight is not uncommon. In New Orleans, predictive policing technology was kept secret because the company provided it for free.[64] In Seattle, police used alternative funding to install surveillance cameras after the city council refused to provide funding.[65] Similarly, police in Bellingham, Washington, purchased a predictive policing system in the face of community and city council opposition, and while the

---

61. *See infra* note 317 and accompanying text (discussing use of procurement ordinances as a method to increase government transparency with regards to the purchase of surveillance technology).

62. Kevin Rector & Luke Broadwater, *Report of Secret Aerial Surveillance by Baltimore Police Prompts Questions, Outrage*, BALT. SUN (Aug. 24, 2016, 10:22 PM), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-secret-surveillance-20160824-story.html [https://perma.cc/9KKF-VHHY] (describing how the program was kept secret); Kevin Rector, *Aerial Surveillance by Baltimore Police Has Promise, Should Be Studied More, Report Concludes*, BALT. SUN (Feb. 10, 2017, 10:11 PM), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-surveillance-report-20170210-story.html [https://perma.cc/L8TM-NMMZ] (listing officials who did not know about the system).

63. *See* Rector, *Aerial Surveillance by Baltimore Police Has Promise*, *supra* note 62.

64. Matt Sledge & Ramon Antonio Vargas, *Controversial Policing Software Draws Criticism in New Orleans*, GOV'T TECH. (Mar. 2, 2018), http://www.govtech.com/public-safety/Controversial-Policing-Software-Draws-Criticism-in-New-Orleans.html [https://perma.cc/52UG-Z7RW]. The policing program, which would have generally needed city council approval, was listed in the budget as a "philanthropic venture" allowing it to "[fly] under the radar" for years. Nicole Lindsey, *Predictive Policing Raises Important Privacy and Human Rights Concerns*, CPO MAG. (Mar. 16, 2018), https://www.cpomagazine.com/2018/03/16/predictive-policing-raises-important-privacy-and-human-rights-concerns/ [https://perma.cc/BJ9Q-9UZT].

65. Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595, 1606 (2016).

public was notified, the hearing where public comment was solicited was held after the decision to purchase the system was already finalized.[66]

Police and prosecutors have also actively misled courts and defense counsel through "parallel construction" tactics to obscure the actual data relied on in their investigations.[67] Authorities routinely cite contractual nondisclosure agreements (NDAs)[68] and developer claims of trade secrets to avoid releasing all relevant information about predictive policing systems.[69] All of these tactics threaten constitutional freedoms and increase state capacity to successfully target and control populations. This is doubly problematic

---

66. DAVID ROBINSON & LOGAN KOEPKE, STUCK IN A PATTERN: EARLY EVIDENCE ON "PREDICTIVE POLICING" AND CIVIL RIGHTS 10 (2016), https://www.teamupturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf [https://perma.cc/9VQU-42DR].

67. *See* Claire Powers, *Surveillance Remedies: Stingrays and the Exclusionary Rule*, 96 OR. L. REV. 337, 351–55 (2017) (discussing use of parallel construction, nondisclosure agreements, euphemisms and other techniques to hide technologies such as cell site simulators); Elizabeth N. Jones, *Possible Problems at the San Clemente Checkpoint*, 6 VA. J. CRIM. L. 43, 83–86 (2018) (detailing investigations into parallel construction in drug enforcement cases, including reports suggesting that government officials are encouraged and trained to mislead courts and defense counsel); *see also* United States v. Patrick, 842 F.3d 540, 546 (7th Cir. 2016) (Woods, J., dissenting) (finding the government purposefully concealed the Stingray's use from a magistrate, the district court, defense counsel, and the Court of Appeals for the Seventh Circuit). Prosecutors have also dismissed charges against defendants rather than disclose particular surveillance technologies. *See* Alexandra Burlacu, *FBI Drops Child Pornography Case to Avoid Disclosing Tor Vulnerability*, TECH TIMES (Mar. 7, 2017, 10:42 AM), http://www.techtimes.com/articles/200592/20170307/fbi-drops-child-pornography-case-to-avoid-disclosing-tor-vulnerability.htm [https://perma.cc/NS4M-MLY8].

68. At least one court has held that police reliance on nondisclosure agreements to intentionally withhold information from a court when seeking a warrant "obstructs a court's ability to make the necessary constitutional appraisal." State v. Andrews, 134 A.3d 324, 338–39 (Md. Ct. Spec. App. 2016). In 2017, a New York trial court held that nondisclosure agreements, without more, could not insulate the New York City Police Department from a Freedom of Information Law (FOIL) request concerning information about predictive policing technologies. *See* Brennan Center for Justice v. N.Y.C. Police Dep't, 2017 WL 6610414, at *10–12 (N.Y. Sup. Ct. Dec. 27, 2017).

69. *See* Joh, *supra* note 58, at 119. Some states are attempting to increase transparency in algorithmic risk modeling systems. The Pennsylvania Sentencing Commission sought public input and then rejected commercial products that refused to allow defendants to review the algorithm. Joshua Brustein, *This Guy Trains Computers to Find Future Criminals*, BLOOMBERG MEDIA (July 18, 2016), https://www.bloomberg.com/features/2016-richard-berk-future-crime/ [https://perma.cc/K5F9-WJ2X].

considering that algorithmic tools target the populations least able to challenge them.[70]

Even in circumstances where government officials act with integrity and are transparent about their intentions to deploy predictive technology, significant issues remain. The analytics used are flawed and the databases the algorithms run on are riddled with errors.[71] This is a devastating combination, which creates algorithmic decision-making systems that reinforce historical patterns of discrimination and bias.

B. Problematic Analytics

The predictive algorithm systems that governments rely on do not work as advertised and are far from infallible. In addition, the systems conceal the political choices used to program the algorithms, and the opaque nature of the code obfuscates the feedback loops that reinforce their discriminatory application. Much of the harm caused by big data analytics could be minimized if the agencies adopting them did minimal due diligence prior to purchase. Given the over-zealous marketing of big data analytics as a panacea to much of society's ills, it is important to pause and consider just how fallible and dangerous these systems can be.[72]

There is little research on whether predictive policing systems actually work. Most of the studies on these systems are either authored or paid for by the very companies developing them,[73]

---

70. *See, e.g.*, Alvaro M. Bedoya, *The Color of Surveillance: What an Infamous Abuse of Power Teaches Us About the Modern Spy Era*, SLATE (Jan. 18, 2016, 5:55 AM), http://www.slate.com/articles/technology/future_tense/2016/01/what_the_fbi_s_surveillance_of_martin_luther_king_says_about_modern_spying.html [https://perma.cc/2HXN-MELD] (noting that targets of state surveillance are historically people of color and immigrants).

71. *See infra* Sections I.B. and I.C.

72. This Article addresses how various states within the United States utilize algorithmic social control mechanisms. However, other countries have implemented such technologies with similarly horrendous outcomes. One glaring example is the Australian Centrelink debacle, which falsely accused thousands of defrauding the government. *See* Justin Warren, *Australian Government Fails at IT Again*, FORBES (Jan. 1, 2017, 10:05 PM), https://www.forbes.com/sites/justinwarren/2017/01/17/australian-government-fails-at-it-again/#6e3e211f60d5 [https://perma.cc/5XQD-5VBZ].

73. ROBINSON & KOEPKE, *supra* note 66, at 7–8 (2016) ("We are currently aware of two rigorous, scholarly studies of predictive policing in the United States whose authors have no interest in the success of the method being evaluated. Both of these were conducted by the RAND Corporation. Neither analysis found any safety benefit in the predictive policing tools studied.").

leaving police departments with little reliable information to use when deciding whether to procure predictive algorithms.[74] Early successes in crime control have not always been sustained, and while new jurisdictions continue to purchase predictive policing systems, others have discontinued or cancelled contracts.[75]

Similarly, independent research on one of the common algorithms used to assess a defendant's likelihood of reoffending found that the algorithm correctly predicted violent recidivism only twenty percent of the time.[76] When all crimes, including misdemeanors, were taken into account, the algorithm was only "somewhat more accurate than a coin flip."[77] But the errors of this algorithm are far worse than being merely incorrect — the mistakes it made were racially biased. The algorithm wrongly labeled black defendants as future re-offenders at almost twice the rate as white defendants, and white defendants were mislabeled as low risk more often than black defendants.[78]

Criminal justice algorithms are not the only error ridden ones. Michigan's implementation of its MiDAS unemployment algorithmic decision-making system[79] was particularly destructive. Designed as a fraud detection system, MiDAS reviewed not only current unemployment applications but also any benefits received within the past six years.[80] The ninety-two percent error rate of the "robo-adjudicated" reviews upended countless lives, flooded the state administrative appeals system with cases,[81] and ultimately cost the

74. Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109, 1159 (2017).

75. THE RISE OF BIG DATA POLICING, *supra* note 6, at 70 (noting that data on effectiveness of predictive policing remains inconclusive).

76. 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/Z4N2-JB23].

77. *Id.* ("Of those deemed likely to re-offend, 61 percent were arrested for any subsequent crimes within two years.").

78. *Id.*

79. *See supra* note 46 and accompanying text.

80. *See* Plaintiff's First Amended Class Action Complaint and Jury Demand at ¶¶4-5, Cahoo et al. v. SAS Inst., No. 17-10657, 2017 WL 3405195 (E.D. Mich. July 7, 2017).

81. Ryan Felton, *Inside Michigan's Faulty Unemployment System that Hit Thousands with Fraud*, GUARDIAN (Feb. 12, 2016), https://www.theguardian.com/us-news/2016/feb/12/michigan-unemployment-insurance-benefit-automated-system-fraud-penalties [https://perma.cc/5QD4-LCEW] (reporting that the system created a backlog of 23,000 unemployment appeals cases).

State of Michigan tens of millions of dollars in addition to the $47 million dollars it has already paid to create the system.[82]

There are similar concerns with the predictive analytics used in child welfare. One of the developers who designed a child maltreatment risk assessment tool for Allegheny County, Pennsylvania, designed a similar system to be used in New Zealand.[83] The risk assessment system was implemented in Allegheny County,[84] but implementation in New Zealand was halted in part because subsequent research showed it had a nearly seventy percent error rate when identifying children at highest risk.[85] The Los Angeles County Office of Child Protection halted the adoption of another child welfare algorithm when auditing indicated a ninety-five percent false-positive rate.[86] Illinois recently terminated its contract with a company providing a child abuse prediction system because, in the words of the director, "it didn't seem to be predicting much."[87]

Lack of governmental understanding of the algorithmic tools they purchase involves issues beyond purchasing error-prone systems. The development of decision-making algorithms, from inception through complex and layered computer coding, is a multistep affair requiring

---

82. *See* Paul Egan, *Michigan Agency Review Finds 70% Error Rate in Jobless Fraud Findings*, DETROIT FREE PRESS (Aug. 11, 2017, 8:39 PM), https://www.freep.com/story/news/local/michigan/2017/08/11/michigan-agency-review-finds-70-error-rate-fraud-findings/559880001/ [https://perma.cc/AP4B-LZG5] (discussing how the agency gives various error rates depending on whether the review was completely automated (robo-adjudication) or included human review of the files flagged by the algorithm).

83. EUBANKS, *supra* note 6, at 136–38.

84. *Id.* at 137.

85. *Id.* at 138.

86. *See* JUDGE MICHAEL NASH, EXAMINATION OF USING STRUCTURED DECISION MAKING® AND PREDICTIVE ANALYTICS IN ASSESSING SAFETY AND RISK IN CHILD WELFARE (May 4, 2017), http://file.lacounty.gov/SDSInter/bos/bc/1023048_05.04.17OCPReportonRiskAssessmentTools_SDMandPredictiveAnalytics_.pdf [https://perma.cc/BL3K-7U7V]. The Director of the Los Angeles County Office of Child Protection indicated that the system had a 95.6% false-positive rate. Daniel Heimpel, *Uncharted Waters: Data Analytics and Child Protection in Los Angeles*, CHRON. SOC. CHANGE (July 20, 2015), https://chronicleofsocialchange.org/featured/uncharted-waters-data-analytics-and-child-protection-in-los-angeles/10867 [https://perma.cc/YL3K-YS2L].

87. David Jackson & Gary Marx, *Data Mining Program Designed to Predict Child Abuse Proves Unreliable, DCFS Says*, CHI. TRIB. (Dec. 6, 2017), http://www.chicagotribune.com/news/watchdog/ct-dcfs-eckerd-met-20171206-story.html [https://perma.cc/RZ59-SNN6] (quoting Illinois Department of Children and Family Services Director Beverly "B.J." Walker). Even with these predictive failures, at least seven other states continue to use similar systems from this vendor. *Id.*

choices that create many opportunities for human error and bias.[88] For example, when building an algorithmic system, a choice has to be made as to how different errors, false positives and false negatives, are weighed. This means that in developing a predictive policing system, a decision will have to be made as to which is worse: to have an innocent person treated as a potential criminal (a false positive) or to have the algorithm overlook potential criminal activity (a false negative).[89]

False positives upend people's lives in a manner that cannot be disregarded or minimized. For those involved with the child welfare system, for instance, false positives are not mere inconveniences. A child welfare investigation can have profound and long-lasting consequences on children and families,[90] including increased risk of juvenile delinquency,[91] parental loss of employment,[92] and deportation.[93] Simultaneously, a false negative means that potential

---

88. *See* Lehr & Ohm, *supra* note 3, at 665–66 (describing the multiple steps in algorithmic development and potential challenges); *see also* Rich, *supra* note 8, at 885–86 (describing points of human decision making in development of algorithms that can cause inaccuracies and errors). It is likely that systems developed by humans are inherently biased. *See* NOBLE, *supra* note 7, at 2 (suggesting that the racist and sexist attitudes of those developing search algorithms undermine the idea that they are capable of developing neutral or objective decision-making tools).

89. Rich, *supra* note 8, at 885.

90. *See* Paul Chill, *Burden of Proof Begone: The Pernicious Effect of Emergency Removal in Child Protective Proceedings*, 41 FAM. CT. REV. 457, 459 (2003) (describing the harm to families and children from child removals and also noting the danger children face in the foster care system); Doriane Lambelet Coleman, *Storming the Castle to Save the Children: The Ironic Costs of a Child Welfare Exception to the Fourth Amendment*, 47 WM. & MARY L. REV. 413, 417–19 (2005) (describing the damage child welfare investigations inflict on children).

91. Alicia LeVezu, *Alone and Ignored: Children Without Advocacy in Child Abuse and Neglect Courts*, 14 STAN. J. CIV. RTS. & CIV. LIBERTIES 125, 126 (2018) (describing studies which found that children in the foster care system have higher rates of juvenile delinquency and involvement with the criminal justice system).

92. *See* Humphries v. County of Los Angeles, 554 F.3d 1170, 1178 (9th Cir. 2009) (noting that the consequences of parents being listed in California's Central Index include the inability to secure licenses for a variety of jobs); Amy Sindin, *"Why Won't Mom Cooperate?": A Critique of Informality in Child Welfare Proceedings*, 11 YALE J.L. & FEMINISM 339, 362–63 (1999) (describing the mental health consequences created by family separation on children and parents); *see also* EUBANKS, *supra* note 6, at 161 (describing the impact that a child welfare investigation has on families).

93. *See* Nina Rabin, *Disappearing Parents: Immigration Enforcement and the Child Welfare System*, 44 CONN. L. REV. 99, 102 (2011) (explaining that the intersection of child welfare and immigration systems increases the likelihood of family separation and deportation); David B. Thronson, *Creating Crisis: Immigration Raids and the Destabilization of Immigrant Families*, 43 WAKE FOREST L. REV. 391,

child maltreatment is missed. Because there is an "unavoidable nexus" between the two types of errors, an algorithmic shift towards one automatically creates an opposing shift away from the other.[94]

Computer programmers must "tune" an algorithm to favor one type of error over the other, or, if possible, must attempt to weigh each of these algorithmic mistakes equally. Each such "tuning" is not only a technological decision, but a political one, the outcome of which privileges different stakeholders.[95] Unfortunately, these political decisions are often made without the input of anyone other than a private company or individual programmer.[96] Worse yet, these choices, created through the process of selecting and assigning weights to variables,[97] can be shifted to actively penalize already targeted populations. One striking example of this is how older benefits automation systems were coded so that the computers would interpret all errors against the recipient rather than the agency.[98]

Developing algorithmic decision-making systems to prioritize false positives, especially in systems that involve state coercion and control, is politically driven and often connected to economic concerns. A probation algorithm implemented in Philadelphia was initially intentionally coded to overpredict the likelihood that an inmate would commit a violent crime if paroled.[99] When the city realized the cost of serving the large number of inmates flagged by a system tuned to prioritize false positives, it had the developer alter the weighting of

---

408–09 (2008) (discussing how states are using immigration status to decline family reunification services).

94. Robert J. Lukens, *The Impact of Mandatory Reporting Requirements on the Child Welfare System*, 5 RUTGERS J. L. & PUB. POL'Y 177, 213 (2007).

95. Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 120 (2018).

96. *See supra* note 3 and accompanying text (describing how individual code writers alter governmental policy) and *supra* notes 42–46 and accompanying text (describing governmental ceding of authority to third-party system developers).

97. *See* Virginia Eubanks, *A Response to Allegheny County DHS*, VIRGINIA EUBANK BLOG (Feb. 16, 2018), https://virginia-eubanks.com/2018/02/16/a-response-to-allegheny-county-dhs/ [https://perma.cc/6MRJ-RXK4] (noting that to understand a predictive analytic system, one needs to know the variables and the weight the system assigns to each variable).

98. Jason Parkin, *Adaptable Due Process*, 160 U. PA. L. REV. 1309, 1357–58 (2012). An agency mindset that assumes fraud on the part of those it is supposed to assist is also evident in Michigan's MiDAS system. There, a court determined that the system's questionnaire automatically targeted applicants rather than being a neutral request for an explanation about any discrepancies, which was "decidedly accusatory" and violated a claimant's Fifth Amendment right against self-incrimination. Zynda v. Arwood, 175 F. Supp. 3d 791, 809 (E.D. Mich. 2016).

99. Brustein, *supra* note 69.

the system variables to reduce the number of inmates scored as "high risk" for violent recidivism.[100]

Politics, or at least the sociocultural reflections of politics, influence big data analytics in other ways. Since society is reflected in the information contained in data sets utilized by algorithms in making predictions, even well-designed systems will replicate and amplify the preexisting biases and discrimination inherent in society.[101] Current legal doctrine is often of limited value in remedying these types of harms, because the bias or discrimination created by algorithmic decision-making, even if it tracks constitutionally prohibited prejudice, is masked by outwardly neutral proxy variables coded into the systems.[102] This creates a sort of algorithmic "rational" racism,[103] which can be as destructive as overt prejudice but is easier to miss and harder to challenge.[104]

That predictive algorithms mask preexisting patterns of discrimination is perhaps most visible in policing. Given law enforcement's long history of racial discrimination, proxies for race become "baked"[105] into predictive policing systems. For example, if police primarily arrest people of color from minority neighborhoods for marijuana-related offenses, even though people of all races and all neighborhoods use marijuana at equal rates, the algorithm will

---

100. *Id.*

101. Predictive analytics rely on an iterative process: actions are taken based on algorithmic information; these actions are then translated into further data that is fed back into the system. When run on biased data this creates a feedback loop that perpetuates bias. *See* KADIJA FERRYMAN & MIKAELA PITCAN, DATA & SOC'Y, FAIRNESS IN PRECISION MEDICINE 11 (2018), https://datasociety.net/output/fairness-in-precision-medicine/ [https://perma.cc/YTR7-B38T].

102. A proxy variable is a characteristic that correlates with another attribute that the algorithm's developer wants to include. For example, variables such as neighborhoods or zip codes are outwardly neutral proxies that allow an algorithm to take race into account without referencing race directly. *See* Barocas & Selbst, *supra* note 8, at 712.

103. EUBANKS *supra* note 7, at 190. *See also* Philip Hacker & Bilyana Petkova, *Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers*, 15 NW. J. TECH. & INTELL. PROP. 1, 7–9 (2017) (noting that big data analytics can uncover correlations that are seemingly neutral but track discriminatory traits).

104. *See, e.g.*, Barocas & Selbst, *supra* note 8, at 712–13 (arguing that the intent necessary under Title VII and similar civil rights laws can be masked through manipulation of variables, which serve as proxies obscuring even intentional discrimination).

105. THE RISE OF BIG DATA POLICING, *supra* note 6, at 122. Anywhere race and poverty correlate, systems using variables that measure poverty as any part of their predictive algorithm, such as foreclosures or concentration of multifamily dwellings, will end up replicating systemic racism. *Id.*

correlate both race and minority neighborhoods with marijuana use.[106] When police departments develop strategies based on the results of such an algorithm, the strategies will correlate race with drugs even if race was completely removed from the model, because of the location correlation.[107]

But bias is not limited to predictive policing systems. When Allegheny County was developing its Family Screening Tool (AFST), it selected two outcome variables to be used as stand-ins for child maltreatment.[108] The first variable was community re-referral, where a call to the child maltreatment hotline was initially screened out, but the county received another call to the hotline on the same child within two years;[109] the second was child placement, where a call to the hotline was initially screened in, and resulted in the child being placed in foster care within two years.[110] The county admitted that these two variables were not optimal, but argued that the "model has to test what's available."[111] One of the outcome variables, community re-referral, is based entirely on the most racially biased part of Allegheny County's child welfare system.[112] Thus the county used the activity known to introduce the most racial bias into its child

106. *Id.*

107. *Id.*

108. Outcome variables are used to measure the phenomenon a system is trying to predict. In the Allegheny County screening tool, the outcome variables are "how" child maltreatment was defined in the algorithm. Predictive variables are factors the algorithm determines correlate with finding the outcome variables (child maltreatment). When building the AFST, the developers initially began with close to 300 predictive variables, but ultimately ended up with 131 predictive variables they found highly correlated with either re-referral or child placement. EUBANKS, *supra* note 6, at 144.

109. *Id.* at 143.

110. *Id.* at 144.

111. *Id.* The number of significant individual instances of child maltreatment in the county was not large enough to be able to develop a statistically significant model, so the developers had to select other events or actions to include as outcome variables. *Id.*

112. Community members call the hotline three and a half times more often on black and biracial families than they do on white families. EUBANKS, *supra* note 6, at 153. In its own study, Allegheny County determined that the greatest racial disproportionality in its child welfare system takes place at the point when a community member calls to refer a child via the abuse and neglect hotline, not when a screener determines whether or not to screen the child into the system. *Id.*; *see also* Press Release, Marc Cherna, Dir., Dep't of Human Servs., *DHS Response to Automated Inequality by Virginia Eubanks* (Jan. 31, 2018), https://www.alleghenycounty.us/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=6442461672 [https://perma.cc/S3CQ-SCTA] (acknowledging racial bias in call referrals).

welfare system as one of two events the model defined as child maltreatment.[113]

The AFST system also oversampled poverty as an indicator that a child was at high risk of harm. This is because the majority of the predictive variables[114] the algorithm analyzed tracked income-based programs such as food stamps, TANF grants,[115] county medical assistance and supplemental security income (SSI), or other indicators of poverty such as homelessness, lack of food, or any family involvement with the juvenile justice or probation systems.[116] Thus by its selection of which outcome and predictive variables the system would measure, Allegheny County created an algorithm that directly links poverty and race to the likelihood of child maltreatment.[117]

Once a family is scored as "at high risk" by the AFST, they come under increased scrutiny and surveillance, creating a potential cycle of bias. The information is permanently stored in the Allegheny County database.[118] Behavior that might have once been seen as inconsequential will forever be viewed through a lens that marks the family as potential abusers.[119] If Allegheny County implements a

---

113. This was done even though there were other variables that could have reduced algorithmic bias — the system could have used likelihood of being screened into the system or only used the likelihood of removal, both of which are based on the professional judgments of caseworkers and family court judges. EUBANKS, *supra* note 6, at 155.

114. *Id.* at 143–44 (explaining the difference between predictive and outcome variables). Once the AFST system is implemented, the algorithm searches the information in the county database on those living with the child for any of the predictive variables and, using a system that weights each variable, assigns the family a score suggesting how more or less likely it is the child will be maltreated. *Id.*

115. Temporary Assistance for Needy Families (TANF) is the federal program that provides monies to states via block grants for aiding poor families. Andrew Hammond, *Welfare and Federalism's Peril*, 92 WASH. L. REV. 1721, 1722 (2017).

116. EUBANKS, *supra* note 6, at 156.

117. *Id.* at 144.

118. *Id.* at 150.

119. In the past, a family that successfully extracted itself from the child welfare system or a person found not guilty of a crime could fade into "practical obscurity," because the government did not have the capacity to capture and analyze the data necessary to reveal past entanglements with government entities. *See* Fred Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 435 (2008) (noting that technology erodes the individual privacy once provided by "practical obscurity"). Eubanks' exploration of the AFST demonstrates the persistent and discriminatory nature of algorithmic scoring. The reader is introduced to a family with a child that was subject to a series of child welfare investigations, all unfounded — meaning there was no indication of child maltreatment — based on referral calls possibly made by an angry neighbor. Even though all of those calls were unfounded, that call information goes into and remains in the county data pool. Because the algorithm uses chance of re-referral as one of its

predictive policing algorithm, this information could be forever factored into that system as well.[120] A similar phenomenon occurs when predictive policing systems target those who live in high crime areas or have had repeated contacts with police, because those variables correlate with crime.[121] This feedback loop, which has been tellingly described as "selection bias meets confirmation bias,"[122] consistently directs police back into the same neighborhoods, thereby continuing to populate databases with data reinforcing the systems' initial biased predictions.

Challenging algorithmic decision-making is made even more difficult because the technology consists of multiple layers of complex subsystems. For example, during the litigation challenging Arkansas's implementation of its Medicaid algorithm,[123] it became clear that there were at least two major subsystem errors causing mistaken reductions in benefits. One was within the algorithm itself and the other was in the software of another company responsible for creating the platform that allowed the algorithm to interface with the state's database.[124] While this particular error was somewhat

---

proxy variables, this child is forever connected to a series of referral calls. Allegheny County is apparently considering applying its system to every child born in the county. EUBANKS, *supra* note 6, at 171–72. If this child grows up and gives birth in Allegheny County that data will follow her, increasing the likelihood that the algorithm will flag her own newborn child as at risk for maltreatment, regardless of her parenting capacity. *See id.*

120. *See id.* at 135 (describing the different county entities whose records are stored in a central repository in which the child welfare algorithm is run. These include adult and juvenile probation records, county jail records, and Allegheny County police records.); *see also* THE RISE OF BIG DATA POLICING, *supra* note 6, at 14–18 (describing the interlinked and permanent digital record of information on individuals based on information collected by local, state, and federal governments which are often searchable by a myriad of government entities); EUBANKS, *supra* note 6, at 93–94 (personal information about those seeking homeless services in Los Angeles shared with the Los Angeles Police Department).

121. THE RISE OF BIG DATA POLICING, *supra* note 6, at 46–48.

122. Kristian Lum & William Isaac, *To Predict and Serve?*, 13 SIGNIFICANCE 14, 16 (2016), https://doi.org/10.1111/j.1740-9713.2016.00960.x [https://perma.cc/8HYA-4Q8H].

123. *See* Lecher, *supra* note 40 (describing Arkansas's adoption of algorithmic assessment system for Medicaid patients).

124. *Id.*; Transcript of Trial at 38, 40, Jacobs *ex rel.* v. Gillespie, 3:16-cv-00119 (E.D. Ark. Oct. 27, 2016) [hereinafter *Jacobs* Trial Transcript] (on file with author). Similarly, in a recently filed class action in the Michigan Unemployment Insurance debacle, the complaint alleged that three different groups of private corporate actors designed, created, implemented, or maintained the error-ridden automated MiDAS system deployed by the state. Cahoo v. SAS Inst. Inc., 322 F. Supp. 3d 772, 787 (E.D. Mich. 2018).

complex,[125] even simple calculation errors can create a cascade of algorithmic mistakes.[126] Additionally, coding errors remain hidden unless there is a concerted challenge to the system or repeated annual testing.[127]

C. Inaccurate and Discriminatory Data

Big data analytics includes not just the computer algorithms themselves, as straightforward or complex as they may be. Big data analytics includes "big data." Even carefully constructed and transparent algorithms are only as good as the data they process. It is through the data that algorithms detect patterns and make predictions, and it is the data that determines how well algorithms actually function.[128] Data sets, especially the massive data sets needed to train predictive analytic systems, are another important reason why the predictive analytics used by governments to target and control vulnerable populations are dangerously flawed.

The immense data sets that big data analytics require are often inaccurate and incomplete and are generally impervious to attempts at correction. While governments have always surveilled people within their borders, one key aspect of modern data collection is the extent to which data is aggregated to create vast, searchable, ever-growing data sets. This "big data" comes in large part from private data brokers[129] that collect, aggregate, and sell information gleaned from an almost unimaginable range of sources.[130] Government

---

125. *See Jacobs* Trial Transcript, *supra* note 124, at 36–37 (documenting the difficulty the State's attorney and the judge had with understanding where the errors occurred and how each might affect the case).

126. *See* Eric Westervelt, *Did a Bail Reform Algorithm Contribute to this San Francisco Man's Murder?*, NAT'L PUB. RADIO (Aug. 18, 2018, 2:00 PM), https://www.npr.org/2017/08/18/543976003/did-a-bail-reform-algorithm-contribute-to-this-san-francisco-man-s-murder [https://perma.cc/G29J-LDY7] (reporting that mistakes in calculating the number of days an inmate had spent in jail led to an incorrect risk assessment score for the court to review when making pre-trial release determination).

127. *See* K.W. v. Armstrong, 180 F. Supp. 3d 703, 714 (D. Idaho 2016) (noting that inaccuracy of algorithmic "budget tool" for Medicaid recipients "puts a premium on testing the tool for accuracy").

128. Lehr & Ohm, *supra* note 3, at 677.

129. Data brokers supply data or inferences about people gathered mainly from sources *other than* the data subjects themselves. RIEKE ET AL., *supra* note 53, at 11.

130. *See id.* at 9–11 (observing that data is gathered from public sources such as state licensing information, school data, social media, etc., as well as from private sources such as information provided by healthcare systems, financial institutions, employers, and retailers); THE RISE OF BIG DATA POLICING, *supra* note 6, at 12–15

agencies also compile their own massive data sets, built on arrest records, convictions, alleged gang affiliations, probation and parole records, child welfare reports, licensing applications, education records and other sources.[131] Technological advances allow these data sets to be searched across formats without requiring the data to be centrally located or merged.[132]

As governments routinely purchase data from data brokers, the separation between public and private data is continuously eroded.[133] This "collect it all" mindset,[134] which endorses the gathering and retention of as much data as possible, serves two functions. First, it reifies data analytics as a tool of state control.[135] Second, it creates the massive data sets necessary for predictive analytics.[136] Additionally, governments' propensity to collect, store, and search ever-increasing amounts of information fosters a public-private symbiotic relationship which reinforces the market for algorithmic social control systems.

The problem is that all large data sets are "dirty," filled with errors and mistakes.[137] Neither private companies[138] nor governments spend the time and money necessary to ensure their accuracy.[139] In

---

(describing the myriad ways in which individuals are tracked and surveilled, and the data sold to data brokers).

131. THE RISE OF BIG DATA POLICING, *supra* note 6, at 17–19.

132. Max N. Helveston, *Consumer Protection in the Age of Big Data*, 93 WASH. U. L. REV. 859, 867 (2016).

133. Governments can purchase directly from data brokers, or indirectly when they use systems provided by private companies that themselves rely on data provided by data brokers.

134. THE RISE OF BIG DATA POLICING, *supra* note 6, at 107.

135. Wayne A. Logan & Andrew Guthrie Ferguson, *Policing Criminal Justice Data*, 101 MINN. L. REV. 541, 549 (2016).

136. *See* THE RISE OF BIG DATA POLICING, *supra* note 6, at 13 (observing that the combination of big data and new analytic tools supports development of predictive policing algorithms).

137. *See, e.g.*, Madden et al., *supra* note 29, at 87 (noting the "troublingly high" error rate in consumer credit reports); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 398–99 (2015) (describing the errors in police gang databases, arrest reports, and FBI files); Richard Warner & Robert H. Sloan, *The Ethics of the Algorithm: Autonomous Systems and the Wrapper of Human Control*, 48 CUMB. L. REV. 37, 44–45 (2018) (stating predictive analytics require data to be simplified and decontextualized, removing ambiguity and narrative essential to explaining human behavior).

138. *See* Madden et al., *supra* note 29, at 88 (describing the difficulty consumers face when attempting to correct errors in credit reports).

139. Barocas & Selbst, *supra* note 8, at 689 (2016) (noting that decision-makers justify using easily accessible but inaccurate data because of the higher cost of creating accurate data sets).

addition, data brokers do not merely sell factual data, incorrect or not. They also sell model data — inferences about individuals based on algorithmic predictions.[140] This creates an additional layer of less than accurate information government algorithms analyze. Thus, error rates in government systems are often exacerbated when governments combine data from data brokers with already problematic government data.[141] Large data sets are also vulnerable to generating their own errors in the form of false or spurious statistical relationships. This is because the risk of an algorithm surfacing a statistically significant but contextually meaningless connection between variables increases as the size of data sets increases.[142]

Data error leads to faulty predictions and potentially dangerous wrong decisions.[143] In 2009, Justice Ginsburg warned that "[i]naccuracies in expansive, interconnected collections of electronic information raise grave concerns for individual liberty."[144] That

---

140. RIEKE ET AL., *supra* note 53, at 11.

141. Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109, 136 (2017) (describing how data brokers assemble and organize their data on the assumption that it will be used for advertising, a very risk-tolerant activity, which means that brokers have no incentive to correct errors).

142. Rick Swedloff, *Risk Classification's Big Data (R)evolution*, 21 CONN. INS. L.J. 339, 355 (2015); *see also* Nicholas Taleb, *Beware the Dangers of Big Data*, WIRED MAG. (Feb. 8, 2013), https://www.wired.com/2013/02/big-data-means-big-errors-people/ [https://perma.cc/LY3Q-HEMT] ("[I]n large data sets the large deviations the algorithms surface are vastly more attributable to variance (or noise) than to information (or signal)"). One example of this was the claim that algorithmic mining of Google search results predicted the spread of the flu more accurately and quickly than the Center for Disease Control and Prevention. This heralded prediction capacity faltered and ultimately failed in part because the size of the data set surfaced spurious correlations. *See* Gary Marcus & Ernest Davis, *Eight (No, Nine!) Problems with Big Data*, N.Y. TIMES (Apr. 6, 2014), https://www.nytimes.com/2014/04/07/opinion/eight-no-nine-problems-with-big-data.html [https://perma.cc/CXE8-WT36].

143. For example, Intrado's "Beware" system promises to provide "real time threat scores" to police. Threat scores have real time consequences because they affect and alter police response to a particular address. *See* THE RISE OF BIG DATA POLICING, *supra* note 6, at 187.

144. Herring v. United States, 555 U.S. 135, 155 (2009) (Ginsburg, J., dissenting). The impact of database reliability issues continues to percolate through the courts. *See, e.g.*, United States v. Esquivel-Rios, 786 F.3d 1299, 1302 (10th Cir. 2015) ("This court and others have regularly upheld traffic stops based on information that the defendant's vehicle's registration failed to appear in a law enforcement database — at *least when the record suggested no reason to worry about the database's reliability*." (emphasis added)). Here, the Court of Appeals for the Tenth Circuit found that there was evidence "suggesting that the database on which the officer relied to justify his stop might bear a real problem — a problem that might mean a 'no return' *doesn't* suggest criminal conduct but only some bureaucratic snafu." *Id.*

warning was not heeded, and as more governmental decisions become automated, the situation has only worsened. Unfortunately, as we have become a nation reliant on technology, "data error" has become a mundane excuse that conceals real harm.

That data error has the potential to disrupt individual liberty is made clear in police creation of gang databases. Law enforcement conceptualizes gangs as a problem of racialized young men, as evidenced by the fact that most people in gang databases are men of color, most of whom do not have criminal records.[145] Being incorrectly labeled a "gang member" has negative consequences not only for the person so labeled, but also for those associated with such person.[146] Since predictive policing technologies operate within these racialized databases, the algorithms used in these systems cannot avoid being racially discriminatory.[147]

Data errors not only infect data sets created by commercial data brokers or law enforcement — large government agencies, such as state health and human services departments or education systems, create, collect, and (often poorly) manage large amounts of data pertaining to various populations. State agency data error is comically widespread with potentially tragic results.[148] In Indiana's rush to privatize and automate its public benefits system, for example, the state moved to a centralized document processing center.[149] So much of the data either went missing or was incorrectly entered in digital case files that the processing center became known as the "black hole in Marion."[150]

---

145. RUTHANN ROBSON, DRESSING CONSTITUTIONALLY: HIERARCHY, SEXUALITY, AND DEMOCRACY FROM OUR HAIRSTYLES TO OUR SHOES 124 (2013). In California, a state auditor found systemic failures in gang databases including the listing of forty-two infants as gang members. *See also* THE RISE OF BIG DATA POLICING, *supra* note 6, at 52.

146. Predictive policing uses social networking to link individuals to friends, family, and associates, and uses this information to target those connected to the initial target. *See* Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109, 1137–38, 1140 (2017).

147. THE RISE OF BIG DATA POLICING, *supra* note 6, at 53.

148. *See, e.g.*, Zynda v. Arwood, 175 F. Supp. 3d 791, 806 (E.D. Mich. 2016) (deciding that allegations of high error rate in an unemployment fraud detection system supported standing for legal services office); State of New Mexico *ex rel.* Stewart v. N.M. Pub. Educ. Dep't, D-101-CV-2015-00409, at 24–27 (Santa Fe County Ct. Dec. 2, 2015) (noting large numbers of errors in data used in teacher assessment system, suggesting the system could not be trusted); K.W. v. Armstrong, 180 F. Supp. 3d 703, 711–12 (D. Idaho 2016) (describing the massive errors in Idaho's Medicaid data base).

149. *See* EUBANKS, *supra* note 6, at 50.

150. *Id.*

Automating the processing of public benefits not only increases the chance for data error through centralization, but also by drastically reducing the number of caseworkers assisting clients navigating public benefits systems.[151] By reducing the ability to talk to a human caseworker who can resolve errors and mistakes, these systems create an inflexible process where data error, no matter how inconsequential or inadvertent, no matter whose fault, is deemed a "failure to cooperate,"[152] which is the bureaucratic conclusion that terminates someone's healthcare, food stamps, or housing allotment. The landscape of state attempts to automate their benefit systems is littered with thousands of people in dire circumstances who, because of data error, lost their benefits.[153] The designation of "failure to cooperate," especially when it emanates from an automated system that minimizes the ability to engage with another human being to solve the problem, is dehumanizing, frightening, and destabilizing.[154]

Data errors contained in the large data sets used by governments are almost impossible to challenge or correct,[155] not to mention that the existence of the databases themselves is often kept secret.[156] Because predictive analytics require as much data as possible in order to function, private companies and public agencies are inclined to use data even when they know it is wrong. For example, the officials using analytics to predict child maltreatment in Allegheny County argued that allowing parents to expunge hotline reports on their

---

151. *Id.* at 62–63; *see also* Perdue v. Murphy, 915 N.E.2d 498, 501 (Ind. Ct. App. 2009) (noting that because of the loss of caseworkers, "[w]hile it is mathematically possible, it is unlikely that a client calling about his or her case would speak to the same employee each time").

152. EUBANKS, *supra* note 6, at 53; *see also supra* note 98 and accompanying text (noting how systems are tuned so that all errors run against the recipient).

153. *See, e.g.*, *supra* notes 46–50 and accompanying text; *see also* EUBANKS, *supra* note 6, at 53 (describing in detail the impact of data error in attempted automation of Indiana's public benefit system).

154. *See* EUBANKS, *supra* note 6, at 53, 70 (providing narratives from some of those harmed by Indiana's implementation of its privatized benefits system).

155. THE RISE OF BIG DATA POLICING, *supra* note 6, at 62 (discussing the fact that there are no processes for correcting errors in many police documents such as rap sheets and arrest records); Rebecca A. Hufstader, *Immigration Reliance on Gang Databases: Unchecked Discretion and Undesirable Consequences*, 90 N.Y.U. L. REV. 671, 680 (2015) (noting how difficult it is to challenge being incorrectly listed in a gang database, and that most people are unaware they may be included in a gang database because the databases are considered confidential).

156. Many law enforcement or security databases remain secret. *See* Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1745–46 (2015) (law enforcement databases classified or confidential); *see also* Hufstader, *supra* note 155, at 684 (gang data bases as confidential).

children, no matter how spurious, would rob the agency of critical data.[157] However, without expungement, this misleading and erroneous data will continue to be used by the algorithm to score children and families in the future.

In addition to data error, there is the issue of who is included and who is missing from data sets. Wealth and social privilege provide protections from aggressive police surveillance, creating a data gap that can shield the privileged from predictive policing systems.[158] In contrast, poverty and race attract over-policing and hyper-surveillance, which disproportionately populates police databases with information on poor communities and people of color.[159] Given that predictive algorithms learn from the data sets they analyze, predictive policing algorithms based on skewed crime data replicate and exacerbate preexisting biases already inherent in the system.

Similar problems exist in algorithms built to predict child maltreatment. These algorithms analyze data regarding a person's history of public assistance, drug use and mental health issues, as well as their past experiences with the child welfare or the juvenile justice systems, to determine risk scores.[160] This is information based almost entirely on whether someone uses public services or has contact with the criminal justice system. Missing almost completely, however, is data on people able to access private drug or alcohol treatment, mental health services, financial support, or who were able, based on social privilege, to minimize contact with the criminal justice

---

157. EUBANKS, *supra* note 6, at 164. *See also* Humphries v. County of Los Angeles, 554 F.3d 1170, 1175 (9th Cir. 2009) (noting that California refused to expunge parents from a child abuse database even when the parents were found "factually innocent").

158. THE RISE OF BIG DATA POLICING, *supra* note 6, at 180 (describing how private property, economic mobility, and social status create significantly different data patterns for rich and poor persons, and how, in a data driven policing system, that difference would give the wealthy a "presumption of data driven innocence").

159. *Id.* at 75 (describing discrepancies in police stops and searches of people of color, primarily black men in Ferguson, Missouri, and discussing police targeting Skid Row with facial recognition technology and focused data collection via aerial surveillance over West Baltimore — a predominately African-American community).

160. *See supra* notes 114–16 and accompanying text. While this Article is focused on the issues surrounding the use of algorithmic mechanisms to control marginalized populations in the United States, similar systems, often built by the same private companies, are being implemented globally. In the United Kingdom, a similar system monitoring families reviews data on debt, worklessness, benefits, housing, domestic violence, and anti-social behavior, among other factors, to create a "family profile." Luke Stevenson, *Artificial Intelligence: How a Council Seeks to Predict Support Needs for Children and Families*, COMMUNITY CARE (Mar. 1, 2018), http://www.communitycare.co.uk/2018/03/01/artificial-intelligence-council-seeks-predict-support-needs-children-families/ [https://perma.cc/YR7V-Z9GL].

system.[161] Thus, those who can access private programs and support services will disproportionately receive lower risk scores, regardless of their individual likelihood to harm their children, than those using similar services provided by the county.

With algorithmic decision-making, what counts is the content of the data set, even if that content is unreliable, biased, or just plain wrong. Because problematic algorithms rely on flawed and biased data sets, governmental decision-making is bound to repeat and reinforce the already existing discrimination and bias created by past conduct used to control marginalized populations. To successfully challenge government adoption of these technologies, it is important to understand the psychology, history, and politics driving their use.

II. FORCES DRIVING GOVERNMENT ADOPTION OF BIG DATA ANALYTICS

Algorithmic decision-making systems are often promoted with claims of efficiency, cost savings, and reduction of human bias.[162] But they are also sold to the public using language that politicizes poverty and crime. For example, Indiana's governor characterized the state's welfare system as "wasteful, fraudulent," and "broken beyond the ability of state employees to fix it" in order to sell the public on a costly new automated system designed and managed by a private corporation.[163] Predictive policing systems are described as race-neutral and "objective" tools, even though they allow the continuation of aggressive policing practices.[164]

The language used to champion these technologies mirrors the forces driving governments to employ them: a deference to science and technology, the historical success of technological social control mechanisms, and the neoliberal embrace of privatization. To successfully challenge predictive algorithms and the social control mechanisms they perpetuate, advocates must not only understand the technology, they must understand the forces driving its adoption.

---

161. EUBANKS, *supra* note 6, at 147. When asked whether the county was going to seek information from private providers, administrators said they wanted private data but receiving it was likely impossible. *Id.* at 157.

162. *Id.* at 9; THE RISE OF BIG DATA POLICING, *supra* note 6, at 6.

163. These political claims were highly contested. EUBANKS, *supra* note 6, at 46. In addition, Indiana signed a billion-dollar contract with a private company to develop the system after only one public hearing. *Id.* at 48.

164. THE RISE OF BIG DATA POLICING, *supra* note 6, at 6.

A. Deference to Science and Technology

Governments at all levels are flocking to predictive technologies that "bear the glossy veneer of science,"[165] driven in large part by perceptions that the technology is infallible.[166] This is one instantiation of automation bias — the human tendency to disregard contradictory information in light of computer-generated solutions.[167] This bias can lead those using decision-making technologies to rely on automated decisions even when they suspect a system has malfunctioned.[168] Uncritical deference to technology is aggravated by the inability of those outside the technical community to understand algorithms or the science behind predictive analytics.[169] This technological ignorance adds to the mystique of algorithmic infallibility, giving many a distorted, subservient, almost "theological view" of computational accuracy.[170]

Automation bias subconsciously alters behavior. The developers of the Allegheny County child welfare algorithm claimed that the predictive system was designed so that risk scores it generates would be questioned by intake screeners.[171] In actuality, screeners started to defer to the system — in some instances, screeners asked managers for permission to go back and change their initial risk assessment scores if the algorithm produced a different score.[172] Similarly, some police officers have shifted their patrol patterns in response to over-reliance on various predictive policing tools. For example, officers in

---

165. Megan Stevenson, *Assessing Risk Assessment in Action*, 103 MINN. L. REV. (forthcoming 2019) (manuscript at 1) (on file with authors).

166. Deven R. Desai & Joshua A. Kroll, *Trust but Verify: A Guide to Algorithms and the Law*, 31 HARV. J.L. & TECH. 1, 4 (2017).

167. Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669, 711–12 (2010).

168. *See* Citron, *supra* note 1, at 1271 (noting that literature in the field of cognitive systems engineering finds that humans view automated systems as error-resistant and rely on computer output even when they suspect a system malfunction).

169. Bamberger, *supra* note 167, at 712; *see also* Harry Surden, *Values Embedded in Legal Artificial Intelligence* (U. Colo. L. Legal Stud., Research Paper No. 17-17, Oct. 18, 2017), http://ssrn.com/abstract=2932333 [http://perma.cc/3RUC-54PP] (arguing that algorithmic recommendations in sentencing creates an illusion of how mathematical "objectivity" can mask underlying subjective human judgments of system designers).

170. Ian Bogost, *The Cathedral of Computation*, ATLANTIC (Jan. 15, 2015), http://www.theatlantic.com/technology/archive/2015/01/the-cathedral-of-computation/384300 [https://perma.cc/P4AA-UNJ7].

171. EUBANKS, *supra* note 6, at 141 (noting that the developer insisted the model was built in such a way that the screeners would question its predictive accuracy and trust their own judgment).

172. *Id.* at 142.

Los Angeles working with a predictive policing system that highlighted potential crime geographically became overly focused on the areas highlighted by the system, to the point where they had to be explicitly trained to patrol "outside the box."[173]

But automation bias can result in more frightening results. Consider the arrest of Denise Green, a 47-year-old African American municipal worker with health and mobility issues. Late one evening, Ms. Green was pulled over, forced out of her car, told to kneel in the street, and handcuffed as four officers pointed their weapons at her.[174] Ms. Green was stopped because police responded to a faulty alert from an Automatic License Plate Reader (ALPR).[175] As the court noted, ALPR systems are known for "false hits," and police protocol required the officers to independently verify the validity of the information prior to executing a stop.[176]

Ms. Green's experience is indicative not only of police over-dependence on big data analytics, but also of the structural and implicit racism that leads to over policing.[177] Because of the known flaws in our preexisting social structures, the officers were trained that an ALPR "hit" by itself did not justify a vehicle stop. But the officer who stopped Ms. Green not only failed to verify the validity of the license plate number, he instituted a "high risk" felony stop of the vehicle.[178] This stop was so intrusive a court held that a rational jury could find that it amounted to an unlawful arrest.[179] While Ms. Green was "merely" frightened and humiliated, given the history of police violence against unarmed black people,[180] the incident could have turned out far worse.

Deference to science and technology is a component of governmental misuse of algorithmic decision-making tools, but it also reinforces preexisting individual biases. Predictive technologies reproduce societal discrimination, but the tools are also used by

---

173. THE RISE OF BIG DATA POLICING, *supra* note 6, at 80.

174. Green v. County of San Francisco, 751 F.3d. 1039, 1043 (9th Cir. 2014).

175. *Id.* (reversing and remanding the trial court's grant of summary judgment for the City finding that the officers never visually confirmed the license plate match).

176. *Id.* at 1042.

177. *See generally* Robert J. Smith et al., *Implicit White Favoritism in the Criminal Justice System*, 66 ALA. L. REV. 871 (2015) (describing the implicit racial bias in the criminal justice system and arguing that in addition to implicit and structural bias there is also a structural white favoritism).

178. *Green*, 751 F.3d. at 1043.

179. *Id.* at 1047–48.

180. *See, e.g.*, Paul-Emile, *supra* note 26, at 308 (noting increased violence against unarmed black people).

individuals with their own inherent biases, implicit or explicit. Thus, deference to technology is superimposed on and reinforces individual bias. This creates a situation in which people of color are far more likely to be harmed by officers relying on algorithmic decision-making tools, especially where system outputs coincide with and thus "confirm" an individual officer's own biases.[181]

Automation bias also exists within the judicial system. Judges are not immune from the "gravitational pull"[182] of scientific evidence that appears neutral and objective.[183] Case law is littered with instances of courts admitting now discredited "scientific" evidence, such as bite-mark testimony or firearm and toolmark identifications.[184] The discrediting of this evidence came not from new advances in science, but from persistent challenges that the evidence was never valid in the first place.[185] Because courts failed to require validation of new claims of scientifically reliable evidence, much of what is now considered "junk science" gained a foothold in the justice system.[186]

This is of particular concern in criminal and family court, which are far more lenient in admitting scientific evidence proffered by the state than by those challenging the state.[187] Given that states are already

---

181. Rich, *supra* note 8, at 899–900 (discussing how individual officer bias inhibits an officer from determining that an automated suspicion algorithm is wrong when the information coincides with the officer's own biases); L. Song Richardson, *Police Efficiency and the Fourth Amendment*, 87 IND. L.J. 1143, 1146–51 (2012) (discussing the extensive studies showing impact of implicit bias, especially against black men).

182. Clare Huntington, *The Empirical Turn in Family Law*, 118 COLUM. L. REV. 227, 287 (2018).

183. *See id.* at 232–33 (2018) (stating that because empirical evidence appears neutral, the State can argue that it is following the algorithm and thus evade engaging in difficult and complex child welfare issues); *see also* Citron, *supra* note 1, at 1254 (noting that hearing officers in benefits proceedings are likely to trust the computer-supported decision until and unless appellants can produce expert testimony showing potential for error).

184. *See* Simon A. Cole, *Changed Science Statutes: Can Courts Accommodate Accelerating Forensic Scientific and Technological Change*, 57 JURIMETRICS J. 443, 446 (2017) (discussing scientific experts who proffered incriminating testimony at trial and subsequently came to doubt their original testimony).

185. *Id.* at 453–55.

186. *Id.* at 457.

187. Stephanie L. Damon-Moore, *Trial Judges and the Forensic Science Problem*, 92 N.Y.U. L. REV. 1532, 1535 n.18 (2017). While Damon-Moore focuses on criminal cases, child welfare and even benefits administration has come to mimic the criminal justice system in its function of controlling marginalized populations. Child welfare is an area of law that has long allowed a wide array of so-called "syndromes" and other "scientific" evidence to support claims of child abuse. *See generally* Maxine Eichner, *Bad Medicine: Parents, the State, and the Charge of Medical Child Abuse*, 50 U.C. DAVIS L. REV. 205 (2016).

introducing machine learning algorithms into their law enforcement and child welfare systems, the next step may well be attempting to introduce risk scores as "scientific" evidence supporting probable cause or child maltreatment, based on claims that predictive algorithms are objective, neutral, and technologically sound.

Uncritical reliance on technological decision-making tools also interacts with and reinforces other biases. One such example is the "anchor effect," a cognitive bias that describes the human tendency to adjust judgments or assessments in response to previously disclosed external information — an "anchor."[188] In criminal sentencing, appellate courts are beginning to examine how initial sentencing recommendations may improperly "anchor" judges to an improper and inflated sentencing range.[189] The anchoring effect occurs even when the initial anchor is implausible, although the effect on a decision-maker is greater when the initial anchor is plausible.[190]

Consider these combined biases in the context of algorithmic risk assessment systems: automation bias makes an algorithmic risk assessment score seem "more plausible," while the anchoring effect maximizes the algorithm's impact on the decision-making process. Because these psychological forces occur unconsciously,[191] bias and errors in judgment stemming from them go undetected.[192] As more aggressive discriminatory biases are layered on top of problematic but socially benign ones, it becomes clear that algorithmic systems of social control do not only harm people, but also create real and significant obstacles for those attempting to challenge their use.

Deference to technology also makes disputing technological determinations expensive and unattainable for those who cannot

---

188. Hon. Mark W. Bennett, *Confronting Cognitive "Anchoring Effect" and "Blind Spot" Biases in Federal Sentencing: A Modest Solution for Reforming a Fundamental Flaw*, 104 J. CRIM. L. & CRIMINOLOGY 489, 495 (2014).

189. *See, e.g.*, United States v. Navarro, 817 F.3d 494, 501 (7th Cir. 2015) (noting that an improper upper guidelines number offered by the government may well have anchored the district judge to an inflated sentencing range); United States v. Ingram, 721 F.3d 35, 40–41 (2d Cir. 2013) (Calabresi, J., concurring) (noting that a two-step process requiring judicial discussion of individual factors can reduce the anchoring effect in sentencing).

190. Bennett, *supra* note 188, at 499–500. The anchoring effect would influence anyone working with a risk assessment tool that produces a numerical score including those used in child welfare. *Id.*

191. *Id.* at 491 (describing unconscious reliance on mental shortcuts and heuristics when making complex decisions).

192. *Id.* at 491–92 (pointing out that because the cognitive biases are hidden, judges (and others) often actively resist the suggestion that their decisions have been affected by them).

afford the experts necessary to establish system error. Arkansas's adoption of a new algorithmic assessment program for Medicaid inexplicably and drastically reduced benefits to many recipients.[193] It was not until the developer of the algorithm was actually testifying at trial, when he was asked to walk the court through the algorithmic decision-making system, that the specific system errors were discovered.[194] This occurred after months of costly federal litigation, thousands of attorney hours,[195] and, most importantly, loss of medical coverage for many recipients.

Problematically and predictably, Arkansas was implementing the algorithm in a "low rights environments," where there is little expectation of political accountability and those affected have no right to counsel.[196] Governments implement algorithmic decision-making in ways that primarily target already marginalized populations — whether they are focused on reducing welfare rolls or services to the homeless, minimizing support for the disabled, targeting communities of color with predictive policing tactics, or screening people into or out of the state's child welfare systems. The communities most affected by such predictive algorithms must generally rely on underfinanced and understaffed public defender or civil legal services offices to challenge these systems. For those unable to challenge government actions, officials may claim they have waived any right to appeal, even if it is later determined the algorithms used were flawed.[197]

---

193. Complaint at ¶¶ 39–46, 56–61, Jacobs *ex rel.* v. Gillespie, 3:16-cv-00119 (E.D. Ark. 2016) (on file with author) (alleging that the assessment algorithm violated due process, because the basis upon which the algorithm made determinations was never provided, which made it impossible for a recipient to challenge a reduction in services).

194. *See supra* note 124 and accompanying text. As the Legal Aid attorney for the plaintiff pointed out, the mistake was only detected because the one person in the world who could discover it was testifying. *Jacobs* Trial Transcript, *supra* note 124, at 43.

195. As plaintiff's counsel said, "There's this immensely complex system around which no standards have been published, so that no one in their agency caught it until we initiated federal litigation and spent hundreds of hours and thousands of dollars to get here today." Lecher, *supra* note 40.

196. EUBANKS, *supra* note 6, at 12. There is no right to counsel for those challenging reductions in public benefits such as welfare, food stamps, public housing, and Medicaid.

197. *See* Lecher, *supra* note 40. When Arkansas officials learned of the coding error that miscalculated benefits that were due to recipients with cerebral palsy, some officials suggested that recipients who failed to file a timely appeal had waived their rights to the correct benefits, even though no one, including the state officials, knew the algorithm was wrong.

This use of technologies to control marginalized populations is not a coincidence and is not new. The technology allows those in positions of power to sift and sort people — those deserving of aid and support versus those whom society sees as undeserving, dangerous, or criminal.[198] Governments have used technology to contain, control, and criminalize people for hundreds of years, sometimes with spectacularly horrific results.

B. Historical Success of Technology as Domestic Social Control Mechanism

The ability to collect, store, sort, and sift through information about individuals is what has allowed governments to track, stigmatize, and ultimately punish entire populations. Some critics of algorithmic governance systems posit the technology as tremendously useful, but acknowledge it has the capacity to reinforce existing bias and over-criminalize communities of color.[199] Other critics suggest that governments view this technologically enhanced capacity for controlling and criminalizing targeted communities as a feature, not a bug.[200] The latter of these two views is soundly supported by history.

Virginia Eubanks uses the concept of a "digital poorhouse" to compare how the poor and disabled are controlled and managed by state authorized algorithms today with how this population was controlled and managed by the institution of the poorhouse in the 1800s.[201] Eubanks also documents how the United States has evolved in its management of poor populations — from the use of the poorhouse to "scientific charity,"[202] where caseworkers began to investigate and separate the deserving from the undeserving poor in a

198. EUBANKS, *supra* note 6, at 8–9, 123, 176–77.

199. *See, e.g.*, THE RISE OF BIG DATA POLICING, *supra* note 6, at 131–36 (discussing the racist roots of policing and the need for predictive policing systems to be developed to avoid racial bias).

200. *See, e.g.*, EUBANKS, *supra* note 6, at 9–10 (noting how the targeting effects of systems, which reduce aid to the poor in the name of efficiency); NOBLE, *supra* note 7, at 6, 31 (discussing how what many describe as "glitches" in otherwise "near perfect" technology are not mistakes, but either intentional or incredibly reckless coding, and exploring how search algorithms maintain racial and gender subjugation).

201. Reminiscent of the privatization of benefits systems today, the poorhouse was brutal, dehumanizing, established in part to discourage the poor from seeking aid, and often run as a business. EUBANKS, *supra* note 6, at 16–18.

202. *Id.* at 15.

quasi "moral classification" system,[203] and then from scientific charity into the use of eugenics.[204]

Combining white supremacy with fear of the other, eugenics was embraced to protect society from African Americans and the "shiftless, ignorant, and worthless class of anti-social whites."[205] Eugenics was considered a rigorous and data-driven science in its day.[206] It also fit many other aspects of the Progressive Era — the shift to planned capitalism, the reification of efficiency, and the rise of middle class professional managers and scientific experts.[207] The Eugenics Record Office (ERO), overseen by a Harvard biologist and established with funding from the Carnegie Institute, was created to support a modern society by weeding out those considered unfit.[208] To accomplish this, the ERO created a database of family pedigrees, case studies, and indexed records from notes collected by trained field workers.[209]

The ERO, with its "scientific" methodology of data collection and analysis, quickly began to influence government policy. In the 1920s, scientists from the ERO recommended forced sterilization and anti-immigration laws, all based on "science" supported by "data and records."[210] In 1924, Congress passed an Immigration Act effectively barring Eastern Europeans, Jews, Arabs, and East Asians from

---

203. *Id.* at 21–22.

204. *Id.* at 22–23.

205. *Id.*

206. Garland E. Allen, *The Eugenics Record Office at Cold Spring Harbor, 1910–1940: An Essay in Institutional History*, OSIRIS 225, 226 (1986) (eugenics seen as applying "generalized, predictive, and experimentally verifiable concepts of heredity to all living forms); Joshua A. Krisch, *When Racism Was a Science*, N. Y. TIMES (Oct. 13, 2014), https://www.nytimes.com/2014/10/14/science/haunted-files-the-eugenics-record-office-recreates-a-dark-time-in-a-laboratorys-past.html [https://perma.cc/D8SC-J9JY] (characterizing ERO as a premier scientific enterprise in its heyday).

207. Allen, *supra* note 206, at 255; *see also* Krisch, *supra* note 206 (reporting that eugenics started by progressive scientists to assist in creating a more efficient society).

208. Krisch, *supra* note 206 (progressive era scientists at the ERO intent on using genetics to breed "better citizens"); Patrick J. Ryan, *"Six Blacks from Home": Childhood, Motherhood, and Eugenics in America*, 19 J. POL'Y HIST. 253, 255 (2007) (describing the progressive era political embrace of eugenics as a mechanism to address hereditary feeblemindedness as the root of social problems such as crime, delinquency, and poverty).

209. Allen, *supra* note 206, at 240. *See also* Cold Spring Harbor Laboratory's Image Archive on the American Eugenics Movement, Eugenics Record Office, http://eugenicsarchive.org/html/eugenics/static/themes/20.html [https://perma.cc/X7BW-B9ZX] (describing the history and work of the ERO).

210. Krisch, *supra* note 206.

entering the country.[211] At the state level, thousands of people were deemed "unfit" and sterilized.[212] At the time, eugenics served as a science on which to base legal and policy decisions. Today, historians look back and see a pseudo-science sold to legislators and the public that was built on flawed methodologies and evidence that "resonated with social prejudices."[213]

Following the Progressive Era of the early twentieth century, the "science" of eugenics was combined with even greater technological sorting power to assist two of the worst modern-day authoritarian governments in cataloging and culling their citizenry. Nazi Germany and Apartheid South Africa are specters of what "high-tech social sorting" tools can do in countries with severe inequality and totalitarian regimes.[214] Because governments in the United States are actively using predictive analytics to target portions of the American populace, expanding briefly on this history is not an exercise in hyperbole. Rather, it is important to understand how dangerous it can be to wed technology to discrimination through law and policy.[215]

Beginning in 1933, Nazi Germany used a pre-computer punch card system to organize and register its entire population.[216] Once laws were passed that allowed Jews and others deemed unfit to be segregated, stripped of their rights, and ultimately murdered, it was this punch card system, developed by IBM, that created the organizational efficiency that made the Holocaust so catastrophic.[217] The punch card system also allowed the Nazi government to manage the massive logistics of the camps so that one's identity as Jew,

---

211. *See* Katie Kelly, *Enforcing Stereotypes: The Self-Fulfilling Prophecies of U.S. Immigration Enforcement*, 66 UCLA L. REV. DISCOURSE 36, 43–44 (2018) (discussing the Immigration Act of 1924, Pub. L. No. 68-139, 43 Stat. 153 (1924)).

212. Krisch, *supra* note 206. In 1927, with Chief Justice Holmes declaring "three generations of imbeciles are enough," the Supreme Court upheld Virginia's compulsory sterilization law. Buck v. Bell, 274 U.S. 200, 207 (1927).

213. *See* Krisch, *supra* note 206.

214. EUBANKS, *supra* note 6, at 199.

215. *See, e.g.*, Bret D. Asbury, *"Backdoor to Eugenics?": The Risk of Prenatal Diagnosis for Poor Black Women*, 23 DUKE J. GENDER L. & POL'Y 1 (2015) (connecting the racist aspects of the eugenics movement to the degradation of black women's reproductive rights and arguing this history may still be impacting the prenatal genetic counseling provided to poor black women). *See also* Ryan, *supra* note 208, at 274 (seeing eugenics as a constituent part of an ongoing American poverty discourse, rather than a bizarre movement tucked neatly away prior to the Nazi Holocaust, is ever more important at the dawn of the twenty-first century).

216. EDWIN BLACK, IBM AND THE HOLOCAUST: THE STRATEGIC ALLIANCE BETWEEN NAZI GERMANY AND AMERICA'S MOST POWERFUL CORPORATION 54–60 (2001).

217. *Id.* at 8.

Jehovah's Witness, homosexual, work shy, or otherwise cast as asocial or unfit, could never be escaped.[218]

This marriage of social prejudice and technology repeated itself in South Africa. There, to denationalize the non-white population, a complex system of data collection and analysis was institutionalized to sort and track individuals by race.[219] The social engineering that stripped black South Africans of their citizenship was accomplished in large part through advances in computerization that supported the manipulation of the huge amounts of data necessary to establish the passbook system.[220] The passbooks, along with a central registry, worked to "recast raw minority domination as a technological project."[221]

In each of these examples, prejudice and computerization (or its punch code predecessor) enabled an authoritarian government to collect information on vulnerable populations and then sort, track, and target that population in horrendous ways.[222] This is not to say that governmental use of technology will always result in atrocities. But at a time when there is more analyzable data on everyone than ever before, when governmental entities continue to take questionable steps to keep various types of surveillance technology secret, to ignore this history is naïve at best. As the social control functionality of these tools continues to expand, so does governmental interest in their use.

---

218. *Id.* at 364–65. The five-digit code assigned to each person became part of the numbers tattooed on those in the prison camps. *Id.* at 356.

219. Paul N. Edwards & Gabrielle Hecht, *History and the Technopolitics of Identity: The Case of Apartheid South Africa*, 36 J. SOUTHERN AFR. STUD. 619 (2010); *see also* Consolidated and Amended Complaint at ¶¶ 130–141, *In re* South African Apartheid Litigation, 02 MDL No. 1499 (JES) (S.D.N.Y. Oct. 27, 2008) (on file with author) (explaining IBM's role in creating the South African passbook system).

220. Keith Breckenridge, *The Book of Life: The South African Population Register and the Invention of Racial Descent, 1950–1980*, 40 KRONOS SOUTH AFRICAN HISTORIES 225, 235 (2014). For black South Africans, the "Book of Life" became the passbook that stripped them of their citizenship and controlled their ability to work or travel in and around South Africa. *Id.*

221. Edwards & Hecht, *supra* note 219, at 628.

222. The United States government also used the technology of the day to monitor and control suspect communities, under the infamous COINTELPRO program. *See* ROBERT SCHEER, THEY KNOW EVERYTHING ABOUT YOU 34–35, 170 (2015). Past domestic governmental surveillance also seems eerily parallel to current surveillance targeting black communities. *See* Amna Toor, *"Our Identity Is Often What's Triggering Surveillance": How Government Surveillance of #Blacklivesmatter Violates the First Amendment Freedom of Association*, 44 RUTGERS COMPUTER & TECH. L.J. 286, 295–96 (2018).

Predictive analytics and machine learning continue to evolve as developers push the "predictive" capacity of algorithms further into the lives of targeted populations. The algorithm developed to predict child maltreatment in Allegheny County, for example, is apparently being expanded to apply to every child born in that county.[223] In addition, a well-known developer of risk assessment modeling is working on an algorithm to predict, at the moment of birth, whether a person will commit a crime by his or her eighteenth birthday, based on environmental factors and parental history.[224] Such an approach, which assumes a connection between genetics and criminality, has been described as a eugenics approach to fighting crime — an approach which could lead to forced sterilization,[225] this time directed not by the science of the 1920s but by the big data analytics of the 2020s.

Efforts to extend the capacity of algorithmic social control technologies coincides with China's development of one of the most ambitious predictive policing systems in the world. The Chinese government has amassed a database with information on each and every citizen, and is using predictive analytics to monitor and ensure "social stability."[226] All this makes one law enforcement vendor's

---

223. EUBANKS, *supra* note 6, at 171. This expansion of application to all children at birth is counter to the ethical review of the system, which found it "significant" that the AFST was being applied to call screening and not to all children at birth. TIM DARE & EILEEN GAMBRILL, ETHICAL ANALYSIS: PREDICTIVE RISK MODELS AT CALL SCREENING FOR ALLEGHENY COUNTY 2 (2017), http://alleghenycountypa.gov/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=6442457402 [https://perma.cc/T9UR-G583].

224. *See* Brustein, *supra* note 69.

225. Caryn Devins et al., *The Law and Big Data*, 27 CORNELL J.L. & PUB. POL'Y 357, 397 (2017) (discussing how a biosocial approach to crime assumes that genetic factors contribute to criminality and supports curtailing the reproductive capacity of people with "crime prone genes by administering anti-androgens to young post pubertal males at high risk of offending"). A mandatory eugenics approach to criminal justice is not far from where we find ourselves today — several states have chemical castration laws for sex offenders that either allow a judge to mandate the use of the drugs or allow a defendant to elect to take the drugs as a condition for release. *See* Zachary Edmonds Oswald, *"Off With His ____": Analyzing the Sex Disparity in Chemical Castration Sentences*, 19 MICH. J. GENDER & L. 471, 483–84 (2013). Family courts have, and continue to, issue no-pregnancy orders even though such orders are likely unconstitutional. *See* Laura T. Kessler, *A Sordid Case:* Stump v. Sparkman*, Judicial Immunity, and the Other Side of Reproductive Rights*, 74 MD. L. REV. 833, 909–10 (2015).

226. The Chinese government has amassed a database on all its citizen and is using predictive analytics to monitor them. *See* Bryont Chin, *From Tragedy to Statistic: How Big Data Has Changed the Practice of Law*, 9 SING. L. REV. 3 (2018), http://www.singaporelawreview.com/juris-illuminae-entries/2018/from-tragedy-to-statistic-how-big-data-has-changed-the-practice-of-law [https://perma.cc/4ZAD-

marketing claim that it can leverage big data analytics "to anticipate criminal activity" and "predict future events"[227] less unrealistic than it may initially seem.

Big data analytics promises to governments the ability to collect tremendous amounts of data on individuals and then sort, track, and target them at will. In each of the examples above, private individuals and companies — third parties — played outsized roles in the automation of authoritarianism. Whether it is the lure of money, prestige, or prejudice, third parties have been and remain one of the driving forces in governmental adoption of the technologies necessary for algorithmically guided social control.

C. Private Sector Profitability

Privatization of police and social services functions limits democratic transparency, increases the market for algorithmic decision-making technology, and ultimately undermines governmental responsibility to individuals. We are well into an era of hyper-privatization, with a well-documented reduction in government spending and a concurrent attempt to shift much of governmental responsibility to the private sector.[228] This is exacerbated by the fact that most governments, especially local or state governments, do not have the capacity to develop predictive analytic systems without help from private companies or non-profit organizations.[229] This need for outside expertise coincides with neoliberal demands to privatize provision of the social safety net.[230]

L2GP]. *See also China: Police 'Big Data' Systems Violate Privacy, Target Dissent*, HUMAN RIGHTS WATCH (Nov. 19, 2017), https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent [https://perma.cc/4AJX-2FZ6] (describing China's Police Cloud system).

227. AXON, LAW ENFORCEMENT TECHNOLOGY REPORT 22–23 (2017), https://prismic-io.s3.amazonaws.com/axon%2F3f45a833-2abf-417b-ba48-9f77b130b025_2017-le-tech-trends-report.pdf [https://perma.cc/WQM4-S7ED]. Axon was formerly called Taser International, and is attempting to corner the market in police body cameras, along with controlling and analyzing the data the cameras collect. Gelles, *supra* note 59.

228. *See, e.g.*, Brenda Cossman, *Contesting Conservatisms, Family Feuds and the Privatization of Dependency*, 13 AM. U. J. GENDER SOC. POL'Y & L. 415, 416 n.1 (2005) (documenting the dismantling of the Keynesian welfare state). *See also* Ingrid V. Eagly & Joanna C. Schwartz, *Lexipol: The Privatization of Police Policymaking*, 96 TEX. L. REV. 891 (2018) (describing the hidden but significant role of one private company in police policymaking).

229. Brauneis & Goodman, *supra* note 95, at 107.

230. Ann Cammett, *Welfare Queens Redux: Criminalizing Black Mothers in the Age of Neoliberalism*, 25 S. CAL. INTERDISC. L.J. 363, 363–65 (2016) (describing neoliberal goals of privatizing core aspects of the social safety nets such as pensions,

Government contracts associated with developing and implementing algorithmic decision-making tools are highly profitable. The companies selected to privatize Indiana's benefits system, for example, received a billion-dollar contract.[231] While costs vary, child welfare analytics cost states hundreds of thousands of dollars.[232] Companies profit not only from the development of the algorithms, but also from maintaining the data sets the algorithms process.[233] In addition to money, companies that provide data analytics to governments gain access to data they may not have had otherwise.[234]

Given these rewards, it is no surprise that private companies and non-profits are developing algorithmic decision-making technologies and offering them to governments with an eye towards future markets. The child maltreatment algorithm implemented in Allegheny County, first developed for use in New Zealand,[235] is already being marketed to other states.[236] The company that provided aerial surveillance footage to the Baltimore Police

---

education, healthcare, childcare and the prison system). Indiana's former Governor, Mitch Daniels, had what was described as a "Yellow Pages" approach to privatization: if a product or service was offered in the Yellow Pages, government should not provide it. EUBANKS, *supra* note 6, at 45. Mississippi recently passed a law not only requiring its Department of Human Services to develop an automated eligibility and fraud detection system, but mandating that the state use an outside vendor to do so. *See* 2017 MISS. LAWS CH. 421 §3(2)(b)(2).

231. EUBANKS, *supra* note 6, at 48.

232. Jackson & Marx, *supra* note 87 (noting that the Illinois system costed $366,000). The developer of the surveillance flights operated above Baltimore estimated that a long-term contract with a single police department could be worth two million dollars a year. Monte Reel, *Secret Cameras Record Baltimore's Every Move from Above*, BLOOMBERG (Aug. 23, 2016), https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/ [https://perma.cc/9GKZ-VS5C].

233. Axon's (formerly Taser's) contract for five years of data storage with the city of Birmingham, Alabama, is valued at $899,000, not including the one-time costs of the cameras. *See* Joh, *supra* note 58, at 115.

234. Ali Winston, *Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology*, VERGE (Feb. 27, 2018), https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd [https://perma.cc/5ER2-R3FZ] (reporting that New Orleans granted Palantir access to city civil and criminal databases, as well as access to the city's LexisNexis Accurint product, which is comprised of millions of searchable public records, court filings, licenses, addresses, phone numbers, and social media data).

235. *See supra* note 83 and accompanying text.

236. Richard Wexler, Opinion, *The Scarlet Number: Is Pittsburgh's Ethically Risky System of Big Data for Foster Care Coming to California?*, WITNESSLA (Apr. 5, 2018), https://witnessla.com/op-ed-the-scarlet-number-is-pittsburghs-ethically-risky-system-of-big-data-for-foster-care-coming-to-california/ [https://perma.cc/WB75-2W6L] (reporting that the California Department of Social Services has contracted with one of the developers of the Allegheny County AFST tool).

Department is considering using the expertise gained and raw data developed while surveilling the city to market its system to auto insurance companies.[237] Facial recognition software was donated to an Arizona school system with the hope of developing a market for the technology in schools.[238] Amazon designed a facial recognition system that it is currently marketing to various law enforcement agencies.[239]

Using private vendors to build algorithmic social control technologies is problematic for a variety of reasons not the least of which is that it increases opacity and lack of accountability. Not only are government officials, who are implementing the predictive systems, generally unable to explain them,[240] they are often prohibited from providing information because the algorithms and the analysis produced are considered a proprietary secret by third party developers.[241] A recent study directed Freedom of Information Act (FOIA) requests to a variety of state and local agencies as part of a project to test how responsive government agencies would be to requests for information about predictive analytics.[242] While not the

---

237. Kevin Rector, *As Police Weigh Surveillance Program, Private Company at Helm Looks to Court Private Clients*, BALT. SUN (Oct. 7, 2016), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-surveillance-alternatives-20161007-story.html [https://perma.cc/4EPZ-SDRH].

238. *See* Torin Monahan, *The Surveillance Curriculum: Risk Management and Social Control in the Neoliberal School*, *in* SURVEILLANCE AND SECURITY, *supra* note 21, at 110.

239. *See* Matt Cagle & Nicole A. Ozer, *Amazon Teams up with Law Enforcement to Deploy Dangerous New Face Recognition Technology*, ACLU OF N. CAL. (May 22, 2018), https://www.aclunc.org/blog/amazon-teams-law-enforcement-deploy-dangerous-new-face-recognition-technology [https://perma.cc/WYF4-7XDT]; Martin Kaste, *Orlando Police Testing Amazon's Real-Time Facial Recognition*, NAT'L PUB. RADIO (May 22, 2018), https://www.npr.org/2018/05/22/613115969/orlando-police-testing-amazons-real-time-facial-recognition [https://perma.cc/55BG-WHP2].

240. *See supra* notes 41–48 and accompanying text.

241. *See* Hous. Fed'n of Teachers, Local 2415 v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1177 (S.D. Tex. 2017) (private vendor refused to provide algorithm used to terminate teachers, arguing the codes were trade secrets); K.W. v. Armstrong, 180 F. Supp. 3d 703, 717 (D. Idaho 2016) (the state refused to release algorithmic scoring information in Medicaid dispute, claiming vendor copyright protections). Claims that most algorithms contain proprietary information that cannot be released without the permission of the developer are what undercut New York City's attempt to legislate transparency in algorithmic decision-making technologies. Julia Powles, *New York City's Bold, Flawed Attempt to Make Algorithms Accountable*, NEW YORKER (Dec. 20, 2017), https://www.newyorker.com/tech/elements/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable [https://perma.cc/DK2G-TMF5].

242. Brauneis & Goodman, *supra* note 95, at 136 (describing their methodology and listing the systems they sought information on as the Public Safety Assessment,

only obstacle to transparency, the study found that aggressive trade secret claims and NDAs were a major hurdle in obtaining information about the predictive systems.[243] This lack of transparency about the algorithms creates a lack of accountability that implicates all the issues of bias and unfairness inherent in big data analytics.

Finally, privatization of services meant to provide support to recipients has consequences for how we care for others in need, and fundamentally alters the relationship between those delivering services and those receiving them. Privatization of government programs such as welfare and Medicaid is often seen as a way to reduce both the size of government and cut spending on the poor.[244] Contracts often include explicit incentives for outside contractors to cut caseloads, regardless of recipient need.[245] For example, the performance metrics in Indiana's automated benefits system created incentives for the company running the system to close benefits cases prematurely.[246] In addition to churning cases, the company eliminated professional caseworkers and limited human discretion by removing it from frontline service workers, vesting decision-making almost entirely in the computer system.[247] All of this served one purpose — making it as hard as possible to receive any public assistance, regardless of whether one was entitled to it or not.

Governmental deployment of predictive technologies to manage, track, and control marginalized populations is increasing as the tools

---

the Eckerd Rapid Safety Feedback system, the Allegheny Family Screening Tool, PredPol, HunchLab, and the New York City Value-Added Measure).

243. *Id.* at 153–54.

244. *See* Geneva Brown, *Ain't I A Victim? The Intersectionality of Race, Class, and Gender in Domestic Violence and the Courtroom*, 19 CARDOZO J.L. & GENDER 147, 160 (2012) (identifying key components of welfare reform as reduction in expenditures, decrease in government bureaucracy, and increased privatization). *See generally* Wendy A. Bach, *Welfare Reform, Privatization, and Power: Reconfiguring Administrative Law Structures from the Ground Up*, 74 BROOK. L. REV. 275 (2009) (attributing the privatization of benefits systems to shifts in federal law encouraging states to reduce welfare spending and maximize private sector involvement in service provision).

245. Matthew Diller, *Form and Substance in the Privatization of Poverty Programs*, 49 UCLA L. REV. 1739, 1755 (2002) (describing privatization of its public benefits program in which "contractors' profits and losses depended on the amount of money paid out to recipients — the less money for recipients, the more profits for contractors").

246. EUBANKS, *supra* note 6, at 50–51. This is not to say that issues of economics do not skew government analytic systems. Michigan's implementation of the MiDAS system with its 92% error rate increased the Unemployment Insurance Agency coffers from three to sixty-nine million dollars. Charette, *supra* note 47.

247. EUBANKS, *supra* note 6, at 80–81.

themselves are becoming more powerful and opaque. Given the extent of government use of these systems, as well as the historic and economic forces driving their adoption, it is unlikely that communities will be able to completely proscribe their use. However, creative and tenacious advocacy strategies can force governments to become more transparent about how they use predictive systems and require governments to adopt systems that minimize bias and provide for the ability to test and audit the results.

III. TOWARD GOVERNMENT ACCOUNTABILITY

Those grappling with how to diminish the risks associated with big data analytics have offered many solutions, including demands for system transparency,[248] auditing,[249] and required design modifications.[250] It is clear that all these methods and others are needed. At the same time, advocates and activists confronting predictive algorithm systems must become ever more conversant in how they work. Successful challenges must be multi-faceted, relying on litigation and regulation, in addition to being supplemented and guided by grassroots activism. Many of the legal doctrines and strategies used to challenge governmental overreach in the past will be useful guides for opposing current systems. Regulations can create mechanisms for public notice and enforce transparency. However, it is grassroots activism that will sustain the systematic opposition to algorithmic social control systems necessary to limit their use.

A. Litigation

Courts are only beginning to address government use of algorithmic decision-making technologies,[251] although they have been

248. *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 25 (2014) (describing the need for regulators to have access to data sets and source codes).

249. *See* Pauline Kim, *Auditing Algorithms for Discrimination*, 166 U. PA. L. REV. ONLINE 189, 190 (2017) (discussing how auditing system outputs can help determine if protected groups are disproportionally affected).

250. Kroll et al., *supra* note 2, at 662 (arguing that predictive analytics should include software verification technology).

251. *See, e.g.*, Hous. Fed'n of Teachers, Local 2415 v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168 (S.D. Tex. 2017) (noting that use of private algorithms to terminate teachers is an issue of first impression in the circuit); United States v. Esquivel-Rios, 786 F.3d 1299, 1302 (10th Cir. 2015) (noting that the possibility that database unreliability would support a suppression motion in a criminal case is an issue the circuit had not addressed). The goal of this piece is not a complete review of what case law exists, but rather to highlight common arguments and strategies that have been most successful.

grappling with related issues, such as database errors, for many years.[252] Recent decisions reveal a judiciary that is struggling to grasp the technology and is relying on advocates to contextualize system failures within the appropriate constitutional and statutory frameworks, be they criminal or civil.[253] With the rise of predictive policing tools, the concern in the criminal justice arena is that these technologies will further dismantle the protections enshrined in the Fourth Amendment.[254]

Though not addressing predictive policing systems per se, several United States Supreme Court Justices have recently raised privacy concerns based on the aggregated nature of surveillance inherent in big data analytics.[255] This concern crystalized in 2018 in *Carpenter v. United States*.[256] There, the Court found that when police obtained Cell Site Location Information (CSLI) held by wireless carriers, they conducted a search that invaded the defendant's reasonable expectation of privacy, and that required a warrant.[257] In doing so, the Court noted the "seismic shifts in digital technology that made

---

252. *See* Herring v. United States, 555 U.S. 135, 155 (2009) (Ginsburg, J., dissenting) (arguing that the risk of error in criminal justice databases is "not slim" and that "[i]naccuracies in expansive, interconnected collections of electronic information raise grave concerns for individual liberty."); Arizona v. Evans, 5114 U.S. 1, 17 (1995) (O'Connor, J., concurring) ("Surely it would *not* be reasonable for the police to rely, say, on a recordkeeping system, their own or some other agency's, that has no mechanism to ensure its accuracy over time and that routinely leads to false arrests, even years after the probable cause for any such arrest has ceased to exist (if it ever existed)."); *see also* Humphries v. County of Los Angeles, 554 F.3d 1170, 1175 (9th Cir. 2009) (reversed on other grounds) (stating that parents found factually innocent of child abuse were "living every parent's nightmare" because California would not remove them from its child abuse database).

253. *See infra* notes 255–298 and accompanying text.

254. *See, e.g.*, Margaret Hu, *Cybersurveillance Intrusions and an Evolving* Katz *Privacy Test*, 55 AM. CRIM. L. REV. 127 (2018); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2016); *see generally* Elizabeth Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014).

255. *See generally* United States v. Jones, 565 U.S. 400 (2012). In *Jones*, the issue was not one of big data; instead, the case involved police tracking a vehicle for 28 days based on the manual installation of a GPS device. Concurrences by Justices Alito and Sotomayor referenced the need for the court to begin to grapple with how big data technologies may alter reasonable expectations of privacy under the Fourth Amendment.

256. *See generally* Carpenter v. United States, 585 U.S. ___ , *2018 WL 3073916 (2018). This case involved the warrantless collection of cell phone location data over 127 days, creating a small but recognizable subset of the kind of persistent surveillance and data collection that big data analytics and predictive policing technologies rely on.

257. *Id.*

possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years."[258] This decision provides some hope that courts will be hesitant to accept overreaching reliance on algorithmically determined probable cause or reasonable suspicion.

With the advent of predictive policing technologies, some defendants have argued that use of the technology requires a warrant, or is not appropriately encompassed by the existing warrant through which evidence was obtained.[259] Unfortunately, although courts sometimes find that when police use advanced technologies they need warrants, motions to suppress often fail under the good-faith exception to the exclusionary rule.[260] That said, aggressive defense motion practice has forced some prosecutors who wish to keep the use of specific technology secret, to drop certain cases.[261] Defendants have also begun demanding access to the data collected by predictive policing systems, arguing it may contain exonerating information.[262]

---

258. *Id.* at 2219. The big data analytics discussed herein are built on larger databases and use more powerful analytics than the records of cell phone location data at issue in *Carpenter*. *See id.* (explaining that the records at issue reflected the state of technology at the start of the decade and that current technology is even more powerful and precise).

259. *See, e.g.*, State v. Andrews, 134 A.3d 324 (Md. Ct. Spec. App. 2016) (evidence suppressed because police use of cell site simulator did not fall within a pen register trap and trace order); United States v. Werdene, 883 F.3d 204 (3d Cir. 2018) (deciding that a warrant to search computers outside of the issuing magistrate's jurisdiction using a "Network Investigative Device" violated Fourth Amendment, but evidence was nonetheless admitted under a good faith exception to the exclusionary rule).

260. The Fourth Amendment to the United States Constitution generally excludes the use of evidence obtained under an invalid warrant. *See* United States v. Leon, 468 U.S. 897, 906–07 (1984). However, in *Leon*, the Supreme Court created the good faith exception to the exclusionary rule, holding that the suppression of evidence was not appropriate where an officer relied in good faith on a properly issued warrant, even if the warrant was later determined to be invalid. *Id.* at 922.

261. *See* Burlacu, *supra* note 67 (describing how federal prosecutors dismissed charges in a child pornography case rather than disclosing details about the Network Investigative Technique (NIT) used to overcome defendant's use of an IP masking system; *see also* 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/S6DZ-GR9F].

262. Emily Lane, *Mayor, Police Chief to Face Subpoenas from Convicted Gang Member over Palantir Claim*, TIMES-PICAYUNE, NOLA MEDIA (Apr. 3, 2018), https://www.nola.com/crime/2018/04/palantir_new_orleans_mayor_lan.html [https://perma.cc/E5WC-S628] (reporting that defense counsel in New Orleans, which secretly used a predictive policing system, subpoenaed information about the

Criminal justice automated risk assessment systems have been implemented in pre-trial detention, probation, and sentencing contexts for many years. Most of these systems were created for use in probation determinations, but like many technologies, "mission creep" has allowed them to be adapted and used in sentencing.[263] In *State v. Loomis,* the defendant challenged the court's use of an algorithmic risk assessment score to support its sentencing determination.[264] He argued this violated his due process rights on two grounds: that the proprietary nature of the automated system, called COMPAS, prevented him from challenging the system's scientific validity, and that the system unconstitutionally took gender into account.[265]

The Wisconsin Supreme Court ultimately upheld the trial court's use of the technology because it found the COMPAS score was only one of many factors considered during sentencing.[266] However, unlike an earlier challenge to automated sentencing technologies,[267] the Wisconsin court engaged with the critiques of risk assessment tools, including those alleging racial bias.[268] While permitting use of COMPAS, the court required that all future Presentence Investigation Reports contain a written caution about risk assessment

---

system's data collection and analysis, arguing this information could exonerate defendants).

263. Mission or data creep is the repurposing of data analytics beyond its original purpose. This secondary use is extremely problematic because it relies on data not collected or screened for the purpose it is ultimately used for. *See* Matthew T. Bodie et al., *The Law and Policy of People Analytics*, 88 U. COLO. L. REV. 96, 1000–01 (2017); *see also* Wendy K. Mariner, *Mission Creep: Public Health Surveillance and Medical Privacy*, 87 B.U. L. REV. 347 (2007) (describing mission creep in public health surveillance policies).

264. *See* State v. Loomis, 881 N.W.2d 749, 752–53 (Wisc. 2016).

265. *Id.* at 757. COMPAS is a privately-owned risk assessment system designed to provide a numerical score indicating the likelihood that an individual will commit another crime in the future.

266. *Id.* The court made clear that using COMPAS could not be sentence determinative. *Id.* at 767.

267. Malenchik v. State, 928 N.E.2d 564 (Ind. 2010). The defendant in *Malenchik* made a number of arguments, including that the risk assessment tool was unreliable and discriminatory. The court disagreed, citing the "growing body of impressive research" supporting its use. *Id.* at 573.

268. *Loomis*, 881 N.W.2d at 762–63 (referencing Angwin et al., *supra* note 76, as well as its follow-up story, 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/75X8-ZVBS]). The court also discussed a study done by California's Department of Corrections questioning COMPAS. *See id.*

systems, including a warning to judges about the program's lack of transparency and the potential for bias.[269]

The *Loomis* decision is instructive because the court engaged with critiques of algorithmic technology and set limits for its use. The Wisconsin Supreme Court was also clear that it purposefully did not address an equal protection challenge to the system.[270] In addition, one of the concurrences argued that sentencing judges reviewing risk assessment scores should be required to place on the record their evaluations of strengths, weaknesses, and relevance of the scores to the individuals being sentenced.[271] Given that a concurrence, like a dissent, has the capacity to "sow the seeds for future harvest,"[272] the Wisconsin Court's willingness to take seriously challenges to a well-known, long-used risk assessment system is a step in the right direction, even as the ultimate decision permitted the system's use.

Challenges to governmental use of decision-making technology in non-criminal cases are more common. These cases challenge government actions that negatively affect a plaintiff's constitutional[273]

---

269. Per the court's ruling in *Loomis*, the following cautions must be provided to sentencing judges: (1) the proprietary nature of COMPAS has been invoked to prevent disclosure of information relating to how factors are weighed or how risk scores are determined; (2) because COMPAS risk assessment scores are based on group data, they are able to identify groups of high-risk offenders — not a particular high-risk individual; (3) some studies of COMPAS risk assessment scores have raised questions about whether they disproportionately classify minority offenders as having a higher risk of recidivism; (4) a COMPAS risk assessment compares defendants to a national sample, but no cross-validation study for a Wisconsin population has yet been completed; risk assessment tools must be constantly monitored and re-normed for accuracy due to changing populations and subpopulations; (5) COMPAS was not developed for use at sentencing, rather it was intended for use by the Department of Corrections in making determinations regarding treatment, supervision, and parole. *Loomis*, 881 N.W.2d at 769–70 (numbering added for ease of reading).

270. *Id.* at 766 (noting that Loomis did not bring an equal protection challenge, and specifically basing the decision on due process). Several scholars suggest that gender differentials included in risk assessment tools violate equal protection; *see* Sonja B. Starr, *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, 66 STAN. L. REV. 803, 823–30 (2014); John Lightbourne, *Damned Lies & Criminal Sentencing Using Evidence-Based Tools*, 15 DUKE L. & TECH. REV. 327 (2017).

271. *Loomis*, 881 N.W.2d at 774–75 (Abrahamson, J., concurring). Judge Abrahamson also cited the "mixed reviews" that sentencing algorithms have received in scholarly literature and popular commentary. *Id.*

272. William J. Brennan, *In Defense of Dissents*, 37 HASTINGS L.J. 427, 431 (1986).

273. Perdue v. Gargano, 964 N.E.2d 825, 832 (Ind. Sup. Ct. 2012) (entitlement benefits like Medicaid, Food Stamps, TANF, properly characterized as "property" interests within the meaning of the Due Process Clause); Zynda v. Arwood, 175 F. Supp. 3d 791, 807 (E.D. Mich. 2016) (questionnaire used to determine whether unemployment claimants committed fraud violates the Fifth Amendment's privilege against self-incrimination).

or statutory rights.[274] Most of the cases discussed herein involve two kinds of instances: when the state uses algorithmic decision-making systems to terminate the employment of public school teachers, and when it relies on such technologies to reduce or discontinue a recipient's public benefits such as welfare, Medicaid, or unemployment benefits.

Because these cases involve a property right, plaintiffs have been most successful with procedural due process claims arising under the Fourteenth Amendment.[275] These cases are often characterized as "notice" claims, and the notice requirements prior to termination are fairly substantial. Proper notice requires an opportunity to be heard at a meaningful time and in a meaningful manner,[276] and it must adequately detail the reasons for termination or reduction of rights.[277] In *Houston Federation of Teachers v. Houston Independent School District,* the court found that the School District failed to provide enough information about the algorithm used to terminate teachers, even though it provided significant general, as well as some specific, system details.[278] The court held that what was given was not sufficient to satisfy procedural due process because the information did not allow individual teachers to verify or replicate their scores.[279]

---

274. *Perdue*, 964 N.E.2d at 829 (considering Americans with Disabilities and Rehabilitation Act claims); K.W. v. Armstrong, 180 F. Supp. 3d 703, 706 (D. Idaho 2016) (bringing claims under Medicaid Act); *see generally* State of New Mexico *ex rel.* Stewart v. N.M. Pub. Educ. Dep't, D-101-CV-2015-00409, at 24–27 (Santa Fe County Ct. Dec. 2, 2015) (stating that claim hinges entirely on New Mexico state law).

275. Hous. Fed'n of Teachers, Local 2415 v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1175 (S.D. Tex. 2017).

276. Mathews v. Eldridge, 424 U.S. 319, 333 (1976). *Mathews* also established a balancing test to determine the level of protections a particular situation demands: courts must consider the private interests that will be affected, the risk of erroneous deprivation and probable value of additional safeguards, and the governmental interest (including fiscal and administrative burdens) that additional or substitute procedural requirements would entail. *Id.* at 335.

277. Goldberg v. Kelly, 397 U.S. 254, 267–68 (1970).

278. The district provided an overview of the general measurements — a general description of the testing methodology, how to read the teacher assessment report, a list of students whose scores were linked to the teacher and used in the scoring, and the percentage of those students the individual teacher was responsible for. *Hous. Fed'n of Teachers*, 251 F. Supp. 3d at 1178. In a similar decision, the Indiana court in *Perdue* found that generalized information connected to numerical codes used to explain an adverse action failed to provide any information as to how the decision was reached, and thus was constitutionally inadequate. *Perdue*, 964 N.E.2d at 835–36.

279. *Hous. Fed'n of Teachers*, 251 F. Supp. 3d at 1179.

Procedural due process also requires clear ascertainable standards to insure fairness and avoid arbitrary decision making.[280] In *K.W. v. Armstrong*, plaintiffs sought detailed information of the State's new algorithmic process of determining eligibility for Medicaid.[281] The state refused to provide the information in part because it was copyrighted by a third party.[282] The court found that potential for error in the system was "obvious" and "substantial."[283] Then, applying the balancing test dictated by the Supreme Court in *Mathews v. Eldridge*,[284] the court held that the risk of erroneous denial of benefits outweighed any potential harm to the third party, and thus found a due process violation.[285]

Substantive due process and equal protection challenges to algorithmic technologies have fared less well.[286] Both of these challenges only require the state to show that it has a rational basis for its determination, unless the plaintiff is a member of a protected class or can show that the state is infringing on a fundamental right.[287] The rational basis standard is very deferential to the state, and is rarely met by the plaintiff.[288] However, in a case arising from the "robo-fraud" system utilized by the Michigan Unemployment

---

280. *Armstrong*, 180 F. Supp. 3d at 715 (citing Carey v. Quern, 588 F.2d 230 (7th Cir. 1978)).

281. *Id.* (requiring the state to draft clear standards of the terms used to terminate or reduce benefits).

282. *Id.* at 717.

283. *Id.* at 716–17. The court walked through the steps required to implement the "budgetary tool" and noted the multiple places for potential error, both procedurally (transferring information from various pages of a questionnaire) and substantively (misunderstanding a participant's ability to accomplish a specific task). *Id.*

284. Mathews v. Eldridge, 424 U.S. 319, 334 (1976).

285. *Armstrong*, 180 F. Supp. 3d at 716–17 (finding substantial risk of "mathematical, clerical, or substantive" error). The court also noted that any risk of harm to the company could be substantially or entirely mitigated by a protective order. *Id.*; *see also* Order, Jacobs v. Gillespie, 3:16-cv-119-DPM (E.D. Ark. Nov. 1, 2016) (ordering that state health benefits may not be reduced until the agency provides specific notices explaining benefit reduction, referencing and including a copy of the assessment algorithm).

286. Cook v. Bennett, 792 F.3d 1294, 1300 (11th Cir. 2015) (deciding that a substantive due process and equal protection challenge to a teacher assessment system, which evaluated teachers based on the test scores of students they did not teach or even in subjects they did not teach, passes rational basis).

287. *Id.* at 1300–01.

288. *See* Hous. Fed'n of Teachers, Local 2415 v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1180–83 (S.D. Tex. 2017) (describing several cases where plaintiffs failed in challenging teacher assessment systems because the system passed rational basis review).

Agency, the equal protection claim survived a motion to dismiss.[289] There, the court found that because the system was not uniformly applied and continued to operate after problems were identified, the plaintiffs met their burden of showing intentional and arbitrary disparate treatment of similarly situated people, which was "devoid of any rational basis."[290]

Most of the cases challenging the use of automated decision-making tools also claim the systems suffer from statutory deficiencies, alongside the previously discussed constitutional challenges. The statutes are often relied upon because they contain notice and hearing requirements similar to those protected by procedural due process.[291] Unlike procedural due process, however, statutes, especially those written to implement specific types of assessment frameworks, may include language requiring any state assessment system (including algorithmic decision-making systems) to be transparent and objective.[292] This is most evident in the recent trend of states adopting Value Added Model (VAM) algorithms to determine teacher competency.[293] At least two states that have implemented teacher assessment systems included transparency and objectivity requirements in their statutes.[294]

---

289. Cahoo v. SAS Inst. Inc., 322 F. Supp. 3d 772, 800–02 (E.D. Mich. Mar. 2, 2018).

290. *Id.* at 801.

291. *See, e.g.*, K.W. v. Armstrong, 789 F.3d 962, 970 (9th Cir. 2015) (describing the notice and hearing requirements of the Medicaid Act and regulations).

292. *See* Lederman v. King, 47 N.Y.S.3d 838, 844 (N.Y. Sup. Ct. 2016) (referencing statutory requirement that the teacher assessment system must be transparent and available to those being rated prior to the school year); State of New Mexico *ex rel.* Stewart v. N.M. Pub. Educ. Dep't, D-101-CV-2015-00409, at 24–27 (Santa Fe County Ct. Dec. 2, 2015) (noting the statutory requirement that the teacher assessment system must be objective and uniform statewide). In a case from Idaho, plaintiff challenged the disability needs assessment algorithm by (in part) citing language from 42 U.S.C. § 1396n(j)(5)(D) of the Medicaid Act, which requires that a patient's medical assessment plan methodology use valid, reliable cost data, and be open to public inspection. *See* Plaintiff's Amended Consolidated Class Action Complaint at ¶ 36, K.W. v. Armstrong, 1:12-cv-00022-BLW (E. Idaho July 24, 2014) (on file with author).

293. Brauneis & Goodman, *supra* note 95, at 150–51. Algorithmic teacher assessment systems are fairly recent, and are highly complex systems that assign a score to teachers that allegedly represents the impact or "value added" an individual teacher had on student learning. *See* Regina Umpstead et al., *The New State of Teacher Evaluation and Employment Laws: An Analysis of Legal Actions and Trends*, 322 ED. L. REP. 577, 584–87 (2015).

294. *See generally* N.Y. EDUC. LAW § 3012-c(j)(1) (McKinney 2018) (governing teacher assessment and requiring that the "process by which points are assigned in subcomponents and the scoring ranges for the subcomponents must be transparent and available to those being rated before the beginning of each school year"); N.M.

In *Lederman v. King*, the court found that the teacher challenging New York's VAM assessment system was able to establish that the implementation of the value added model was arbitrary and capricious.[295] While the court focused on the biases and statistical shortcomings of the system,[296] it also noted expert testimony indicating that the system lacked the required transparency for the petitioner to understand what she needed to do to achieve a satisfactory assessment score as required by state law.[297] Similarly, a New Mexico judge issued a preliminary injunction halting the implementation of a teacher assessment system in New Mexico, finding it was not transparent and was not applied uniformly across school districts as required by state law.[298]

In addition, while not a challenge to the technology itself, disabled plaintiffs have successfully used federal disability rights laws to oppose state requirements that impede their ability to interact with automated benefits systems.[299] As states continue to reduce the number of individual caseworkers, recipients are increasingly expected to engage directly with the technologies evaluating them. Thus, federal and state disability protections may become an increasingly important route by which to challenge these automated systems.

Beyond illuminating legal bases for challenging automated decision-making systems, recent cases also highlight various practical strategies. The first and most obvious is the need to educate oneself and the judiciary as thoroughly as possible on all aspects of the technology in question. For this, experts are required. *Loomis* is indicative of the importance of educating judges. As the concurrence pointed out, "this court's lack of understanding of COMPAS was a

---

STAT. ANN § 22-10A-19 (West 2018) (requiring that the education department "adopt criteria and minimum highly objective uniform statewide standards").

295. Lederman v. King, 47 N.Y.S.3d 838, 847 (N.Y. Sup. Ct. 2016).

296. The New York court found that the VAM algorithm was biased against teachers with either high or low performing students, was disproportionately affected by class size, and that the state could not account for the wide year to year swings in teacher scoring. *Lederman*, 47 N.Y.S.3d at 846.

297. *Id.* at 845 (referencing testimony that New York's system failed to provide the information required by New York Education Law).

298. State of New Mexico *ex rel.* Stewart v. N.M. Pub. Educ. Dep't, D-101-CV-2015-00409, at 24–27 (Santa Fe County Ct. Dec. 2, 2015). New Mexico law requires objective and uniform standards for teacher assessment. N.M. STAT. ANN. § 22-10A-19 (West 2018).

299. *See* Perdue v. Gargano, 964 N.E.2d 825, 832, 843–44 (Ind. Sup. Ct. 2012) (finding violations of Americans with Disabilities Act and Rehabilitation Act, where the state provided only telephone interview to deaf plaintiff).

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."[300]

Algorithmic decision-making systems are inherently complex. Many of the opinions discussed here rely heavily on the testimony of plaintiff's experts and their descriptions of the problems with the technology.[301] Because the systems are often seen as infallible, and because the state may refuse to admit system failures, experts are crucial to finding and explaining system errors. In addition, disputes between plaintiff's and defendant's experts can create a genuine issue of material fact, which will allow the plaintiffs to overcome motions for summary judgment.[302]

Expertise is also essential to reveal data errors. Courts assume that government databases are accurate and reliable, which increases the likelihood that they will defer to the analytics that mine these databases.[303] Systematic demonstration of data error is key to convincing courts to review data analytics with a more critical eye.[304] In the challenge to Idaho's algorithmically controlled disability determination, the court, after discussing the large number of data errors the plaintiff was able to establish, held that "a substantial number of *known* errors signals two things: (1) the existence of substantial *unknown* errors; and (2) a lack of quality control."[305]

---

300. State v. Loomis, 881 N.W.2d 749, 774 (Wisc. 2016). The concurrence objected to the denial of the request by the developer of COMPAS to file an amicus brief, which underscores the necessity for those challenging automated systems to have their own experts and amici supporting their positions.

301. *See, e.g.*, *Lederman*, 47 N.Y.S.3d at 896 (in finding that the state's use of an algorithm was arbitrary and capricious, the court explicitly referenced plaintiff's experts); Hous. Fed'n of Teachers, Local 2415 v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1177 (S.D. Tex. 2017) (plaintiff's expert was unable to replicate scoring); *Stewart*, D-101-CV-2015-00409, at 24–28 (citing expert testimony about data errors, missing data, and scoring abnormalities).

302. *See* K.W. v. Armstrong, 180 F. Supp. 3d 703, 718 (D. Idaho 2016) (deciding that a dispute between experts as to the unreliability of a budgeting algorithm makes summary judgment inappropriate).

303. *See* Logan & Ferguson, *supra* note 135, at 543; Erin Murphy, *Databases, Doctrine, and Constitutional Criminal Procedure*, 37 FORDHAM URB. L.J. 803, 823–24 (noting that the presumption of regularity means that absent affirmative evidence to the contrary, courts will assume the soundness of the information generated).

304. *See* Logan & Ferguson, *supra* note 135, at 608–09 (suggesting that courts could adopt the position that unaccredited databases lose the presumption of reliability).

305. *Armstrong*, 180 F. Supp. 3d at 711. The court also noted that sixty-six percent of original training data had to be discarded because of data error and that the state failed to audit the system after implementation even though it knew the extent of the data error. *Id.*; *see also* Hous. Fed'n of Teachers, 251 F. Supp. 3d at 1177 (providing a

Advocates should also aggressively challenge claims that information about the technology cannot be released because it is proprietary, protected by a NDA, or is otherwise privileged. While some courts have refused to require third parties to reveal proprietary information,[306] several others have made it clear that such claims are outweighed by a plaintiff's due process rights.[307] As one court stated, a private company's "trade secrets do not empower, much less compel," a government agency "to violate the constitutional rights of its employees."[308] The court importantly went on to state: "When a public agency adopts a policy of making high stakes employment decisions based on secret algorithms incompatible with minimum due process, the proper remedy is to overturn the policy, while leaving the trade secrets intact."[309]

Advocates would also do well to leverage language indicating judicial concern about algorithmic decision-making systems in general. Given how new, complex, nontransparent, and potentially harmful predictive algorithms are, courts have been willing to look beyond their own jurisdiction for guidance. In the challenge to New Mexico's teacher assessment system, the State, seeking a dismissal, cited a number of cases from other jurisdictions that had upheld similar systems on equal protection and substantive due process grounds.[310] The New Mexico court noted that the challenge at bar was explicitly based on a state statute.[311] The court then used dicta from several of the opinions the state had cited to find that while

---

myriad of reasons why algorithmic scores might be erroneously calculated, and notes further that even when mistakes are found, that they will not be promptly corrected); State of New Mexico *ex rel.* Stewart v. N.M. Pub. Educ. Dep't, D-101-CV-2015-00409, at 24–27 (Santa Fe County Ct. Dec. 2, 2015) (listing errors in the data the algorithm was analyzing).

306. *See generally* State v. Loomis, 881 N.W.2d 749 (Wisc. 2016). In *Loomis* the defendant argued that he was denied the information the sentencing court relied on because the developer of the algorithmic scoring system considered the information proprietary and would not release it. *Id.* at 761. The court found that because the defendant had access to the questions and defendant's answers to the algorithm evaluated, the defendant had enough of the information. The court did require that going forward trial court judges must be told that the proprietary nature of COMPAS prevents disclosure of how factors are weighed and risk scores determined for both courts and defendants even as the questions and answers the system assesses are released. *Id.* at 769–70.

307. *See, e.g.*, *Armstrong*, 180 F. Supp. 3d at 717–18. The court also noted that any harm to the third party could be mitigated with protective orders. *Id.* at 718.

308. *Hous. Fed'n of Teachers*, 251 F. Supp. 3d at 1179.

309. *Id.*

310. *Stewart*, D-101-CV-2015-00409, at 15–16.

311. *Id.* at 17.

those systems may have passed the low bar of constitutional rational basis review, courts viewed those systems as untested, unfair, and problematic.[312] Even in *Loomis*, which upheld use of the assessment tool in Wisconsin, the court provided cautionary language and restrictions that can be used by advocates challenging other algorithmic assessment systems.[313]

However, confronting the many issues raised by governmental use of predictive analytics likely exceeds the capacity of litigation based on current legal doctrines and statutes. Addressing the potential injustices of predictive algorithms can involve pursuing the hard work of legal reform.[314] The language and spirit of well drafted statutes, regulations, and ordinances can provide legal advocates and grassroots activists with the tools to challenge these powerful but fallible systems.

B. Regulation

Regulation,[315] through local ordinances or state statutes, can go far in addressing the lack of transparency that results from government secrecy or third-party claims of proprietary protections. Regulations can also provide mechanisms to challenge database errors, and can require much needed algorithmic testing and auditing. Law not only guides government agencies, it provides a foothold for litigation to keep those agencies in check. While marginalized populations will always be targets of state authority, public policy, including rule-

---

312. *Id.* at 16–17 ("Needless to say, this Court would be hard-pressed to find anyone who would find this evaluation system fair to non-FCAT teachers, let alone be willing to submit to a similar evaluation system." (internal citations omitted)).

313. *See supra* note 269 and accompanying text (describing the holding in State v. Loomis, 881 N.W.2d 749 (Wis. 2016)).

314. Frank Pasquale & Danielle Keats Citron, *Promoting Innovation While Preventing Discrimination: Policy Goals for the Scored Society*, 89 WASH. L. REV. 1413, 1413 (2014).

315. A comprehensive discussion of the myriad of regulations potentially applicable to governmental algorithmic decision making is far beyond the scope of this Article. For example, overarching national legislation similar to the European Union's General Data Protection Regulation (GDPR) could address many of the issues discussed in Part II. *See generally* Francoise Gilbert et al., *Corporate Governance in Insurance: The EU General Data Protection Regulation and Its Implications for United States Companies*, GREENBERGTRAURIG (Aug. 3, 2018), https://www.gtlaw.com/en/insights/2018/12/published-articles/the-eu-general-data-protection-regulation-and-its-implications-for-united-states-companies [https://perma.cc/43J2-TPGW] (providing a brief overview of the GDPR). However, in the current political climate, national legislation regulating use of big data analytics seems unlikely.

making in its broadest sense, can shape and shift the balance of power in civil society.[316]

Technologies that remain secret are unchallengeable. To combat this secrecy, communities are beginning to pass local ordinances that require law enforcement to provide notice to local legislators and the community before acquiring and deploying new surveillance technologies.[317] These ordinances require such notice regardless of whether the systems are purchased, provided by grants, or even gifted to an agency free of charge.[318] Unfortunately, without careful monitoring, governments may attempt to side-step regulations meant to ensure transparency and public access.[319]

Ordinances can also require agencies to provide annual reports about the technologies being deployed or considered by law enforcement.[320] Additionally, ordinances can provide more formal mechanisms for public input. One ordinance, passed in Oakland, California, went beyond requiring community notification — it created standing oversight committees to address police surveillance and technology, with some seats reserved for members of the public.[321] Such laws are critical not only because they mandate notice and input, but also because they provide structures that facilitate community engagement.[322]

---

316. *See* K. Sabeel Rahman, *Policy Making as Power-Building*, 27 S. CAL. INTERDISC. L.J. 315, 318 (2018).

317. *See* Crump, *supra* note 65, at 1605 (discussing local procurement ordinances in Seattle, San Diego and Oakland); Joh, *supra* note 58, at 127 (observing that Santa Clara County became the first county in the nation to require government approval prior to engaging new surveillance tools).

318. *See, e.g.*, Crump, *supra* note 65, at 1614 (noting that Seattle's procurement ordinance requires that any city department obtain City Council approval prior to acquiring surveillance technology and again prior to deployment).

319. Seattle's police department secretly purchased technology to create a database of social media postings in contravention of Seattle's surveillance ordinance. *See* Ansel Herz, *How the Seattle Police Secretly—and Illegally—Purchased a Tool for Tracking Your Social Media Posts*, STRANGER (Sept. 28, 2016) https://www.thestranger.com/news/2016/09/28/24585899/how-the-seattle-police-secretlyand-illegallypurchased-a-tool-for-tracking-your-social-media-posts [https://perma.cc/C3WH-XEFE].

320. THE RISE OF BIG DATA POLICING, *supra* note 6, at 188.

321. *See* Crump, *supra* note 65, at 1626.

322. These are similar to the structures provided by consent decrees. *See* Sunita Patel, *Toward Democratic Police Reform: A Vision for "Community Engagement" Provisions in DOJ Consent Decrees*, 51 WAKE FOREST L. REV. 793, 796 (2016) (noting that structures created by consent decrees requiring public input have increased transparency of and oversight over local law enforcement).

Regulations aimed at increasing local law enforcement transparency arose because police were purchasing and implementing predictive systems in secret.[323] Laws mandating transparency in public purchasing already bind state agencies that oversee public benefits programs.[324] Thus, the problem with automated public benefits systems is not that they are purchased in secret, it is that the systems themselves are opaque, the data sets contain errors and bias, and error rates are hidden from the public.[325] This lack of transparency is often aggravated by contractual NDAs or claims that the information is proprietary.[326]

The intermingling of public, private, and law enforcement data into large data sets makes assessing the data for accuracy and completeness difficult. However, there are existing statutes and regulatory structures that could provide a framework for individuals to inspect and correct inaccurate data.[327] The federal Fair Credit Reporting Act (FCRA),[328] for example, provides consumers with the right to inspect and challenge their credit records for data error.[329] Similarly, the federal government has data control requirements, including expungement of overturned convictions, for large unwieldy databases like the combined DNA profile database.[330] There is also

---

323. Crump, *supra* note 65, at 1604–05 (describing case studies suggesting that police departments often acquire surveillance technologies without participation by elected officials or the community); *see also supra* notes 61–68 and accompanying text (providing examples of how police departments have concealed predictive policing systems).

324. *See, e.g.*, Brauneis & Goodman, *supra* note 95, at 109–10 (indicating that most states have public records laws mandating disclosure of contracts with third-party vendors); Natalie Gomez-Velez, *Proactive Procurement: Using New York City's Procurement Rules to Foster Positive Human Services Policies and Serve Public Goals*, 9 CUNY L. REV. 331, 350–51 (2006) (describing New York City's procurement rules, which require open, competitive bidding, as applying to contracts for the provision of social services).

325. *See supra* Part I.

326. *See supra* notes 241–43 and accompanying text.

327. *See* Citron & Pasquale, *supra* note 248, at 20–21 (arguing that the private use of algorithmic scoring requires that once firms have gathered data on more than 2000 individuals, those individuals should have the same rights to inspect, correct, and dispute inaccurate data as those provided by the federal Fair Credit Reporting Act).

328. 15 U.S.C. § 1561 *et seq.*

329. Citron & Pasquale, *supra* note 248, at 16. This is not to say the FCRA system works well; indeed, it has been described as a "kafkaesque no man's land that, more often than not, fails to resolve the problem." Madden et al., *supra* note 29, at 87.

330. Logan & Ferguson, *supra* note 135, at 551, 600 (suggesting that while the statutes require systematic data correction for all agencies that access CODIS, a comprehensive DNA profile database accessible by all levels of law enforcement, the FBI (which manages the database) has been lacking in its upkeep of data quality).

the federal e-verify system, which is used to police who may or may not legally work.[331] This system has been plagued with data errors that raise real barriers to employment.[332] But e-verify does have an online self-check system, which allows for some ability to challenge data errors.[333] While none of these systems work exceedingly well, each provides some process for addressing and potentially correcting data error — they can serve as guides for legislation that will address errors in other types of data sets.

Regulating agency contract requirements can also increase system transparency by limiting third-party NDAs or claims that the technology is proprietary. When jurisdictions demand fewer and narrower NDAs, third-party vendors often comply.[334] In addition, regulations that govern contracts for algorithmic decision-making technologies can mandate that all the results from validation testing conducted prior to implementation be made public, and, more importantly, that post-implementation testing and auditing be made public as well.[335] Support for these transparency and accuracy requirements comes not only from case law, but also from statutes governing the doctrinal areas these systems function within.[336]

Attempts to regulate and limit government use of algorithmic decision-making technologies will not be easy. Litigation and law reform, while critical to minimizing the harm these tools can cause, are not standalone solutions. Both rely on community activism and long-term grassroots organizing to be effective.

---

331. *See About E-Verify*, https://www.e-verify.gov [https://perma.cc/ZE9Q-FKCP] (describing E-verify as a web-based system that allows enrolled employers to confirm the eligibility of their employees to work in the United States).

332. Hu, *supra* note 156, at 1778.

333. *Id.* at 1764–66.

334. Brauneis & Goodman, *supra* note 95, at 164–66 (discussing successful usage of contract language to limit trade secret and NDA claims).

335. *Id.* These requirements will increase costs but will also minimize adoption of error prone systems and the litigation that follows. The need for testing and the implications of systemic system failure is not unnoticed by courts. *See* K.W. v. Armstrong, 180 F. Supp. 3d 703, 714 (D. Idaho 2016) (noting that given the failure rates of the system, a premium should have been put on testing it in the first place); Zynda v. Arwood, 175 F. Supp. 3d 791, 806 (E.D. Mich. 2016) (concluding that the high error rate in an unemployment fraud detection system supports standing for legal services office).

336. *See supra* note 292–94 and accompanying text (discussing statutes requiring assessment systems be valid, transparent, and objective).

C. Activism and Organizing

Social control algorithms are impoverished and impoverishing. Challenging them requires an engaged community knowledgeable about their fallibility and willing to establish coalitions to confront them. Most importantly, it requires expanding the current focus on law enforcement technologies to include all of the systems used to control and punish people. Governmental deployment of data analytics to manage marginalized populations is a political decision, albeit one that reframes large political questions as "mundane issues of efficiency and systems engineering."[337] Confronting such dangerous politics requires prolonged and aggressive advocacy.

Some see government use of algorithmic social control tools as a *fait accompli* and focus on how to cabin and tweak the technology to minimize its harm.[338] Others call for more aggressive tactics, folding challenges to governmental use of algorithmic decision-making into a larger fight for social justice.[339] As they are used today, predictive technologies are destructive not only to individuals, but also to the very concepts of equality and justice. Additionally, once these technologies become acceptable as tools to manage any one population, it will be much harder to challenge its use to control others. As in any battle for civil rights and equity, a wide range of approaches and tactics will be necessary. However, given the complexity of predictive analytics, thorough community education is a critical first step.

Education is central in large part because predictive algorithm systems have flourished in secret, which has allowed their use to go undetected and unchallenged for extended periods of time. The more communities and advocates understand predictive algorithm systems and how they are used, the easier it will be to identify when they are deployed. The more people learn about the fallibilities inherent in predictive analytics — the biases, feedback loops, erroneous data, and unchecked, undemocratic power hidden within them — the easier it will be to challenge unquestioning societal acceptance of predictive

337. EUBANKS, *supra* note 6, at 197. Governmental use of the social control technology can be seen as political because it reflects a choice of where to focus public resources and because purchasing tools specifically designed to control unpopular groups furthers a particularly neoliberal politic.

338. THE RISE OF BIG DATA POLICING, *supra* note 6, at 6, 187–88.

339. EUBANKS, *supra* note 6, at 204–05.

technologies. Community education is also necessary to maintain what is bound to be an ongoing, long-term battle.[340]

Education can also support calls to repurpose predictive systems. Instead of being used to target and control, the technology could be used to help and uplift vulnerable populations. Big data analytics can be used to identify risks to a community, but instead of addressing those risks through law enforcement, other social service systems could be employed.[341] Similarly, predictive technology could be used to ensure that the poor and families in distress receive all the benefits to which they are entitled.[342] These systems can also be repurposed to strengthen judicial oversight of warrant requests,[343] or to identify police officers with poor decision-making skills so they can go through additional training.[344] Thus, education is key to creating the necessary narratives to challenge how, and for what purpose, governments use predictive analytics.

This is not a new fight — there have already been many successes,[345] and organizing and advocacy is ongoing.[346] However,

---

340. *See* Crump, *supra* note 65, at 1628–29 (noting that the success of Oakland's citizen task force requires high levels of community involvement, which is supported by Oakland's long tradition of activism — indeed, communities without that history may have difficulty sustaining similar levels of input and engagement).

341. THE RISE OF BIG DATA POLICING, *supra* note 6, at 170–71 (discussing how systems could augment a public health approach to social ills by decoupling risk identification from a policing solution).

342. EUBANKS, *supra* note 6, at 81–82.

343. Andrew Manual Crespo, *Systemic Facts: Toward Institutional Awareness in Criminal Courts*, 129 HARV. L. REV. 2049, 2074–76 (2016) (describing the capacity of algorithms to help courts identify, track and assess the accuracy of the probable cause scripts used to support warrant requests).

344. Studies show that applying predictive analytics to internal police data can identify which officers are more likely to make bad decisions or have inappropriate use of force complaints made against them. *See* THE RISE OF BIG DATA POLICING, *supra* note 6, at 147–48.

345. *See, e.g.*, EUBANKS, *supra* note 6, at 64–72 (arguing that grassroots organizing is key to stopping attempts at privatizing benefits systems); *see also* Michele Gilman & Rebecca Green, *The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization*, 42 N.Y.U. REV. L. & SOC. CHANGE 253, 303–04 (2018) (describing how Seattle's homeless population successfully fought the city's mandatory data collection program).

346. One example of ongoing advocacy is the Stop LA Spying Coalition, which provides community outreach and joins legal challenges to stop predictive policing campaigns in Los Angeles and elsewhere. *About Us*, STOP LAPD SPYING COAL., https://stoplapdspying.org/about-slsc/ [https://perma.cc/DKT6-WV34]. Another example is Our Data Bodies: Human Rights and Data Justice, which works with local communities to show how different data systems impact reentry, fair housing, public assistance, and community development. *See Our Data Bodies: Human Rights and*

most of the current organizing is framed as a civil liberties issue, focusing on surveillance and predictive policing technologies.[347] This is worrisome, as it allows other governmental use of these systems to escape scrutiny. It is critical for advocates to realize that predictive technologies used by government share a commonality of consequences,[348] that they target the same populations regardless of which agencies are involved. State violence against marginalized populations is not just police violence, it is the violence of being policed and controlled by opaque and unchallengeable tools, regardless of the context.

While organizing is never easy, especially across race and class,[349] the technology itself is conducive to the creation of broad alliances. The analytics and databases used in predictive policing are similar to those used to target and control Medicaid recipients or families mired in the child welfare system. The predictive analytics used to assess eligibility for unemployment are similar to those used to asses teacher competency. The problems with predictive technologies, including failure rates, biased feedback loops, data errors, and lack of transparency, are all the same. Organizing around the similarities of the systems that governments use to control and manage people can strengthen and speed coalition building.

Readers, especially those from a legal background, may avoid consciously engaging with calls for social justice organizing. Many within the legal system tend to rely on legal strategies and the drafting of laws and regulations to address social concerns. However, Eubanks's description of how these systems create and maintain a digital poorhouse should cause all of us to stop and realize that

---

Data Justice, ODB PROJECT, https://www.odbproject.org [https://perma.cc/EM9Q-P8PU].

347. *See, e.g.*, ACLU COMMUNITY CONTROL OVER POLICE SURVEILLANCE (CCOPS) MODEL BILL, ACLU, https://www.aclu.org/files/communitycontrol/ACLU-Local-Surveillance-Technology-Model-City-Council-Bill-January-2017.pdf [https://perma.cc/GKN5-L7UK] (providing a model act to "Promote Transparency and Protect Civil Rights and Civil Liberties with Respect to Surveillance Technologies"). While the model act has a broad definition of "surveillance technology," which includes "software designed to integrate or analyze data from Surveillance Technology," it is unlikely it would encompass the types of algorithmic decision-making systems used to assess and regulate public benefits or sentencing algorithms. *Id.* § 12(E)(1)(q).

348. Hu, *supra* note 156, at 1740.

349. *See* EUBANKS, *supra* note 6, at 216. Pointing out the "deep classism" of many progressive organizations that inhibits coalition building, which actually results in progress for the poor.

surveillance and data collection, which is now used to police the poor, will be turned on others once it is perfected:

> Think of the digital poorhouse as an invisible spider web woven of fiber optic strands. Each strand functions as a microphone, a camera, a fingerprint scanner, a GPS tracker, and alarm trip wire, and a crystal ball. Some of the strands are sticky. They are interconnected, creating a network that moves petabytes of data. Our movements vibrate the web, disclosing our location and direction. Each of those filaments can be switched on or off. They reach back in history and forward into the future. They connect us in a network of association to those we know and love. As you go down the socioeconomic scale, the strands are woven more densely and more of them are switched on.[350]

Clearly, we are not individually in charge of the systems that create this web and cannot easily switch the strands on or off. Because the criminal justice and social welfare systems are fused, to successfully challenge the use of advanced technologies in one arena requires challenging them in all arenas. This means that advocates must organize around issues of poverty and disability as well as surveillance and predictive policing. Dismantling any part of the digital poorhouse means asking not just whether the technology will increase surveillance by the state or displace probable cause — it means asking why we have a digital poorhouse in the first place.

CONCLUSION

We live in a country where marginalized populations are seen as problematic, a people to be contained and controlled rather than as equal citizens. We also live with a justice system that has historically been used to police race and poverty. These historic patterns are being re-codified in a technological redlining that reinforces oppressive social relationships and enacts new models of profiling and policing.[351] Misguided government reliance on flawed algorithms as social control mechanisms endangers vulnerable populations and impoverishes our country.

As our legal system becomes ever more intertwined in big data analytics, advocates must learn to recognize the harms caused by these technologies and think creatively about how to oppose them. Challenging governmental deployment of social control technologies will require melding social activism with pragmatic legal and

---

350. EUBANKS, *supra* note 6, at 188–89.
351. *See* NOBLE, *supra* note 7, at 1.

legislative advocacy. Only then will we be able to untangle our clients, ourselves, and ultimately our democracy from their grasp.