2020

Constitutional Rights in the Machine Learning State

Aziz Z. Huq

Constitutional Rights in the Machine Learning State

Aziz Z. Huq†

Abstract

A new class of "machine learning" tools is able to make better predictions and inferences from data than was previously feasible. For the state, machine learning is a powerful and supple device to reveal citizens' beliefs, actions, and expected behaviors. Its deployment to allocate investigative resources, material benefits, and coercive penalties to particular individuals, though, can implicate due process, privacy, and equality interests. Substantive doctrinal frameworks and enforcement regimes for those entitlements, however, arose in the context of human action. Neither is apt for a machine learning context. This Article offers a start to the larger project of developing a more general account of substantive rules and enforcement mechanisms to promote due process, privacy, and equality norms in the machine learning state. After cataloging notable state and municipal adoptions of machine learning tools, it considers how existing constitutional norms can be recalibrated (in the case of due process and equality) or retooled (in the case of privacy). It further reexamines the enforcement regime for constitutional interests. Today, constitutional rights are (largely) enforced through discrete, individual legal actions. Machine learning's normative implications arise from systemic design choices. The retail enforcement mechanisms that currently dominate the constitutional remedies context are therefore particularly inapt. Instead, a careful mix of ex ante regulation and ex post aggregate litigation, which are necessary complements, is more desirable.

† Frank and Bernice J. Greenberg Professor of Law, University of Chicago Law School. Thanks for Sharad Goel and Ravi Shroff for many helpful comments and critical conversations. The Frank J. Cicero Fund provided support for this research, All errors are mine.

Table of Contents

Constitutional Rights in the Machine Learning State

Introduction

A deep skepticism of the state lies at the heart of American constitutionalism.[1] Aspiring toward government under the rule of law, constitutionalism aims to tame the state's risks to individual entitlements even as it enables contributions to the public good. Technology mediates this trade-off.[2] The state's power to shape the lives of its citizens, whether for good or ill, has always been a function of the instruments at its disposal.[3] Today, one technology transforming how the state acts is a class of computational tools called "machine learning." These instruments derive predictions and inferences in new ways, often exploiting pools of otherwise largely opaque data.[4] Many encounter machine-learning tools first in the marketplace. Facebook, for example, uses them to determine what clickbait tempts best, Amazon to predict what products you'll likely purchase.[5] In state hands, however, machine-learning tools do more than recommend dietary supplements or fashion accessories. Rather, they can exploit previously low-value data—*e.g.*, administrative records, criminal justice records, or public surveillance footage—to generate startling insight into citizens' beliefs, actions, and likely behavior.

Consider some examples of present and future implications. Public surveillance cameras typically produce thousands of hours of footage. This is far too much to be examined manually absent some very particularized starting inquiry. Machine learning tools can be cheaply trained to analyze large volumes of footage, and to recognize faces or patterns of conduct through analyses that take a fraction of the time and effort needed for human inspection.[6] In a different context, new computational tools can be trained to analyze the way in which a person holds and swipes her cellphone so as to uniquely identify a user.[6a] Commercial banks are already using such biometric

---

[1] *See* Judith Shklar, *The Liberalism of Fear*, in LIBERALISM AND THE MORAL LIFE 22, 24–25 (Nancy Rosenblum, ed., 1989).
[2] This is a central theme of JAMES C. SCOTT, SEEING LIKE A STATE: HOW CERTAIN SCHEMES TO IMPROVE THE HUMAN CONDITION HAVE FAILED 23-24 (1998) (exemplifying the "pattern of relations between local knowledge and practices" and "state administrative routines."); *see also* CHARLES S. MAIER, LEVIATHAN 2.0: INVENTING MODERN STATEHOOD 86-93 (2012) (describing the interaction of technological changes during the Industrial Revolution and the European state).
[3] Technology is not the only determinant of this liberal dilemma. The range of institutional forms available to the state also matters. Most famously, the historian Stephen Skowronek underscores the move from a state of "courts and parties" to one channeled through national bureaucracies. STEPHEN SKOWRONEK, BUILDING A NEW AMERICAN STATE: THE EXPANSION OF NATIONAL ADMINISTRATIVE CAPACITY 1877-1920, at 24, 35 (1982).
[4] Sendhil Mullainathan & Jann Spiess, *Machine learning: an applied econometric approach*, 31 J. ECON. PERSP. 87, 88 (2017) (defining machine learning in terms of its capacity for "out of sample" prediction). For further details on machine learning and its functionalities, *see infra* text accompanying notes 28 to 38 (defining machine learning)
[5] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 233-34 (2018).
[6] James Vincent, *Artificial Intelligence is Going to Supercharge Surveillance*, THE VERGE, Jan. 23, 2018, https://www.theverge.com/2018/1/23/16907238/artificial-intelligence-surveillance-cameras-security [https://perma.cc/YGR4-3GAY]. Machine learning-driven analysis of video surveillance, though, is not proof against counter-strategies, such as the use of "adversarial patches" on clothing that undermine common inference strategies. Simon Thys et al., *Fooling Automated Surveillance Cameras: Adversarial Patches to Attack Person Detection*, PROC. IEEE CONF. COMPUTER VISION & PATTERN RECOGNITION WORKSHOPS (2019), http://openaccess.thecvf.com/content_CVPRW_2019/html/CV-COPS/Thys_Fooling_Automated_Surveillance_Cameras_Adversarial_Patches_to_Attack_Person_Detection_CVPRW_2019_paper.html [https://perma.cc/F2QP-TTV6].
[6a] Claire Reilly, *The way you swipe your phone could be used to track you*, CNET, July 31, 2018, https://www.cnet.com/news/the-way-you-swipe-your-phone-could-be-used-to-track-you/.

signatures to regulate remote account access.[7] Some day soon, state uses of the same functionality will follow.

Such examples may understate the significance of machine learning. The latter is a "powerful and highly generalizable set of capabilities" that "in principle . . . can be applied to the management of *any complex system*, from the steering and guidance of a car to the shaping of public policy."[8] As such, machine learning can generate action-guiding predictions about who should be detained,[9] who should be deported,[10] who should be audited,[11] who should be fired from state office,[12] who should ranked in need of state assistance,[13] and even who should be killed.[14] Across these applications, machine learning has the potential to greatly improve on imperfect human action, or alternatively to generate new social costs and compound malign forms of social stratification.

This Article documents this ongoing technological shift in state action. I then analyze how important individual rights to due process, equality, and privacy may be appropriately conceptualized and implemented in the context of growing state reliance on machine learning. My first aim is hence descriptive in character. I highlight a subset of ground-level applications of the machine-learning state that most sharply implicate rights-related concerns. While new computational tools technology can be used at many different points of the policy-making, legislating, and administrative processes, I think the sharpest normative concerns are likely to arise when an algorithm proximately causes a benefit or penalty to be assigned (or withheld) to (from) a specific individual.[15] Sharp normative concerns can also arise when a machine-learning tool is used to allocate investigative resources, especially when the becoming a target of investigation has immediate costs. Documenting both existing and likely future deployments of machine learning, particularly by state and local governments, I draw attention to ways such deployments can implicate due process, equality, and privacy concerns. I do not claim such worries are wholly new. In some instances, constitutional concerns track those presented by human action. At other instances, novel worries arise.

---

[7] Alison Arthur & Bethany Frank, *Five Examples of Biometrics in Banking*, ALACRITI (May, 8, 2019), https://www.alacriti.com/biometrics-in-banking [https://perma.cc/ZS8Z-UEVY].

[8] ADAM GREENFIELD, RADICAL TECHNOLOGIES: THE DESIGN OF EVERYDAY LIFE 226 (2017) (emphasis added).

[9] Aziz Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, 68 DUKE L. J. 1043, 1072-76 (2019) [hereinafter "Huq, *Racial Equity*"] (describing the use of machine-learning tools in bail and sentencing contexts).

[10] Spencer Woodman, *Palantir Provides the Engine for Donald Trump's Deportation Machine*, INTERCEPT (Mar. 2, 2017, 1:18 PM), https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/ [https://perma.cc/D2LK-EAYR] (reporting that the Department of Homeland Security ("DHS") awarded a private contractor a $41 million contract to build an "Investigative Case Management" system to allow DHS to "access a vast 'ecosystem' of data to facilitate immigration officials in both discovering targets and then creating and administering cases against them").

[11] Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 GEO. L.J. 1147, 1163 (2017) [hereinafter "Coglianese & David Lehr, *Regulating by Robot*"].

[12] Derek Black, *The Constitutional Challenge to Teacher Tenure*, 104 CAL. L. REV. 75, 92-96 (2016) (describing federally mandated adoption of "valued added models" for teacher evaluation).

[13] Colin Lecher, *What Happens when an Algorithm Cuts Your Health Care*, THE VERGE, Mar. 21, 2018, https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy [https://perma.cc/J9RD-3KMJ].

[14] Will Knight, *The Dark Secret at the Heart of AI*, MIT TECH. REV., Apr. 11, 2017, https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/ [https://perma.cc/7D94-2FD2] ("The U.S. military is pouring billions into projects that will use machine learning to pilot vehicles and aircraft, identify targets, and help analysts sift through huge piles of intelligence data.").

[15] Those concerns are not wholly absent where individualized determinations are not at stake, but I will focus here on cases of individualized machine determinations because they present the constitutional issues most acutely.

This descriptive exercise exploits the fact that a disparate scattering of plaintiffs are starting to challenge algorithmic instrument in federal and state court.[16] Cases have arisen in the bail and sentencing context in Wisconsin,[16a] California,[16b] Ohio,[16d] and New York.[16e] Litigation often hinges on whether a particular algorithm can be disclosed consistent with trade secrets law.[17] Legal questions are not confined to the criminal justice realm. In Houston, a teachers' union brought an action against an algorithmic tool used to evaluate job performance and determine discharges on due process grounds.[18] In Arkansas, state disability recipients filed suit against the Arkansas Department of Human Services alleging that an "unlawful switch to the computer algorithm" had violated the state's administrative procedure act.[19] None of these cases, though, grapple head-on with the novel questions presented by constitutional challenges to the machine learning state. To the contrary, their evasion of this question hint at a need for more systemic thinking about how those constitutional norms should be adapted, and the regulatory and litigation structures best fitted to inducing constitutional compliance.

Having established a descriptive baseline, I develop two lines of normative analysis. The first takes up ways in which norms of due privacy, privacy, and equality might be usefully recalibrated as the state shifts from human to machine action. Second, I offer a general account of how the enforcement regime for these rights might best account for the distinctive qualities of the machine-learning state. I sketch here the core points of both analytic arcs in brief here.

In regard to the first question of constitutional substance, I focus on due process, equality, and informational privacy concerns because they seem to be the rights most immediately pertinent in the machine learning state. Whereas the Court has developed detailed doctrinal accounts of due process and privacy, the constitutional law of informational privacy is thin. Despite this difference in the degree of doctrinal development, a gap separates extant doctrinal formulations of all three rights and the technological terrain of machine learning. Present doctrinal formulations do not necessarily realize well the values underlying the rights to due process, equality, or privacy when the focus shifts from human to machine action. (Perhaps those doctrinal formations are a bad match to more mundane institutional settings and problems. But demonstrating that is not my concern here). Even if they do not completely displace human judgment, and even if prior dispensations entailed some human reliance upon structured decision-making tools such as checklists or simple algorithms, I contend that machine learning tools raise constitutional concerns in different ways from human action.

---

[16] An algorithm is "any well-defined computational procedure that takes some value, or set of values, as input and produces some value, or set of values, as output." THOMAS H. CORMEN ET AL., INTRODUCTION TO ALGORITHMS 5 (2d ed. 2001) (emphases omitted)). Machine learning tools are a distinctive subset of algorithms; most of the algorithms challenged in the cases discussed here have been simpler beasts.

[16a] State v. Loomis, 881 N.W.2d 753 (2016).

[16b] People v. Superior Court (*Chubbs*), No. B258569, 2015 WL 139069, *3 (Cal. Ct. App. Jan. 9, 2015).

[16d] State v. Jennings, 2014-Ohio-2307, at ¶ 24 (Ohio Ct. App. 2014).

[16e] Flores v. Stanford, No. 18-2468, 2019 WL 4572703, at *11 (S.D.N.Y. Sept 20, 2019).

[17] *See* State v. Loomis, 881 N.W.2d 749, 760 (2016); People v. Superior Court (*Chubbs*), No. B258569, 2015 WL 139069, *9 (Cal. Ct. App. Jan. 9, 2015).

[18] Houston Fed'n of Teachers, Local 2415 v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1171 (S.D. Tex. 2017) (challenging "the use of privately developed algorithms to terminate public school teachers for ineffective performance" on due process grounds).

[19] Ark. Dep't of Human Servs. v. Ledgerwood, 2017 Ark. 308, 10, 530 S.W.3d 336, 344 (2017); *see also* K.W. v. Armstrong, 180 F. Supp. 3d 703, 706–07 (D. Idaho 2016) (due process challenge to software used to calculate Medicaid benefits); T. v. Bowling, No. 2:15-CV-09655, 2016 WL 4870284, at *7–*9 (S.D. W. Va. Sept. 13, 2016) (same for algorithmic benefits calculation for the developmentally disabled).

Yet constitutional rights have been calibrated with human behavior in mind.[20] My modest aim here is to suggest some ways in which doctrine can be adjusted or extended given the novel technological landscape. To emphasize, these are suggestions rather than definitive prescriptions. The technological and social landscape is changing rapidly, and it would be foolish to aver certainty. I aim here to start a conversation, and not provide conclusive answers.

Technological changes places pressure on the formulation of due process, equality, and privacy interests in subtly different ways. For example, in the most familiar cases that courts have historically addressed, due process is advanced by giving regulated subjects an opportunity of a hearing before an individual adjudicator, or an appeal to a new adjudicator. If we are concerned with minimizing the net volume of false positives and false negatives, however, there is reason to believe that a human appeal of a machine decision will often be counterproductive. Rather, due process may requires changes to an classifier to reduce the risk of errors. An equality-related example of the constitutional implications of changing from human to machine-derived judgments of recidivism risk in the criminal justice system. On the one hand, the increasing use of computational prediction tools may well reduce the opportunities for individual bias on the part of adjudicators such as judges and magistrates to influence decisions. On the other hand, those same tools may embed assumptions about racial and ethnic groups in ways that reproduce undesirable patterns of residential, economic, and social stratification. Whereas equality-related regulation of human actors might usefully focus on concepts of bias and discriminatory intent, it may be more useful to consider computational predictive tools in terms of their predictable disparate effects. Finally, constitutional rules under the Fourth Amendment regulate how the state collects data about its citizens and other regulated subjects, and have little to say ln how that information is used.[21] A technology that allows the state to exploit publicly available data—surveillance footage, public records, and commercial records not protected by the Fourth Amendment—for insights into individual conduct means the state can eschew surveillance regulated by the Fourth Amendment, and yet acquire the same information with relative ease. Thanks to technological change, therefore, the existing Fourth Amendment will increasingly fail to shelter constitutional privacy interests. Indeed, the risk to privacy from the state might soon emerge in quite unexpected ways, for instance through the incidence of data theft from the databases that the state creates in order to implement machine learning tools.[22]

There is a second, somewhat more abstract, reason for looking closely at the implementation of constitutional rights in the machine learning state. Knowledge and understanding of computational

---

[20] In addition, this is because lawyers and judges are not trained in either computer science or statistics, understanding of how machine learning tools work—and how they are similar to, or diverge from, other governance instruments—is not yet widespread. Obviously, this article is an effort to start filling that gap—albeit from the perspective of a lawyer, and not a computer scientist or statistician!

[21] For an analysis of technological change's influence on surveillance, see Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 3 (2008) (describing the "National Surveillance State [as] a special case of the Information State—a state that tries to identify and solve problems of governance through the collection, collation, analysis, and production of information"). In contrast, there is surprisingly little scholarship on how the state *uses* information it can collect without constitutional regulation. For a prescient but lonely treatment of use restrictions under the Fourth Amendment, see generally Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49 (1995) (arguing that the reasonableness of a seizure extends to uses even after law enforcement seizes information).

[22] Consider, for example, the risk of data breaches that comes with expanded algorithmic capacity. Owen Daugherty, *Oregon state agency suffers data breach, potentially exposing personal information*, THE HILL, March 21, 2019, https://thehill.com/homenews/state-watch/435218-oregon-state-agency-suffers-breach-potentially-exposing-personal-data [https://perma.cc/TBB8-CFQ5]; *see infra* Part II.C (discussing privacy implications of data breaches).

tools is presently not widely shared. The general public in particular lacks a clear or precise understanding of those instruments, or their limits. Machine learning is taking root in the state before legal professionals have absorbed sufficient technical knowledge or practical understanding. It is reasonable to predict that the adoption of machine learning will endow the state with new capabilities, but will also be distinctly difficult to understand from the perspective of both legal actors and the public. Indeed, it is reasonable to worry that increases in state power will be correlated with a diminishing capacity on the part of regulated subjects to understand or challenge exercises of that power.[23] To be sure, this asymmetrical effect may be buffered by the efforts of well-meaning computer scientists to educate the public and the legal profession about machine learning. But I am skeptical that such efforts will be sufficient. As a result, state adoptions of predictive and inference tools are likely to increase the difficulty that citizens have monitoring and responding to its activities, even as the scope of those activities grows.

The second main analytic contribution of this article is an analysis of the institutional arrangements through which constitutional values might best be vindicated. At present, constitutional norms of due process, privacy, and equality are principally developed and vindicated via a common-law process of discrete, incremental and ex post litigation. It thus follows the "liability in tort" model commonly identified with the common law.[24] In previous work, I have criticized the discrete and individuated forms through which constitutional rights are enforced in the ordinary course of non-machine governance for failing to properly constrain the state, and also for embodying controversial and regressive moral intuitions.[25] I have also argued in favor of conceptualizing constitutional harms in terms of systemic dynamics implicating collective interests.[26] That is, I have previously expressed skepticism about the dominant "liability in tort" model as applied in traditional contexts. Consistent with those arguments, I argue below that the constitutional concerns raised by machine learning tools, like many other public policies, are best addressed through a mix of ex ante regulation and aggregate litigation (i.e., litigation seeking to vindicate the interests of a specific individual). Outside the machine learning state, this aggregate model has largely failed, thanks in large measure to judges hostile toward certain constitutional rights (and perhaps also to certain populations, such as criminal defendants and prisoners). But the novelty of computational tools presents an opportunity for doing better. I thus press here the claim that the machine learning state is well suited to a combination of ex ante regulation and ex post collective auditing (albeit without assuming that non-algorithmic policies would not benefit from this same approach).

---

[23] *Cf.* JAMIE SUSSKIND, FUTURE POLITICS: LIVING TOGETHER IN A WORLD TRANSFORMED BY TECH 168-87 (2018) ("The future state, armed with digital technologies, will be able to monitor and control our behaviour much more closely than in the past.").
The literature's relative inattention to machine-learning and other analytic tools is perhaps a result of the Constitution's direct regulation of information acquisition through the Fourth Amendment, and its more diffuse and indirect regulation of information processing and use.

[24] Steven Shavell, *Liability for harm versus regulation of safety*, 13 J. LEG. STUD. 357, 357 (1984).

[25] *See, e.g.,* Aziz Z. Huq and Genevieve Lakier, *Apparent Fault* 131 HARV. L. REV. 1525, 1547–48 (2017) (arguing that courts require apparent fault, i.e. that a defendant violated not only the law but also a social understanding of legality, before remedying constitutional wrong); Aziz Z. Huq, *Judicial Independence and the Rationing of Constitutional Remedies*, 65 DUKE L.J. 1, 70–74 (2015) (noting that a fault regime for constitutional remedies leads to unequal treatment of constitutional wrongs, unequal vindication of constitutional rights, and unequal treatment of litigants); Aziz Z. Huq, *Habeas and the Roberts Court*, 81 U. CHI. L. REV. 519, 581–86 (2014) arguing that habeas review applies a similar fault regime).

[26] *See, e.g.,* Aziz Z. Huq, *The Consequences of Disparate Policing: Evaluating Stop and Frisk as a Modality of Urban Policing*, 101 MINN. L. REV. 2397, 2438–39 (2017)(arguing that police misconduct fails to breed collective efficacy).

In particular, I explore the application of strategies of ex ante regulation, such as technology mandates and transparency regimes of various forms. One aim of such interventions is to facilitate ex post inquiry into whether and how a machine-learning tool behaves 'in the wild' (which may be quite different from how it behaves 'in the lab'). Then, in respect to auditing instruments through ex post litigation, I underscore the utility of wholesale, prospective, and system-wide forms of relief. Again, nothing in what follows should be construed to imply that similar mixes of regulation and aggregate litigation would be inapt for other contexts. Quite the contrary. Perhaps the 'shock of the new' in the machine-learning context will prompt a more general reconsideration.

The argument proceeds as follows. Part I recounts how the state leans increasingly on machine-learning tools as aid or substitute for human decision-making. Part II considers how due process, privacy, and equality values might be recalibrated. Part III then examines how ex ante regulation and ex post aggregate litigation might be combined to ensure that machine-learning instruments remain consistent with constitutional norms.

I. The Machine Learning Turn in Governance

In the last decade, advances in the computational science of machine learning have enabled new functionalities of prediction and inference.[26a] The state leverages these new tools to vindicate traditional policy ends or to pursue novel goals. Whatever the consequent hazard to constitutional values, there is little chance that the state will forego these new technologies . Quite apart from their efficiency gains, the United States is under intense pressure from domestic interest groups, such as big tech firms, and from geostrategic competitors to accelerate development and diffusion of machine learning.[27] One reason to analyze constitutionalism in the machine-learning state is thus the political inevitability of the latter's adoption in respect to a growing range of state functionalities. To that end, this Part describes the core of the technology at issue, recent and impending state and local adoptions, and some of the ensuing litigation challenges.

A. New Instruments of Prediction and Inference

In general terms, a machine learning algorithm is a computational tool designed to solve a "learning problem . . . of improving some measure of performance when executing some task, through some type of training experience."[28] At an operational level, machine learning has been described in simple terms as follows: "[y]ou give the machine data, a goal and feedback when it's on the right track – and leave it to work out the best way of achieving the end."[29] The common method of supervised

---

[26a] *See* Jonathan Schmidt et. al, *Recent Advances and Applications of Machine Learning in Sold-State Materials Science*, 5:83 NPJ COMPUTATIONAL MATERIALS 1, 1–2 (2019).

[27] For a political economy of machine learning's adoption by the state, see Mariano-Florentino Cuéllar & Aziz Z. Huq, *Privacy's Political Economy and the State of Machine Learning: An Essay in Honor of Stephen J. Schulhofer*, 72 NYU ANN. SURV. AM. L. 14–18 (forthcoming 2020).

[28] M.I. Jordan & T.M. Mitchell, *Machine learning: Trends, perspectives, and prospects*, 349 SCIENCE 255, 255 (2017); *see also* Susan Athey, *The Impact of Machine Learning on Economics* 3 (Jan., 2018), https://www.nber.org/chapters/c14009 ("[M]achine learning is a field that develops algorithms designed to be applied to data sets, with the main areas of focus being prediction (regression), classification, and clustering or grouping tasks.").

[29] HANNAH FRY, HELLO WORLD: BEING HUMAN IN THE AGE OF ALGORITHMS 11 (2019); *see also* JERRY KAPLAN, ARTIFICIAL INTELLIGENCE: WHAT EVERYONE NEEDS TO KNOW 32 (2016) (providing a similar colloquial description).

learning,[30] for example, entails first supplying an algorithm with a labeled set of training data,[31] and then instructing it to derive (or learn) a rule that discriminates between two subsets within the training sample.[32] Thus, the training data might comprise a set of images, says labeled "dog," "cat," and "rat." The algorithm might then be instructed to learn a rule to separate images of dogs those from cats or rats. Supervised learning can be binary or multi-class, as in this example.[32a] It can also entail estimation of a continuous rather than categorical variable. Using a random starting formulation of a decision rule, the algorithm will at first do no better than random at predicting the right subset. But by perturbing the rule, and evaluating whether changes produce more or less accurate results, the algorithm can 'learn' a rule that does predict well how the data's features map onto those subsets.[33] This classifying rule, though, is not the direct result of human design.

Notwithstanding the simplicity of this explanation, machine learning tools can be highly complex in ways that defeat any effort at either facile explication or reverse engineering of their decisional processes. To get a sense of this potential for complexity, consider the example of deep learning networks. The latter are 'deep' in the sense of relying on multiple layers of nodes through which inputs are channeled and processed.[34] Important forms of deep learning are recurrent neural nets (RNN), which are used in text recognition and translation tools, and convolutional neural nets (CNN), which are central to machine vision.[35] Both RNNs and CNNs process large volumes of training data (such as millions of images or large bodies of text) each with thousands or millions of features. They exploit networked structures to process this data in ways that their constituent elements could not do on their own. An early and influential deep learning such instrument, designed by Geoffrey Hinton and colleagues, thus handled data with some 60 million parameters.[36] Deep networks can perform some inference tasks that simple instruments cannot. Today, the ChronoNet CNN can

---

[30] Jordan & Mitchell, *supra* note 28, at 257 (defining supervised learning as a process in which "the training data take the form of a collection of (*x*, *y*) pairs and the goal is to produce a prediction *y** in response to a query *x**"). Note that this definition is framed in terms of binary classification. This process can also be described in terms of a "classifier" rather than a function, that examines inputs with "feature values" and outputs a class variable. Pedro Domingos, *A Few Useful Things to Know About Machine Learning*, COMM. ACM, Oct. 2012, at 79-80 ("A *classifier* is a system that inputs (typically) a vector of discrete and/or continuous *feature values* and outputs a single discrete value, the *class*."). An *unsupervised* machine-learning algorithm begins with unlabeled training data and develops classifications based on the data's immanent structure. PETER FLACH, MACHINE LEARNING: THE ART AND SCIENCE OF ALGORITHMS THAT MAKE SENSE OF DATA 14-17 (2012).

[31] Comm. on the Analysis of Massive Data et al., *Frontiers in Massive Data Analysis* 104 (2013), http://www.nap.edu/catalog.php?record_id=18374.

[32] ETHEM ALPAYDIN, MACHINE LEARNING: THE NEW AI 46-47 (2016) ("A *class* is a set of instances that share a common property . . . there exists a formulation of the class in terms of those [certain] characteristics, called a *discriminant*.").

[32a] *See* Javaid Nabi, *Machine Learning—Multiclass Classifications with Imbalanced Datasets*, TOWARDS DATA SCIENCE (Dec. 22, 2018), https://towardsdatascience.com/machine-learning-multiclass-classification-with-imbalanced-data-set-29f6a177c1a [https://perma.cc/U9N4-9X2F].

[33] ARLINDO OLIVEIRA, THE DIGITAL MIND: HOW SCIENCE IS REDEFINING HUMANITY 96-97 (2017) (exploring inductive character of machine learning).

[34] Yann LeCun, Yoshua Bengio & Geoffrey Hinton, *Deep Learning*, 521 NATURE 436, 438 (2015) (defining deep learning).

[35] JOHN KELLEHER, DEEP LEARNING 160–62, 181–83 (2019).

[36] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton, *Imagenet classification with deep convolutional neural networks*, ADVANCES IN NEURAL INFORMATION PROCESSING SYS. 5 (2012).

examine photographic images to estimate the date at which they were taken,[37] and inspect electroencephalograms images to predict the incidence of epilepsy and other brain disorders.[38]

The design of any machine learning tool requires a number of judgments not mechanically determined by computational theory or the logical limits to algorithmic design. Importantly, choices first need to be made about what training data will be used.[39] Different selections of training data will yield different predictive models.[40] In the state-action context, available data will often be a product of historical state practices, such as the management of public benefits or the policing of a particular geographic area or ethnoracial concentration. If such historical practices were flawed or biased, the data thereby produced also may also be deficient or misleading in the sense of incorporating biases, blind spots, or unwarranted assumptions. Such gaps or other deficiencies in the data then precipitate for the designer a further question of about whether (and if so how) corrective measures might be taken.[41] Then, once a set of training data set is in hand, a designer must decide on which attributes, or "features," of the training data to employ in learning a new rule.[42] Should gender, race, or another protected trait, for instance, be among them? What about variables that might closely and predictably correlate with a protected trait, such as residential ZIP code? What if an impermissible classification or its close proxy is necessary to reasonably good algorithmic performance (however that is defined)?

At the same time, the designer needs to decide on an "outcome variable."[43] An algorithm will optimize a function of the outcome variable and the model parameters, (together called the cost function) to generate predictions.[44] Several such outcome variables may be available, and yet none may precisely track the underlying matter of policy interest. The designer must then choose among unreliable proxies.[44a] Similarly, the designer must decide which algorithmic method (*e.g.*, naïve Bayes, random forests, neural network, etc.) best fits her problem, a choice which requires her *inter alia* to decide whether to use a relatively straightforward instrument or to select a more complex deep learning tool.[45] This methodological choice is no simple matter.[46] Insiders describe "a field in constant tribal

---

[37] Blaise Agüera y Arcas, Margaret Mitchell and Alexander Todorov, *Physiognomy's new clothes*, MEDIUM, May 6, 2017, https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a [https://perma.cc/Q8NU-CYM7].

[38] Subhrajit Roy et al., *ChronoNet: A Deep Recurrent Neural Network for Abnormal EEG Identification*, ARXIV PREPRINT ARXIV:1802.00308, at 1 (2018).

[39] In a useful article, Lehr and Ohm call this stage "playing with the data." David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. DAVIS L. REV. 653, 700–01 (2017) (describing feature selection).

[40] ALPAYDIN, *supra* note 32, at 68-83; Susan Athey, *Beyond Prediction: Using Big Data for Policy Problems*, 355 SCIENCE 483, 483 (2017) (explaining that machine-learning "programs take as input training data sets and estimate or 'learn' parameters that can be used to make predictions on new data").

[41] Lehr & Ohm, *supra* note 39, at 681-83.

[42] *Id.* at 700–01.

[43] *Id.* at 672-73.

[44] *Id.* In a bit more detail, each possible model (given by a set of parameters like the coefficients in a regression equation) corresponds to a set of predictions of the outcome variable. The cost function defines a "cost" or penalty between predictions and the true (observed) outcome, and then the aim is minimize that cost. For example in the familiar context of linear regression, one is trying to minimize the sum of least squares.

[44a] *Id.* at 675.

[45] OLIVEIRA, *supra* note 33, at 110-11. Note that the choice of features and method is often made simultaneously.

[46] Indeed, sometimes researchers mislabel the method that they have in fact chosen. For cases of this, see Adrien Jamain and David J. Hand, *Where are the large and difficult datasets?* 3 ADVANCES IN DATA ANALYSIS & CLASSIFICATION 25, 29–31 (2009).

warfare" between different approaches.[47] Within this field of contestation, the value of increasingly complex instrument design is particularly contested, with some computer scientists warning that the increasing complexity and sophistication of newer predictive tools has not yielded performance gains sufficiently robust to "translate into real advantages in practice" on real-world problems.[48]

This, moreover, is not the full extent of necessary judgments by our designer. Another important challenge in designing machine learning tools is the problem of "overfitting."[49] This occurs, in effect, when an instrument has been too good at writing a predictor for the training data without accounting for the fact that the latter is merely a noisy sample drawn from the world. Solutions to overfitting require a measure of judgment about how much to constrain the model's learning from the training data.[50] Moreover, an instrument learns "specific contingencies for particular scenarios."[51] It does not grasp underlying concepts. A consequence of this thin form of 'understanding' is that tools can be brittle when confronted with examples outside their training data. There is hence a risk that the rate of successful prediction will drop rapidly when an instrument is "confronted with scenarios that differ in minor ways from the one ones on which the system was trained show that deep reinforcement learning's solutions are often extremely superficial."[52] "[H]idden feedback loops" can emerge after beta testing.[53] Adversarial tactics, such as the strategic deployment of other machine learning tools, can also induce misclassification.[54] Such vulnerabilities can have nontrivial, even "catastrophic[]," consequences.[55] For all these reasons, it is not safe to assume that a machine learning tool will operate predictably on data drawn from a different distribution from the training data.

B. The Machine Learning State

Since the eighteenth-century, a central component of state-building has involved deepening information-gathering capabilities and eroding private efforts to shield the person from the state's gaze.[56] The state has also sought "legible form[s]" in which to record data about individual citizens for easy "reading, processing, and relaying."[57] Machine learning advances these epistemic

---

[47] Carlos E. Perez, *The Many Tribes of Artificial Intelligence*, MEDIUM, Jan. 12, 2017, https://medium.com/intuitionmachine/the-many-tribes-problem-of-artificial-intelligence-ai-1300faba5b60 [https://perma.cc/52CG-PRYS] (listing symbolists, evolutionists, Bayesians, kernel conservatives, tree huggers, and connectionists among those warring factions).

[48] David J. Hand, *Classifier technology and the illusion of progress*, 21 STAT. SCI. 1, 2 (2006).

[49] PEDRO DOMINGUOS, THE MASTER ALGORITHM: HOW THE QUEST FOR THE ULTIMATE LEARNING MACHINE WILL REMAKE OUR WORLD 71-72 (2015) (describing overfitting and characterizing it as the "central problem" of machine learning design); *see also* Krizhevsky et al., *supra* note 36, at 6 (describing technical solutions).

[50] *See, e.g.,* Mullainathan & Spiess, *supra* note 4, at 91-93 (describing the process of regularization and empirical tuning to mitigate overfitting with decision tree models).

[51] Gary Marcus, *Deep Learning: A Critical Approach*, ARXIV PREPRINT ARXIV:1801.00631, at 8 (2018).

[52] *Id.*; *see, e.g.*, Robin Jia and Percy Liang, *Adversarial examples for evaluating reading comprehension systems*, ARXIV PREPRINT ARXIV:1707.07328, at 2 (2017) (demonstrating that the accuracy of a language recognition CNN can be halved by inserting ungrammatical 'junk' into the data).

[53] David Sculley et al., *Machine learning: The high interest credit card of technical debt* 3 (2014), https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43146.pdf.

[54] Nicolas Papernot et al., *Practical black-box attacks against machine learning*, PROC. 2017 ACM ON ASIA CONF. ON COMP. & COMM. SEC. 506, 510 (2017).

[55] Brenden M. Lake and Marco Baroni, *Generalization without systematicity: On the compositional skills of sequence-to-sequence recurrent network*s, ARXIV PREPRINT ARXIV:1711.00350, at 1 (2017).

[56] JAMES C. SCOTT, SEEING LIKE A STATE: HOW CERTAIN SCHEMES TO IMPROVE THE HUMAN CONDITION HAVE FAILED 91–92 (1998).

[57] COLIN KOOPMAN, HOW WE BECAME OUR DATA: A GENEALOGY OF THE INFORMATIONAL PERSON 37 (2019).

projects by introducing new means of exploiting data that public authorities have to hand for other reasons. In private contexts, machine learning tools are used for tasks such as ranking (Google's and Netflix's algorithms) and classification (credit scoring tools and spam blockers).[58] The state can employ the same techniques of ranking and classification to infer facts about regulated subjects' past behavior or to predict their future actions. These inferences can then be deployed to advance a wide range of policy ends: improving criminal justice; refining education policy (especially teacher hiring and retention decisions); targeting regulatory inspections (such as restaurant health inspections); identifying youth at risk of criminal conduct or involvement; and predicting individual financial outcomes such as default.[59] At the same time, there is no reason why prediction will be used solely for benevolent or wise ends. Predictive instruments are already used overseas to stifle political opposition.[60] As a policy tool, that is, machine learning is not intrinsically 'good' or 'bad.' Its normative valence depends on how it is used, and what collateral costs it imposes.

This section canvasses current and likely future uses of machine learning being by federal, state, and local governments in both civil and criminal domains. In the former, predictive instruments are used to facilitate allocate enforcement resources, make employment decisions, and assign benefits. In the latter domain, algorithms are used to allocate coercion either in the form of policing resources or incarceration either before or after criminal trial and sentencing. Adoption of machine learning is, I should emphasize, presently uneven. At the moment, many jurisdictions use predictive instruments that have not been developed using the methods described in Part I.A . Baltimore, for instance, makes bail decisions using a form generated by the City's Pretrial Release Services containing seven questions and a list of twelve mitigating or aggravating factors.[61] This seems unlikely to endure. A recent study using New York bail data, for example, boasts that deep learning might generate large efficiency gains in pretrial practice.[62] Given the allure of cost savings (and, no doubt, lobbying by firms wishing to sell predictive instruments and the academics who advise them), states are likely to adopt machine learning tools over clinical assessments or simple human judgment sooner rather than later. Hence, what follows should be understand as exemplifying, and not exhausting, the range of likely near-future uses.

1. Machine Learning and the Regulatory State

The use of machine learning to guide enforcement resources, such as restaurant inspectors, tax audits, and fraud detection is increasingly common.[63] Some instances of these machine-guided

---

[58] FRY, *supra* note 29, at 8-9; *see also* PEDRO DOMINGOS, THE MASTER ALGORITHM: HOW THE QUEST FOR THE ULTIMATE LEARNING MACHINE WILL REMAKE OUR WORLD 8 (2015) (citing "pattern recognition, statistical modeling, data mining, knowledge discovery, predictive analytics, data science, adaptive systems, self-organizing systems, and more").

[59] Jon Kleinberg et al., *Prediction policy problems*, 105 AM. ECON. REV. 491, 494 (2015).

[60] *See, e.g.,* Steven Feldstein, *How Artificial Intelligence is Reshaping Repression*, 30 J. DEM. 40, 42 (2019) (noting how effective AI technology is for repressing dissent). For a graphic and troubling example, see Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame, and Lots of Cameras*, N.Y. TIMES, July 8, 2018.

[61] George Joseph, *Justice by Algorithm*, CITYLAB, Dec. 16, 2018, https://www.citylab.com/equity/2016/12/justice-by-algorithm/505514/ [https://perma.cc/NCG8-V3X3]. This comprehensive piece notes both ambiguity in how the instrument was created, and how it is applied. *Id.* (noting that "the relationship between risk scores, bail recommendations, and bail decisions remains opaque").

[62] Jon Kleinberg et al. *Human Decisions and Machine Predictions*, 133 Q. J. ECON. 237, 239–41 (2018).

[63] Cary Coglianese and David Lehr, *Transparency and Algorithmic Governance*, 71 ADMIN. L. REV. 1, 7–8 (2019) [hereinafter "Coglianese & Lehr, *Transparency and Algorithmic Governance*"] (collecting examples); *see also* Katelynn Devinney, Adile Bekbay, Thomas Effland, Luis Gravano, David Howell, et al., *Evaluating Twitter for Foodborne Illness Outbreak Detection in*

discretion raise important ethical and constitutional questions. For example, decisions about how enforcement resources are allocated can raise concerns about racial or ethnic bias.[64] Cases in which a predictive instrument is used to directly assign coercion or benefits to an individual obviously can raise due process. And any data aggregate can prompt privacy concern. By way of example, I flag here one machine learning tool used to allocate investigative resources in a context fraught with normative concerns.

This predictive tool was introduced in August 2016 in Allegheny County, Pennsylvania.[64a] Allegheny Family Screening Tool (AFST) extracted 71 features from a dataset created collaboratively by several state agencies as a basis in order to predict instances of abuse of neglect amongst calls made to a state hotline.[65] An AFST score capturing a risk of abuse was displayed to case workers who receive and screen such calls, and used to inform the decision to investigate or not.[65a] An investigation in turn could potentially end in a child's removal from a home. Carefully timed disclosure was meant to avoid excessive reliance on the score at the expense of more granular information.[66] Nevertheless, case workers may presume the AFST score is more accurate than their own observations.[67] Florida implemented a similar predictive tool in 2016, and several states are studying its experience to determine whether to follow suit.[68]

Commentators have raised three normative concerns about the AFST system. First, there is evidence from Allegheny County of racial disparities in the decisions taken with the AFST scores. African-American families, for example, appear to experience "disproportionate referrals" based on seemingly innocuous events such as a missed doctor's appointments.[69] The designers of AFST identified a risk that either caseworker animus or correlations between nonracial data (e.g., residential zip code) and race could induce differential treatment of equally at-risk black and white children.[70] Second, some observers have raised a concern about the "dehumanizing" effect on parents of having "their entire history . . . summed up in a single number."[71] Finally, the AFST system draws upon considerable stocks of state data by aggregating disparate information. The creation of such aggregates, which might shed considerable light on private facts and behaviors, likely creates a risk of data breaches.[72] Equality, due process, and privacy, in short, are all potentially in play.

New York City," 10 J. PUB. HEALTH INFORMATICS e120 (2018) (reporting on New York's use of Twitter data to guide health inspection of restaurants).

[64] Kristen M. Altenburger and Daniel E. Ho, *When Algorithms Import Private Bias into Public Enforcement: The Promise and Limitations of Statistical De-biasing Solutions*, 175 J. INST. & THEO. ECON. 98, 99 (2019) (finding overreporting for ethnic restaurants).

[64a] Alexandra Chouldechova et al., *A case study of algorithm-assisted decision making in child maltreatment hotline screening decisions*, CONFERENCE ON FAIRNESS, ACCOUNTABILITY & TRANSPARENCY 138, 143 (2018).

[65] *Id.*; *see also* VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 132-42 (2018) (describing AFST's implementation).

[65a] Chouldechova et al., *supra* note 65, at 138–39.

[66] *Id.* at 141 (noting that AFST is "a decision-support tool that is presented to call screeners at a specific juncture in the decision-making pipeline").

[67] EUBANKS, *supra* note 65, at 141-42.

[68] Stephanie Cuccaro-Alamin et al., *Risk assessment and decision making in child protective services: Predictive risk modeling in context*, 78 CHILD. & YOUTH SERVS. REV. 291, 294 (2017).

[69] EUBANKS, *supra* note 65, at 153-54.

[70] Chouldechova et al., *supra* note 65, at 145.

[71] EUBANKS, *supra* note 65, at 152.

[72] *See infra* text accompanying notes 236 to 262 (discussing data breaches in more detail).

Despite these concerns, the use of machine learning in a form akin to an AFST score appears relatively weakly constrained by constitutional norms. Federal administrative law imposes little check on decisions to forego enforcement[73] or otherwise to manage the "day-to-day" implementation of regulation.[74] Indeed, "nearly unfettered discretion" is "the hallmark of many executive decisions."[75] The deployment of algorithmic technologies will make such evaluation yet more difficult. Those against whom enforcement is initiated typically (if not inevitably[76]) will also lack an evidentiary basis to complain about being unfairly singled out on due process or equality grounds. Litigation challenging AFST's equality-related or due process concerns, in short, faces an uphill battle.

2. Machine Learning and the Allocative State

Machine learning tools can be used in the allocation or withdrawal of individualized benefits such as employment or financial aid.[77] In the early 2000s, states such began moving to automate the distribution of public benefit systems in the context of a larger movement to eliminate recipients from welfare.[78] Michigan, for example, introduced an algorithmic tool to detect fraudulent applications for unemployment benefits as part of a larger overhaul of the information technology by the state.[79] Since then, states have increasingly relied on algorithmic tools to allocate both public benefits and state employment.[80] Legal challenges to the substitution of algorithmic for human decision-making in these domains tend to focus on the procedural adequacy of the machine decisions.[80a] In particular, plaintiffs underscore the risk of erroneous deprivations. Although less attention is given to equality or privacy concerns, they too may be present. Two examples illustrate how such tools are used, and how they are now being challenged in court.

A first example comes from 2016, when the state of Arkansas adopted an algorithm developed by a company called InterRAI to calculate disability benefits.[80b] The InterRAI algorithm was not

---

[73] Heckler v. Chaney, 470 U.S. 821, 832-33 (1985).
[74] Norton v. S. Utah Wilderness All., 542 U.S. 55, 64, 66–67 (2004).
[75] Mariano-Florentino Cuellar, *Auditing Executive Discretion*, 82 NOTRE DAME L. REV. 227, 229–30 & n.2 (2006); *accord* Rachel E. Barkow, *Overseeing Agency Enforcement*, 84 GEO. WASH. L. REV. 1129, 1131 (2016) ("Most aspects of agency enforcement policy generally escape judicial review.").
[76] It is not impossible to imagine complaints about political targeting, such as those levelled against the Internal Revenue Service (perhaps unfairly) from 2014 onward. Alan Rappeport, *In Targeting Political Groups, IRS Crossed Partisan Lines*, N.Y. TIMES, Oct 5, 2017. Similarly, if a municipality relied on public complaints about restaurants to drive the allocation of enforcement resources, it would also risk potentially biased enforcement patterns. Kristen M. Altenburger and Daniel E. Ho, *When algorithms import private bias into public enforcement: The promise and limitations of statistical de-biasing solutions*, -- J INST'L & THEO. ECON. --, at 4–5 (forthcoming 2019).
[77] *See* Esther Shein, *The dangers of automating social programs*, 61 COMM. ACM 17, 17 (2018) (describing machine learning tools used for Medicaid allocation).
[78] EUBANKS, *supra* note 65, at 45-51 (noting that automation resulted in a 54 percent increase in denials of food stamps, Medicaid, and cash benefits).
[79] Robert N. Charette, *Michigan's MiDAS Unemployment System: Algorithm Alchemy Created Lead, Not Gold*, IEEE SPECTRUM, Jan. 24, 2018, https://spectrum.ieee.org/riskfactor/computing/software/michigans-midas-unemployment-system-algorithm-alchemy-that-created-lead-not-gold [https://perma.cc/ZLZ9-T29S].
[80] Matt Leonard, *Government leans into machine learning*, GCN. Aug 19, 2018, https://gcn.com/articles/2018/08/17/machine-learning.aspx [https://perma.cc/5JBY-NJQF].
[80a] *See, e.g.*, Houston Fed'n of Teachers, Local 2415 v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1176–77 (S.D. Tex. 2017) (arguing that the machine-learning tool used to evaluate, and potentially terminate, teachers violated procedural due process).
[80b] Lecher, *supra* note 13.

developed using machine learning methods. Rather, InterRAI is a clinical assessment tool[81] that relies on about sixty "descriptions, symptoms, and ailments" to determine the quanta of home-care provision.[82] (I include it here because it usefully illustrates the kind of challenges that more sophisticated tools might face). According to the suit filed by Legal Aid of Arkansas challenging the InterRAI algorithm on state administrative law grounds, the instrument gave "no weight" to the beneficiary's physician's input.[83] The Supreme Court of Arkansas enjoined the instrument's use on the ground that it had been implemented in violation of the state's administrative procedures act without sufficient notice and comment.[84] One of the points raised in the litigation was the possibility that the InterRAI tool was brittle in the face of subtle or unusual variations in the way symptoms presented in a particular case.[84a] For instance, entering different evaluations of "foot problems" produced "wildly different scores when the same people were assessed, despite being in the same condition.[85] Similar concerns have been raised for the algorithmic determinations of Medicaid eligibility.[86] In the machine-learning context, the existence of brittleness raises questions about the external validity of the classifier learned from training data.[87]

A second domain in which large pools of government data have been exploited to power algorithmic determinations about specific individuals concerns the hiring and retention of public school teachers. Again, this practice is illuminated by litigation. In 2010, the Houston Independent School District moved to "data-driven" teacher evaluation.[87a] It adopted the Educational Value-Added Assessment System (EVAAS).[88] EVAAS evaluates teachers by comparing their students' average test score gains with statewide average gains to compute a "Teacher Gain Index."[89] A teachers' union, however, persuaded a district court judge that due process was violated when a teacher was fired for a low EVAAS score.[89a] It was impossible, the union argued, for teachers to replicate their scores, even with access to the algorithm's underlying code.[89b] Yet that score "might be erroneously calculated for any number of reasons."[90] The School District settled the union's suit by disbursing backpay and discontinuing EVAAS's use.[91]

---

[81] It is described in more detail in Brant E. Fries et al., *A screening system for Michigan's home-and community-based long-term care programs*, 42 GERONTOLOGIST 462, 467 (2002).
[82] Lecher, *supra* note 13.
[83] Compl. in *Ledgerwood v. Arkansas Dep't of Hum. Servs.*, No. --. Jan. 26, 2017, at 33, available at https://arktimes.com/arkansas-blog/2017/01/27/legal-aid-sues-dhs-again-over-algorithm-denial-of-benefits-to-disabled-update-with-dhs-comment [https://perma.cc/HQ7Q-WHVB].
[84] Arkansas Dep't of Human Servs. v. Ledgerwood, 2017 Ark. 308, at 11–14, 530 S.W.3d 336, 344–45 (2017).
[84a] Lecher, *supra* note 13.
[85] *Id.*
[86] *See* Shein, *supra* note 77, at 17.
[87] *See supra* text accompanying note 176 (discussing technical responses to the problem of overfitting).
[87a] Houston Fed'n of Teachers, Local 2415 v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1171 (S.D. Tex. 2017).
[88] *Id.* at 1172 (internal quotation marks omitted).
[89] *Id.* (internal quotation marks omitted).
[89a] *See id.* at 1180.
[89b] *Id.* at 1177.
[90] *Id.*
[91] Ian Sample, *Computer says No: why making AIs fair, accountable and transparent is crucial*, THE GUARDIAN, Nov. 5, 2017, https://www.theguardian.com/science/2017/nov/05/computer-says-no-why-making-ais-fair-accountable-and-transparent-is-crucial [https://perma.cc/QB68-SNT5].

Houston, however, is not alone in reaching for algorithmic solutions in the hiring context. In 2015, the Atlanta Public Schools retained the HireVue company to facilitate teacher hiring.[91a] HireVue offers deep-learning tools to extrapolate job performance from facial features and interview performance from on-line video interviews.[92] HireVue's materials do not disclose how applicants are evaluated, but their descriptive is consistent with the use of affect detection software.[93] Nor is it clear whether the Atlanta school district (or other public authorities) is using HireVue's video capture functionality alone, or its suite of predictive tools too.[93a]

Other challengers to algorithmic allocations of state benefits have also turned to due process arguments. In Indiana, for example, the automated rejection of a benefit application was successfully challenged in 2012 on the due process ground that the system provided recipients with insufficient information concerning the basis deprivations of benefits.[94] In Michigan, the automated system for flagging fraudulent unemployment benefit applications was challenged on the ground that the system "provide[d] no notice of the allegations brought against them, and that this lack of notice, among other systemic problems, deprives claimants of a fair hearing."[95] In contrast, I have not been able to find examples of challenges to algorithmic allocation systems based on equality or privacy concerns. This may be because due process claims are easier to allege. They require information about how decisions appear to be made, and not how different groups experience classification decisions or how data is handled in a back-office context. Alternatively, the gap might be because of the historical origins of procedural due process in challenges to the allocation and withdrawal of welfare benefits.[96] This means due process challenges are more readily imagined than equality or privacy ones.

Nevertheless, the racial or privacy effects of benefit distributions may well also be real.[97] To see why, consider work by Khiara Bridges on the intersection of informational privacy and the welfare regime for poor mothers. Bridges' analysis does not concern computational decision tools *per se* but nonetheless illuminates the possibility of important yet unaddressed normative questions arising from the use of algorithms to allocate public benefits.[97a] She underscores the extent to which state aid to

---

[91a] *Atlanta Public Schools Hires A+ Teachers with HireVue*, 2017, https://www.hirevue.com/customers/atlanta-public-schools-fills-vacancies-teacher-recruitment-software [https://perma.cc/BH9B-6EJ3] [hereinafter *HireVue Hires Teachers*].

[92] *Hirevue Video Interview Software*, HIREVUE, https://www.hirevue.com/products/video-interviewing [https://perma.cc/XAT5-L877] (last visited Mar. 3, 2020); Loren Larsen, *HireVue Assessments and Preventing Algorithmic Bias*, HIREVUE (June 21, 2018), https://www.hirevue.com/blog/hirevue-assessments-and-preventing-algorithmic-bias [https://perma.cc/JQB3-UX5Y]. The HireVue site does not disclose what kind of machine learning tool the company uses. *See HireVue Video Interview Software*, *supra* note 92. But the general description fits the use of deep learning to track elements of facial motion, and thereby to create composite scores for various kinds of affect. How this relates to teacher quality is an unexplored question.

[93] *See infra* text accompanying notes 86 to 87 (discussing this possibility).

[93a] *See HireVue Hires Teachers*, *supra* note 91a.

[94] Perdue v. Gargano, 964 N.E.2d 825, 832 (Ind. 2012) (finding that "due process requires a more detailed explanation of the reasons underlying an adverse determination").

[95] Zynda v. Arwood, 175 F. Supp. 3d 791, 799 (E.D. Mich. 2016).

[96] Maggie McKinley, *Petitioning and the Making of the Administrative State*, 127 YALE L.J. 1538, 1624 (2018) ("In a series of cases in the 1970s, litigated largely in the context of public benefits, the Court developed a test for administrative due process . . . .").

[97] In May 2019, the Illinois General Legislature passed the Artificial Intelligence Video Intelligence Act. *See* IL: HB 2557, https://www.billtrack50.com/BillDetail/1067171 [https://www.billtrack50.com/BillDetail/1067171]. The measure, which the governor signed into law in August 2019, imposes notice and consent rules on the use of such tools, and also allows applicants to request that their video interviews be destroyed within thirty days of the interview. The act would also limit the sharing of such videos.

[97a] *See* KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 5–6, 8–11 (2017).

poor mothers is conditioned on the disclosure of a good deal of personal information about a mother's behavior and her social context.[98] This deprivation of privacy, Bridges contends, cannot be explained by a concern about the health or well-being of either mother or child. She instead reasons that it "would not even be attempted without the baseline supposition about the group to which she belongs."[99] Bridges' analysis resonates with a longer line of sociological and political science work emphasizing how racial stereotypes have tended to shape welfare policy.[100] But the normative concerns she raises may become increasing relevant in the algorithmic context. The public entities that collect information used for algorithmic allocation of benefits, for example, may be more vulnerable to data breaches than private entities such as commercial banks.[101] This would mean that an increasingly reliance on those tools for benefit allocations will likely shift more data-breach risk to the indigent.[102] Machine learning's adoption would then have a regressive and racially disparate economic impact as well as imposing a burden upon privacy rights.

3. Machine Learning and the Punitive State: Facial Recognition as a Case Study

The third domain in which machine learning is increasingly used involves the provision of public security through policing, incarceration, and (in the most extreme cases) force. There is already a large body of literature on how machine learning is deployed in policing,[103] bail and arraignment proceedings,[104] and sentencing.[105] This literature depicts how machine learning tools and other algorithms are used to generate predictions of future violence or criminality. Location-based predictions, such as those generated by policing applications like PredPol, are used to allocate investigative resources.[106] Other predictions can focus on specific individuals. The COMPAS algorithm, for instance, is used in many jurisdictions to facilitate bail determinations by generating a

---

[98] *Id.* at 1-5.

[99] *Id.* at 149.

[100] *See* MARTIN GILENS, WHY AMERICANS HATE WELFARE: RACE, MEDIA, AND THE POLITICS OF ANTIPOVERTY POLICY 102 (1999) (describing the racialization of opposition to welfare spending, which has "reflected a preexisting stereotype of blacks as lazy").

[101] Danielle Keats Citron, *A Poor Mother's Right to Privacy: A Review*, 98 B.U. L. REV. 1139, 1147 (2018) ("A common source of data breaches involves public hospitals where the personal data of poor mothers is collected and stored.").

[102] To be clear, this theory has not been tested empirically: I raise it here as a possibility to be evaluated through regulation or litigation.

[103] *See, e.g.,* Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109, 1120–44 (2017) (providing a careful catalogue of predictive policing tools); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 383–85 (2015) (similar); *see also* Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 929 (2016) (developing a "framework" for integrating machine-learning technologies into Fourth Amendment analysis).

[104] Richard A. Berk, Susan B. Sorenson & Geoffrey Barnes, *Forecasting Domestic Violence: A Machine Learning Approach To Help Inform Arraignment Decisions*, 13 J. EMPIRICAL LEGAL STUD. 94, 110 (2016) (reporting experimental results suggesting gains from machine learning prediction of violence risk); Richard Berk & Jonathan Hyatt, *Machine Learning Forecasts of Risk to Inform Sentencing Discretion*, 27 FED. SENT'G REP. 222, 223 (2015) (explaining advantages of machine-learning tools); Richard F. Lowden, *Risk Assessment Algorithms: The Answer to an Inequitable Bail System?*, 19 N.C. J.L. & TECH. 221, 230–31 (2018) (listing jurisdictions that have adopted algorithmic tools).

[105] Richard Berk, *An Impact Assessment of Machine Learning Risk Forecasts on Parole Board Decisions and Recidivism*, 13 J. EXPERIMENTAL CRIMINOLOGY 193, 195 (2017) (discussing the 2010 decision of the Pennsylvania Board of Probation and Parole to use a machine-learning protocol to generate forecasts of recidivism); *see generally* John Monahan & Jennifer L. Skeem, *Risk Assessment in Criminal Sentencing*, 12 ANN. REV. CLINICAL PSYCHOL. 489, 493–95 (2016) (describing the general context of risk assessment in sentencing).

[106] Aaron Shapiro, *Reform Predictive Policing*, 541 NATURE 458, 459 (2017) .

risk score from one to ten for defendants, a score that provides guidance to a magistrate charged with setting or denying bail.[107]

Rather than retread details of predictive policing and bail algorithms that have been well covered elsewhere, I focus here on a new frontier in the law enforcement deployment of machine learning. This is use of facial recognition technologies to identify individuals from public surveillance and body-camera footage.[108] Facial recognition technologies provide a useful case study of the complex and unpredictable ways that norms of procedural fairness, equality, and privacy interact when the state deploys machine learning tools to draw inferences from otherwise unilluminating data.

Roughly half of all American adults are already profiled in one or another American law-enforcement agencies' facial-recognition database.[109] These can be used to match with visual evidence in specific cases and make arrests.[110] More controversially, they can be used to identify participants of protests against government policies.[111] The rate of its adoption is uncertain. In May 2018, Axon—one of the largest manufacturers of body-worn cameras in the United States—secured a patent on real-time identification of faces caught on an officer's body-worn camera[112] Then in June 2019, the company announced that it was not installing the tool because of reliability concerns.[113] For now, individualized facial-recognition results may not reach officers at a time and in a manner that permits them to act upon the data. But this equilibrium is unlikely to hold.

Facial recognition raises interrelated privacy, procedural fairness, and equality concerns. Consider a much-noted 2015 study using eight facial traits to identify specific persons.[113a] Finding no duplicates among a sample of 3982 facial images provided by the U.S. Army, it favorably compared

---

[107] EQUIVANT, PRACTITIONERS GUIDE TO COMPAS CORE 1–2, 8 (2017), http://www.equivant.com/assets/img/content/Practitioners_Guide_COMPASCore_121917.pdf [https://perma.cc/7ML8-NC9U]; *see also In re* Hawthorne v. Stanford, 22 N.Y.S. 3d 640, 641–42 (N.Y. App. Div. 2016) (describing the COMPAS assessment tool).

[108] Dakin Andone, *Police Used Facial Recognition to Identify the Capital Gazette Shooter. Here's How It Works*, CNN (June 29, 2018), https://www.cnn.com/2018/06/29/us/facial-recognition-technology-law-enforcement/index.html [https://perma.cc/HL2R-487J].

[109] Clare Garvie et al., Geo. L. Ctr. on Privacy & Tech., *The Perpetual Line-Up: Unregulated Police Face Recognition in America* 1 (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%C20Privacy%C20and%C20Technology% 20at%20Georgetown%C20Law%20-%20121616.pdf [https://perma.cc/EK75-6HRG]; *see also* Jennifer Lynch, Electronic Frontier Foundation, *Face Off: Law Enforcement Use of Face Recognition Technology* 1–2 (2018), https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf [https://perma.cc/4JDQ-CC2M] (noting one in two Americans are already in a face recognition database accessible to law enforcement).

[110] *See, e.g.,* State v. Alvarez, No. A-5587-13T2, 2015 N.J. Super. LEXIS 1024, at *1–*2 (N.J. Super. Ct. App. Div. May 4, 2015) (searching every image in the state's repository to determine if individuals were maintaining more than one identification document).

[111] *See, e.g.,* Kevin Rector & Alison Knezevich, *Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates*, BALT. SUN, Oct. 18, 2016, https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html [https://perma.cc/U5ER-SC3E] (noting that Maryland's image repository was used to monitor protestors during Baltimore protests).

[112] Alex Pasternack, *Body Camera Maker Will Let Cops Live-Stream Their Encounters*, Fast Company (Oct. 8, 2018), https://www.fastcompany.com/90472869/why-tim-ferriss-focus-on-daily-habits-is-not-the-real-secret-to-success [https://perma.cc/845M-D4KG].

[113] Chris Warzel, *A Major Police Body Cam maker Just Banned Facial Recognition*, N.Y. TIMES, June 28, 2019, https://www.nytimes.com/2019/06/27/opinion/police-cam-facial-recognition.html [https://perma.cc/8MBF-A7L7].

[113a] Teghan Lucas & Maciej Henneberg, *Are human faces unique? A metric approach to finding single individuals without duplicates in large samples*, 257 FORENSIC SCI. INT'L 514, 514.e5 (2015).

the accuracy of facial recognition to that of DNA matching.[114] A 2019 paper, however, observed that this result rested on untested assumption about the statistical distribution of certain parameter values for those traits.[114a] It doubted the external validity of the 2015 study. The latter, for instance, assumed that human faces are static. But "ageing, illness, tiredness, the expressions we're pulling or how our faces are distorted by a camera angle" all can change the values of the eight facial traits.[115] Even if facial recognition were accurate under ideal conditions, police deploy it under non-ideal conditions. They also use it in creative ways. Hence, in New York City, when officers had a partial surveillance shot of a face from a pharmacy larceny, they used a high-quality video image of the actor Woody Harrelson to find matches on the theory that the partial image from the surveillance video looked like Harrelson.[116]

Patterns of error rates in lab-based facial recognition systems are also asymmetrical across racial, gender, and age lines. This is a consequence of using predominantly older, more male and whiter exemplars in training data. One 2018 study of two commercially available facial-recognition tools IJB-A and Adience, for example, found that both were trained with predominantly white subjects, and had errors rates for black women that were 34.7 percent higher than for white men.[117] In respect to privacy, there is little regulation under federal or state law of the inferences police draw from facial images. There is some evidence that facial images allow for "category jumping" inferences about health. For instance, they may enable predictions of postpartum depression from expectant mothers' prenatal image postings.[118] A 2016 study by two Chinese researchers used a training set of 1,856 photos of convicted Chinese criminals to construct a predictive tool to distinguish two "manifolds" of "criminal" and "non-criminal" face types.[119] Their result was extensively criticized. Their small sample of training data, for example, made overfitting difficult to avoid.[120a] Many of their noncriminal faces (but none of the criminal faces) wore white collared shirts, introducing a likely confound. Nevertheless, it is not far-fetched to envisage police forces generating "criminal type" lists based on such uses of facial recognition tools—much as they have tried to use social network (unavailingly) to create "strategic subject lists" of likely future criminals.[120]

---

[114] *Id.* at 514.e2, e6.

[114a] Ronald Meester, Bart Preneel, and Sylvia Wenmackers, *Reply to Lucas & Henneberg: Are human faces unique?*, 297 FORENSIC SCI. INT'L 217, 218-20 (2019).

[115] FRY, *supra* note 29, at 163.

[116] Claire Garvey, *Garbage in, Garbage out*, May 16, 2019, https://www.flawedfacedata.com/ [https://perma.cc/242U-YEP9].

[117] Joy Buolamwini & Timnit Gebru, *Gender shades: Intersectional accuracy disparities in commercial gender classification*, CONF. ON FAIRNESS, ACCOUNTABILITY & TRANSPARENCY 77, 77-78 (2018); *see also* Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 680 (2017) ("[A]lgorithms that include some type of machine learning can lead to discriminatory results if the algorithms are trained on historical examples that reflect past prejudice or implicit bias . . . ."); Kate Crawford, *Artificial Intelligence's White Guy Problem*, N.Y. TIMES (June 25, 2016), https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html [https://perma.cc/HJ2D-TUG4] (noting that sexism, racism, and other forms of discrimination are often built into machine-learning).

[118] Eric Horvitz & Deirdre Mulligan, *Data, privacy, and the greater good*, 349 SCIENCE 253, 253-54 (2015).

[119] Xiaolin Wu and Xi Zhang, *Automated inference on criminality using face images.* ARXIV PREPRINT ARXIV:1611.04135, at 4038 (2016).

[120a] Agüera y Arcas et al., *supra* note 37.

[120] *See* Jeremy Gorner, *Chicago Police Use 'Heat List' As Strategy to Prevent Violence*, CHI. TRIB. (Aug. 21, 2013), http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_ chicago-police-commander-andrew-papachristos-heat-list [https://perma.cc/DE7Y-Q4LX]. The Chicago "heat list," however, proved to have little or no predictive value. Jessica Saunders, Priscilla Hunt & John S. Hollywood, *Predictions Put into Practice: A Quasi-Experimental Evaluation of Chicago's Predictive Policing Pilot*, 12 J. EXPERIMENTAL CRIMINOLOGY 347, 363 (2016).

There is little litigation testing the constitutional constraints on algorithmic decision-making in the criminal justice context.[121] The litigation that does exist focuses on due process questions, touches briefly on equality concerns, and largely ignores privacy values.[122] One reason for this is the absence of effective vehicles for raising legal challenges to machine learning instruments in the criminal justice context. When it comes to policing, for example, it would be difficult for an individual litigant to challenge the use of a machine-learning tool to allocate policing resources so long the legal basis for his or her encounter with the police was constitutionally sufficient.[123] In addition, systemic challenges filed as class actions to the allocation of policing resources over different geographic spaces are exceedingly rare.[124] Costly to investigate and litigate, they are likely to founder on questions of Article III standing and amenability to Rule 23 class-based resolution.

Some cases have arisen in the context of individualized risk evaluations in pretrial and sentencing. In 2016, for example, the Wisconsin Supreme Court rejected a Due Process challenge to the COMPAS algorithm based on the defendant's limited ability to challenge the algorithm in broad and general terms, rather than being able to scrutinize the individualized data upon which the algorithm relied in a specific instance.[125] The Court reasoned that the algorithm relied on publicly available data alone. It observed that the defendant could have denied or explained any information used to craft his prediction.[126] In passing, the Court noted that traits such as gender were among the large set of inputs to the defendant's sentence.[127] On their own, the Court cautioned, such factors "may not be considered as the determinative factor in deciding whether the offender can be supervised safely and effectively in the community" consistent with due process.[128]

While lawsuits challenging the use of facial recognition have not yet been lodged, regulatory response have already occurred. In May 2019, the San Francisco Board of Supervisors voted to

---

[121] One reason may be the successful exercise of trade secrets objections by the commercial manufacturers of algorithms. Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1349–53 (2018) (arguing that such trade secrets invocations pose a real problem, and contending that new transparency mechanisms are required). Many commonly used machine learning tools are, in fact, quite simple to program in a common language such as R. *See, e.g.,* UC Business Analytics Programming Guide, *Random Forests*, https://uc-r.github.io/random_forests [https://perma.cc/5J4Q-G9F5] (providing an introduction to random forests using R). Claims to the effect that the basic method (be it random forests, naïve Bayes, or even a neutral net) is somehow bespoke and hence worthy of trade secrets protection are probably bunk. What is more distinctive is the manner of regularization and empirical testing used to tweak the rule learned by the algorithm to avoid overfitting or achieve other ends. For example, a model might be adjusted to avoid predictions that correlate too closely with race or gender. It is hard to see why there is

[122] On the possibility of a Fifth Amendment challenge to interviews designed to elicit information from a defendant for the purpose of assigning him or her an algorithmic classification, see Cassie Deskus, Note, *Fifth Amendment Limitations on Criminal Algorithmic Decision-Making*, 21 N.Y.U. J. LEGIS. & PUB. POL'Y 237, 259-66 (2018).

[123] Under Fourth Amendment doctrine, the availability of a legal justification for a police stop obviates any argument that it should be treated as unlawful because of the actual causes of or justifications for the stop. *See* Whren v. United States, 517 U.S. 806, 813 (1996) (rejecting "any argument that the constitutional reasonableness of traffic stops depends on the actual motivations of the individual officers").

[124] For a rare exception, see Cent. Austin Neighborhood Ass'n v. City of Chicago, 2013 Il App. (1st) 123041, ¶ 1, 25 (Nov. 13, 2013) (challenging the failure to provide resources to minority neighborhoods in Chicago).

[125] State v. Loomis, 881 N.W.2d 749 (2016).

[126] *Id.* at 761-62.

[127] *Id.* at 765 ("[T]he due process implications compel us to caution circuit courts that 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.").

[128] *Id.* at 760.

prohibit police adoption or implementation of facial recognition technologies.[129] A raft of other cities, including New York, Las Vegas, Detroit, Boston and Orlando, have however embraced the technology. They show no sign of willingness to abandon it. New York City has enacted an ordinance creating an expert board to monitor and make recommendations about how algorithmic technologies are to be deployed.[132a] It remains to seen how such a body would operate, and whether it be able to take on a powerful interest group such as the police.

The Wisconsin decision, like the Arkansas challenge to disability allocation algorithms and the Houston challenge to teacher evaluations, turned almost exclusively on procedural concerns. Yet even as a contentious literature has emerged analyzing the role of race in the COMPAS algorithm,[130] to date there has been no litigation explicitly challenging those effects. Similarly, there is a dearth of either academic or judicial treatment of the privacy-related risks from the creation of large aggregates of data for public security purposes. Still, even if police forces have more resources at their disposal than (say) public hospitals, there is no reason to think that they will be inured to the risk of data breaches.

* * *

Machine learning tools are rapidly diffusing across both civil and criminal regulatory domains. They are at the moment sporadically regulated. They consistently raise, however, a common cluster of procedural due process, equality, and privacy concerns. Courts and commentators have glimpsed these concerns. But judges to date have offered no coherent account of how they are interlaced, nor of how they can be identified, let alone mitigated.

II. Applying Constitutional Values in the Machine Learning State

Given the rapid and ongoing adoption of machine-learning technologies by federal and state authorities, how should constitutional interests be recalibrated to fit the new terrain fashioned by the machine learning state? This Part focuses on due process, equality, and privacy values, three constitutional norms are repeatedly implicated in the design and operation of predictive tools. It analyzes difficulties that arise in their application to the machine learning state.

A. Procedural Due Process

---

[129] Kate Conger, Richard Fausset and Serge F. Kovaleski, *San Francisco Moves to Ban Facial Recognition Technology*, N.Y. TIMES, May, 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html, [https://perma.cc/26AF-TUD8].

[132a] Local Law No. 49, N.Y. City Council https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0 [https://perma.cc/D68B-JMMG] (creating a task force charged with investigating "agency automated decision systems").

[130] *See* Huq, *Racial Equity*, *supra* note 9, at 1115-23 (discussing different definitions of racial disparities in algorithmic classification, and suggesting why a definition focused on the potential for stratifying effects is most desirable). For a different analysis, albeit one that is critical of COMPAS in a different way, see Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/6L7T-ELPG].

A common complaint lodged in court against machine-learning instruments is their failure to give regulated subjects procedural due process.[131] Anecdotal accounts abound of individuals who have been wrongly classified by an algorithm, when the error could have been quickly and easily fixed by human attention. In an influential treatment, for example, data scientist Cathy O'Neill describes an applicant for a welfare benefit who fails an automated, "web-crawling[,] data-gathering" background check.[132] It is only when "one conscientious human being" takes the trouble to look into the quality of this machine result that error is discovered and corrected.[133] The implication is that machines are prone to error, and that a hearing of sorts before a human adjudicator is a necessary adjust to any algorithmically driven process.

A granular focus on error in the isolated case, however, is an untrustworthy analytic vehicle for the purposes of due process analysis. I shall argue instead that due process is violated when an algorithm fails to achieve an adequate level of accuracy across the population of regulated cases. Due process concerns hence arise from the calibration of design margins in ways that make relevant errors more rather than less likely. A constitutional analysis must therefore focus upon algorithmic design choices remote in time from the instant in which a human is subject to algorithmic classification. Remedies for a due process deficit are unlikely to take the form of additional human review, but rather better algorithmic design. I identify a number of relevant design margins in this spirit. I also emphasize that it is not always possible to eliminate equally false negatives and false positives. A choice, rather, must be made about which to endure. Due process in the algorithmic context—where it is possible to precisely specify ex ante the balance and kind of errors—thus entails normative judgments about the relative cost of different sorts of errors. Although those judgments are implicitly embedded in human decision-making process, they can be isolated and addressed with greater precision in the machine decision context.

1. Procedural Due Process Norms

The doctrinally dominant model of procedural due process is narrowly "utilitarian" in its focus on "attaining the most accurate conclusion in the most efficient manner."[134] 'Accuracy,' in the due process context, can be understood to mean a correlation between a decision procedures outcomes and some empirical ground truth.[135] Alternative conceptions hinging on dignity and the intrinsic value

---

131 Due process concerns are central in several cases. *See, e.g.,* Houston Fed'n of Teachers, Local 2415 v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1171 (S.D. Tex. 2017) (arguing that the teacher evaluation algorithm deprived teachers of due process protections against substantively unfair depravations of property); State v. Loomis, 881 N.W.2d 749, 760 (2016) (arguing that COMPAS risk assessment violated the defendant's right to be sentenced based on accurate information). The challenge to Arkansas's automated disability determinations sounds in state administrative law, but relied on a notice concern familiar to due process jurisprudence. Arkansas Dep't of Human Servs. v. Ledgerwood, 2017 Ark. 308, 10, 530 S.W.3d 336, 344 (2017).

132 CATHY O'NEILL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 152-53 (2016).

133 *Id.* at 153.

134 Martin H. Redish, *Discovery Cost Allocation, Due Process, and the Constitution's Role in Civil Litigation*, 71 VAND. L. REV. 1847, 1863–64 (2018).

135 An alternative conception of accuracy would focus on the expression of confidence (uncertainty) in classifications. *See* Robert J. MacCoun, *The epistemic contract: Fostering an appropriate level of public trust in experts*, in MOTIVATING COOPERATION AND COMPLIANCE WITH AUTHORITY 191, 201–02 (Brian H. Bornstein & Alan J. Tomkins, eds. 2015). Although I do not purpose MacCoun's proposal at length, I do later explain how uncertainty and accuracy interact in a functionally important way. *See infra* text accompanying notes 176 to 160 (discussing the bias/variance trade-off).

of participation have not gained doctrinal purchase.[136] This instrumental, accuracy-focused account of due process crystallized in the famous three-part test announced in *Mathews v. Eldridge*.[137] The Court here directed attention to "the private interest . . . ; second, the risk of an erroneous deprivation of such interest . . . , and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail."[138] These factors are properly considered by looking at an adjudicative mechanisms as a whole rather than at the specifics of a single case. In this sense, due process challenges commonly have the flavor of a facial challenge.

In application, the *Mathews* test relies on difficult, perhaps irremediably hard, counterfactual questions about the state's election between potential alternative institutional arrangements, private individuals' behavior under alternative adjudicatory arrangements, and the expected gains to accuracy from marginal changes to those arrangements.[139] Its categorical exclusion of noninstrumental considerations from due process analysis has also been controversial. But the test has remained good law for almost fifty years. It can logically be applied in new contexts, including machine learning contexts. Indeed, I will suggest that the holistic *Mathews* test may well be easier to apply in the latter context than in many of the institutional domains in which it previously been wielded.

2. Application to Machine Learning

Scholarship concerned with the procedural quality of algorithmic decision-making have read *Mathews* to demand that specific notice be given to regulated subjects and that an individualized determination, often involving a human adjudicator, be available. In an early analysis, Danielle Keats Citron argued that constitutionally adequate notice is supplied by an audit trail documenting all "decisions made in a case" and "the actual rule[] applied in every mini-decision that the system makes."[140] Developing the idea of a hearing right, Citron focused on scenarios in which a human adjudicator is supplied with an algorithmic recommendation, and recommended that "agencies should require hearing officers to explain, in detail, their reliance on an automated system's decision."[141] This assumes the availability of human intervention after an instrument has been applied to a specific case. In a similar vein, Kate Crawford and Jason Schultz have pressed for "procedural data due process [to] regulate the fairness of Big Data's analytical processes with regard to how they use personal data (or metadata . . .)."[142] Like Citron, they seemed to conceptualize the entailment of due process in granular, individualistic terms. Notice, on their view, entails disclosure of the "type of prediction" and "the

---

[136] The dignity rationale is vigorously defended in scholarship. *See, e.g.,* Martin H. Redish & Lawrence C. Marshall, *Adjudicatory Independence and the Values of Procedural Due Process*, 95 YALE L.J. 455, 504 (1986) (advocating for an independent adjudicator to protect procedural due process); Jerry L. Mashaw, *Administrative Due Process: The Quest for a Dignitary Theory*, 61 B.U. L. REV. 885, 899 (1981) (advancing a dignitary theory of due process); Frank I. Michelman, *Formal and Associational Aims in Procedural Due Process*, *in* DUE PROCESS: NOMOS XVIII, at 126, 127-28 (J. Roland Pennock & John W. Chapman eds., 1977) (underscoring participation values as an element of due process).

[137] 424 U.S. 319, 335 (1976).

[138] *Id.*

[139] Jerry L. Mashaw, *The Supreme Court's Due Process Calculus for Administrative Adjudication in* Mathews v. Eldridge*: Three Factors in Search of a Theory of Value*, 44 U. CHI. L. REV. 28, 46–51 (1976) [hereinafter "Mashaw, *Due Process Calculus"*] (offering these critiques in a somewhat looser formulation).

[140] Danielle Keats Citron, *Technological Due Process*, 85 WASH. U.L. REV. 1249, 1305-06 (2008) [hereinafter "Citron, *Technological Due Process*"].

[141] *Id.* at 1307; *cf. id.* at 1284 (rejecting the idea that due process would require access to source code).

[142] Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward A Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 109 (2014).

general sources of data" used in the algorithm.[143] They too would require a hearing, in which an affected person could examine the "data input and the algorithmic logic applied," and then appeal to a "neutral data arbiter" (presumably a human rather than another machine) to resolve disputes about the quality of analysis and prediction.[144] It is not clear whether Crawford and Schultz think that due process requires disclosure of (1) the data used in the training and generation of the learned rule, or (2) the data about the regulated subject used to make a prediction or classification. Finally, Cary Coglianese and David Lehr explicated notice by recommending that individuals receive information "collected about them" and "information about how accurate the algorithm is across individuals when evaluated in a test data set."[145]

The focus of these proposals upon a human appeal of individual cases may, however, miss the best way to vindicate due process interests for a number of reasons. First, as David Lehr and Paul Ohm explain, there are "many ways in which data can be selected and shaped — say, during data cleaning or model training"—that undermine the quality of predictions.[146] Deviations from a tolerably accurate pattern of predictions can result from the design of the training data, the outcome variable selection, or the choice of algorithmic instrument.[147] The individualized hearing model, however, is not well suited to the identification of such systemic problems. Providing an *individualized* hearing right to all regulated subjects is a good way of providing attention to whether a particular person has been correctly classified. Litigants will not necessarily have incentives, however, to uncover systemic problems (as opposed to highlighting errors in their case). Their retail challenges are not necessarily a good way to determine whether there is a problem are inaccuracy-generating flaws in an algorithmic decision-making process.[148] Indeed, the fact that there is error in the individual case before an adjudicator is not necessarily proof of a systemic design problem. And once systemic flaws are rooted out, individualized hearings may be an unnecessary cost.

Second, a common assumption of these proposals is that adding human appeals reduces overall rates of false positives and false negatives. But I have argued elsewhere that it is problematic to assume that human decision-making is generally more accurate than machine classification, or that adding a human appeal to a machine decision will reduce error rates.[149] Writing in 1954, the psychologist Paul Meehle compared statistical prediction tools with clinical judgments by trained specialists, and came to the conclusion (even then) that structured decision-making was better than either humans acting alone or statistical prediction coupled to human review.[150] Recent studies also suggest that adding human oversight to structured (algorithmic decisions) will not always reduce the net volume of false positives and false negatives, and instead will often have undesirable, even

---

[143] *Id.* at 125.
[144] *Id.* at 127.
[145] Coglianese & Lehr, *Transparency and Algorithmic Governance*, *supra* note 63, at 41.
[146] Lehr & Ohm, *supra* note 39, at 656.
[147] *See, e.g.,* Altenburger & Ho, *supra* note 64, at 99-100 (exploring how bias in training data can be minimized by the choice of appropriate computational architecture).
[148] It is not impossible for individualized hearings to provide a vehicle for reviewing systemic problems. But
[149] Aziz Z. Huq, *A Right to a Human Decision*, 105 VA. L. REV. (forthcoming 2020), https://ssrn.com/abstract=3382521 [https://perma.cc/G7F8-ZWZC] [hereinafter "Huq, *Human Decision*"]; *accord* Sharad Goel et al., *The Accuracy, Equity, and Jurisprudence of Criminal Risk Assessment* 3 (Dec. 2018) (on file with author) (summarizing evidence that additional process can have aggregate negative effects on accuracy).
[150] PAUL E. MEEHL, CLINICAL VERSUS STATISTICAL PREDICTION: A THEORETICAL ANALYSIS AND A REVIEW OF THE EVIDENCE 119–120, 136–138 (1954) (predicting that mechanical predictive methods would outperform clinical ones).

perverse, effects.[151] While the possibility of a system that successfully integrated post hoc human oversight with machine decisions cannot be ruled out categorically, current proposals that focus on a 'hearing officer' are more likely to exacerbate, rather than resolve this due process concern.

3. Testing Algorithmic Design Against Due Process Norms

In the spirit of Crawford and Schultz, I would focus due process analysis on systemic design choices. They, however, provide insufficient detail of how design might compromise due process, and how to go about identifying problematic design features. To start filling that gap, I explore here five distinct due process problems that can arise through algorithmic design. All hinge on systemic properties of the machine learning tool.

First, an algorithm might be trained on data that is incomplete, biased, or flawed because of the way that it has been created, selected, or cleaned.[152] Training data produced by state enforcement agencies, such as police or child welfare services, might be shaped by the implicit or explicit bias either of officials or those who provide leads.[153] The result may be an excessive representation of some groups (e.g., racial minorities), not as a consequence of higher misbehavior rates but rather because of the greater propensity of others to report or investigate them. Alternatively, training data might have "black holes" as a consequence of the state's failure to enforce the law in certain locations or against certain populations.[154] Again, the predictable consequences of such flaws is the deviation of predictions from whatever latent construct (e.g., criminality; the risk of benefit ineligibility; or the probability of child abuse) that is the intended object of state intervention. Due process requires at a minimum that an algorithm's designer avoid the unnecessary use of flawed data-sets and, where appropriate, take active steps to mitigate training data flaws.[155]

---

[151] Thomas H. Cohen, Bailey Pendergast, & Scott W. Van Benschoten, *Examining Overrides of Risk Classifications for Offenders on Federal Supervision*, 80 FED. PROBATION 12, 20–21 (2016); R. Karl Hanson & Kelly E. Morton-Bourgon, *The Characteristics of Persistent Sexual Offenders: A Meta-Analysis of Recidivism Studies*, 73 J. CONSULTING & CLINICAL PSYCHOL. 1154, 1154-56, 1159 (2005).

[152] *See* ALPAYDIN, *supra* note 32, at 40 (describing the use of training and validation data in algorithm design); Michael Mattioli, *Disclosing Big Data*, 99 MINN. L. REV. 535, 561 (2014) (arguing that databases contain errors because of their "sheer size[;] . . . the automatic and indiscriminate information-gathering that is a hallmark of the big data method[; and] . . . errors [that] manifest when error-free data from different sources is merged").

[153] A further problem is that "race is such a dominant category in the cognitive field that the 'interim solution' [of using race as a proxy for some other trait of interest] can leave its own indelible mark." Troy Duster, *Race and Reification in Science*, 307 SCIENCE 1050, 1050 (2005). This means that race might well structure the past deployment of state resources, or patterns of private behavior, in ways that are hard to disentangle from readily available training data.

[154] Kate Crawford, *The Anxieties of Big Data*, NEW INQUIRY (May 30, 2014), https://thenewinquiry.com/the-anxieties-of-big-data [https://perma.cc/25L7-4XUM].

[155] Imagine that an algorithm is accurate for a majority of a regulated population, but errs at very high rate for a specific subgroup. Imagine further that this subgroup is not a protected class, defined by race or class. Can members of the non-suspect class thereby created complain of a due process violation? *Cf.* Ian Ayres, *Outcome Tests of Racial Disparities in Police Practices*, 4 JUST. RES. & POL'Y 131, 139 (2002) (describing this problem). Whether this presents a constitutional problem depends on how costly the subgroup error is to fix for the balance of the population. Where the error cannot be mitigated without introducing greater rates of error elsewhere, for example, due process would not be compromised. But it is worth asking whether it would be minimally rational for the state to continue to use the algorithm in question against the subgroup if it is known that the tool is serially inaccurate. It may be, though, that the state could proffer a reason for not permitting an opt-out (e.g., membership in the subgroup us costly to determine ex ante, and hence it is cheaper to keep the subgroup in). I am grateful to Julian Nyarko for conversations on this point.

Second, an outcome variable may be poorly aligned with the underlying variable of interest, which is commonly termed the "latent construct."[156] For instance, the outcome variable may have been defined in terms of a feature that is not present in the original data. Risk assessment algorithms in the criminal justice space, for example, are designed to predict 'dangerousness'—a classification that is not present in the original data.[157] This synthetic classification, however, may not correlate well with the underlying outcome of interest for any number of reasons.[158] The institutional context in which an algorithm is deployed may also influence the fit between an outcome variable and the latent construct. Facial recognition tools are already used to match on police artists' composites.[159] But those composites are likely to be highly imperfect versions of the latent construct of interest, the face of the actual suspect. An algorithm that permits matching on artists' composites therefore introduces a stochastic element associated with a predictably high and racially asymmetrical error rate. Due process might be offended, more generally, by a poor choice of latent construct.

Third, an algorithm's designer might elect a model that is ill-fitted to the policy task at hand. One important election in this regard relates to the important bias/variance trade-off. Model choice, that is, influences a necessary and unavoidable trade-off between bias (how far predictions are from ground truth) and variance (in effect, how much a prediction would vary if the learner was trained on different data sets). There is some evidence that simpler models often performing better than more sophisticated ones because they yield less variance.[160] Depending on the policy context, different models may be desirable based on how they manage this trade-off. Where precision is less important than consistency as a policy matter, the bias-variance trade-off implies that a model with higher bias might be chosen with the expectation that it will produce a certain rate of errors. Simply examining error rates to condemn or endorse an algorithm without understanding how model choice pertains to policy functions, therefore, may lead a due process analysis astray.

Fourth, an algorithm may be trained on appropriate training data, may initially offer useful predictions on the ground, and may then confront cases that defy proper classification. Given the complex and evolving social circumstances in which algorithmic decision tools are likely to work, it is necessary to evaluate periodically an algorithm's performance to determine that its classifications continue to correspond to the latent variable. This concern may be what Coglianese and Lehr are getting at when they advocate for disclosure of an algorithm's accuracy "in a test data set."[161] But their concern can be profitably extended to consideration of how an algorithm performs over time on the ground.

---

[156] Lehr & Ohm, *supra* note 39, at 679 ("Measurements must be faithful not just to what a variable ostensibly indicates on its face, but also to what underlying construct (also called a latent construct) the data scientist believes it represents.").
[157] *Cf.* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 679 (2016) [hereafter "Barocas & Selbst, *Big Data's Disparate Impact*"] (discussing how algorithms measure creditworthiness, despite there being no direct way to measure creditworthiness).
[158] For an argument that "dangerousness" in criminal justice contexts is infected with ideas of race, Bernard E. Harcourt, *Risk as a proxy for race: The dangers of risk assessment*, 27 FED. SENT'G REP. 237, 237 (2014).
[159] Klum et al., *Sketch Based Face Recognition: Forensic v. Composite Sketches*, INT'L CONFERENCE ON BIOMETRICS 3 (2013), *available at* https://www.researchgate.net/publication/235701861_Sketch_Based_Face_Recognition_Forensic_vs_Composite_Sketches [https://perma.cc/69JM-UBZW].
[160] Pedro Domingos, *A unified bias-variance decomposition*, PROC. OF 17TH INT'L CONF. ON MACHINE LEARNING 231, 231 (June 2000); *see also* Lehr & Ohm, *supra* note 39, at 697-98 (discussing bias/variance trade-off in algorithmic design).
[161] Coglianese & Lehr, *Regulating by Robot*, *supra* note 11, at 1187.

Finally, there is a class of cases in which there is no outcome variable available that is well enough correlated to the underlying variable of interest. The algorithm's predictions, therefore, are irrational in the sense of lacking any logical relationship to a legitimate state interest.[162] The problem of irrationality in formal enactments and administrative action has generally been styled as an Equal Protection violation, rather than a Due Process concern.[163] However that problem is phrased, it is plausible to say that a constitutional violation is made out when an instrument's outcome variable has no plausible correlation to the underlying outcome of interest.[164]

Teacher evaluations and criminal risk assessments may be cases in point. There is substantial evidence that many available measures of teacher performance, especially student evaluations, are distorted by various improper biases,[165] or uncorrelated with measures of learning success.[166] Standardized test data, meanwhile, suffers from vulnerability to gamesmanship by other teachers. As a result, measures of teacher effectiveness based on such scores experience arbitrary fluctuations on a year-to-year basis.[167] Given this, an algorithm trained on either student evaluations or standardized test scores may well be per se invalidity on either due process of equal protection grounds. Or consider the HireVue tool, which may be in use by the Atlanta Public Schools to hire teachers.[168] Apparently, HireVue uses a facial data analytic tool developed by Affectiva, "a leading company in emotion recognition that works in market research and advertising."[169] Even setting aside the doubts that have been raised about the theoretical presuppositions of affect recognition,[170] it is not at all clear how affect, as detected in facial images, is meaningfully predictive of performance as a teacher. Such use of affect recognition in hiring is likely to raise a serious question of rationality that, at least in the public sector, has constitutional implications.

---

[162] I should distinguish this point from a similar one made in the literature. Invoking a concern about rationality, for example, Citron has argued that certain decisions "explicitly or implicitly require the exercise of human discretion." Citron, *Technological Due Process*, *supra* note 140, at 1302-04. My argument here is different. Citron's argument draws on the well-worn distinction between rules, which are given content before regulated subjects act, and standards, which are given contact after regulated subjects act. I think Citron's point is not technically correct as applied to machine learning. There is no technical reason why an algorithmic tool cannot classify new examples, and thereby liquidate a standard. The k-nearest neighbor (k-NN) algorithm, for example, classifies new instances by assigning the label that most frequently occurs among the *k* training samples nearest to that query point.

[163] Vill. of Willowbrook v. Olech, 528 U.S. 562, 563-65 (2000) (per curiam) (finding that the plaintiffs' allegation that the defendant's actions were "irrational and wholly arbitrary" was "sufficient to state a claim for relief under traditional equal protection analysis" "quite apart from the Village's subjective motivation" (internal quotation marks omitted)); Romer v. Evans, 517 U.S. 620, 631-36 (1996) (holding that Colorado Amendment 2 "lacks a rational relationship to legitimate state interests").

[164] *Cf.* Barocas & Selbst, *Big Data's Disparate Impact*, *supra* note 157, at 715 ("Disputes over the superiority of competing definitions are often insoluble because the target variables are themselves incommensurable.").

[165] *See, e.g.,* Friederike Mengel, Jan Sauermann, and Ulf Zölitz, *Gender bias in teaching evaluations*, 17 J. EURO. ECON. ASS'N. 535, 535-36 (2018) (finding gender bias in teacher evaluations).

[166] *See, e.g.,* Bob Uttl, Carmela A. White, and Daniela Wong Gonzalez, *Meta-analysis of faculty's teaching effectiveness: Student evaluation of teaching ratings and student learning are not related*, 54 STUD. EDUC. EVALUATION 22, 22-23 (2017) (noting that any correlation between student evaluations and learning are flukes instead of due to students' abilities to assess instructors).

[167] O'NEILL, *supra* note 132, at 135-40 (critiquing existing models of teacher evaluation).

[168] *See supra* text accompanying note 91a–92.

[169] Patricia Nilsson, *How AI Helps Recruiters Track Jobseekers' Emotions*, FIN. TIMES, Feb. 18, 2018, https://www.ft.com/content/e2e85644-05be-11e8-9650-9c0ad2d7c5b5 [https://perma.cc/X6JR-DG67].

[170] *See* Marc A. Cohen, *Against basic emotions, and toward a comprehensive theory*, 26 J. MIND & BEHAV. 229, 230 (2005) (arguing that "the empirical evidence does not support the basic emotions project"); Michael Price, *Facial Expressions—Including Fear—May Not Be as Universal as We Thought*, SCIENCE (Oct. 17, 2016), https://www.sciencemag.org/news/2016/10/facial-expressions-including-fear-may-not-be-universal-we-thought [https://perma.cc/R3RS-LE4Y] (discussing findings that Trobriand Islanders use a gasp to convey anger).

Whether criminal risk assessment for bail or probation is ultimately feasible also remains contested. A group of scholars have recently argued that violence risk is so infrequent, even among pretrial detainee populations, that it is statistically infeasible to distinguish the small number who will go on to comment acts of violence.[171] Moreover, these scholars argue, the training data inevitably used for risk rating is inevitably affected by animus.[172] Other scholars have resisted this conclusion, though,[173] and instruments for predicting violence remain in widespread use. I take no view of that dispute here.

This list of potential design flaws whereby algorithmic design can go astray is not intended to be exclusive. Rather, these five examples merely illustrate some of the ways in algorithmic tools can fail to deliver low rates of error.

4. Mathews *and Machine Learning*

The very possibility of specifying ex ante the conditions of due process violation raises an intriguing possibility: Whereas standard applications of the *Mathews* test to agency-based adjudicatory systems can flirt with indeterminacy,[174] its application may be straightforward and predictable in the machine-learning context. Discrete technological design margins can be isolated and then analyzed for their contributions to error rates. Almost fifty years after *Mathews*, that is, technology may be finally making its doctrinal focus empirically tractable. But at the same time, this tractability may also reveal difficulties inherent in the *Mathews* test that until now have been occluded in its judicial application.

For example, algorithmic tools make differently kinds of errors. It will often be the case that it is technically infeasible to minimize both false positives and false negatives.[175] Determining the appropriate mix of false positives and false negatives, however, will require difficult social and normative judgments, judgments that are now often skirted. In familiar applications of *Matthews*, these difficult judgments can be elided. In the algorithmic context, however, they become hard to avoid. To see this, consider a binary classification regime, which has false positives and false negatives, rather than a classifier that generates a continuous output variable, which can make errors of degree. The first, binary case is more familiar in a legal context. Algorithmic design recognizes the different value of false positives and false negatives by allowing for different weights to attach to each one.[176] Much as in the civil and criminal trials false positives (negatives) are assigned different implicit weights by varying the burden of proof, that is, so a computational tool can shift the balance between observed false positives and false negatives. But how should due process be defined as between different mixes of false positives and false negatives? The social value accorded to a false positive as opposed to a false negative in any given situation is a matter of judgment. Wrongful convictions are generally

---

171 *Technical Flaws of Pretrial Risk Assessment Tools Raise Grave Concerns* 2 (2019), https://dam-prod.media.mit.edu/x/2019/07/16/TechnicalFlawsOfPretrial_ML%20site.pdf [https://perma.cc/VP6Q-DDF7].
172 *Id.* at 2-3.
173 *See* Goel et al., *supra* note 149, at 17 (endorsing risk assessment instruments as superior to clinical predictions).
174 *See* Mashaw, *Due Process Calculus supra* note 139, at 46 (noting sources of indeterminacy)
175 For papers exploring the kinds of trade-offs implicit in algorithmic design, see Sam Corbett-Davies, Emma Pierson, Avi Feller, Sharad Goel & Aziz Huq, *Algorithmic Decision Making and the Cost of Fairness*, *in* PROC. OF THE 23RD ACM SIGKDD INT'L CONF. ON KNOWLEDGE DISCOVERY & DATA MINING 798, 804–05 (2017); Jon Kleinberg, Sendhil Mullainathan & Manish Raghavan, *Inherent Trade-Offs in the Fair Determination of Risk Scores* 4, 9, 17 (2016), https://arxiv.org/pdf/1609.05807 [https://perma.cc/9L9J-QZLN].
176 Lehr & Ohm, *supra* note 39, at 690-94.

thought very costly; erroneous plaintiff verdicts in tort less so.[180a] An evaluation of algorithmic due process requires a precise judgment of the relative costs associated with a false negative and a false positive.[177] In respect to bail determinations, employment decisions, and welfare allocations, however, no consensus exists as to the precise values of different error types. In consequence, determining when due process is satisfied will require an anterior policy debate on the value of different kinds of errors in a given policy domain. In current practice, a "very common" solution is to assume equal costs.[178] This seems an implausible global solution. As a result, the application of due process will entail difficult judgments about the social costs of various outcomes subject to regulation by prediction instruments. And that itself may well be a costly and divisive enterprise.

* * *

Determining whether a machine learning tool impinges on due process demands an examination of the fit between quality training data, the learning model, and outcome variable, and the match between the outcome variable and the latent variable. Provided the fit between training data, learning model, outcome variable, and latent variable is sufficiently tight, a machine learning tool should pass muster as a matter of due process. I have described those margins, including both choices about training data and methodological choice, in general and nontechnical terms. In many cases, moreover, it will be possible to make judgments about how these design choices were made without access to a classifier's source code.[179] The nature of due process design margins, and their relatively availability to ex post scrutiny, has implications for the analysis of remedial frameworks offered in Part III.

B. Equality and Anti-Discrimination Norms

The American law of race and gender equality is embodied in the constitutional jurisprudence of the Equal Protection Clause and federal antidiscrimination statutes.[180] Constitutional law, which is my focus here, turns on questions of intent and classification. I explore how these can be adapted to the machine learning context. I suggest, however, that the equality concerns commonly raised by algorithmic systems in practice are better conceptualized in terms of their impact on pernicious social stratification.[181] In the following, I will focus on racial equality norms, although many of the points I can make can be transposed to other contexts.

1. Equal Protection Norms

[180a] In re Winship, 397 U.S. 358, 371–72 (1970) (Harlan, J., concurring).

[177] The ordinary application of *Mathews* entails a similar judgment. But algorithmic design allows one to calibrate a performance threshold for accuracy in far more numerically precise terms than litigation would.

[178] Hand, *supra* note 48, at 2.

[179] *Cf.* Kroll et al., *supra* note 117, at 638 (discussing the limits of source code review).

[180] Note that this standard formulation assumes the identity of equality and antidiscrimination norms. In fact, the conceptual relationship between (different kinds of) equality and antidiscrimination is a complex one. For an excellent treatment, see generally Elisa Holmes, *Anti-Discrimination Rights Without Equality*, 68 MODERN L. REV. 175 (2005) (arguing that anti-discrimination rights do not necessarily require equality).

[181] This builds in an earlier critique, but I have tried not to repeat myself here. *Cf.* Huq, *Racial Equity*, *supra* note 9, at 1101-02 (suggesting a need for substantial rethinking of constitutional norms given the diffusion and adoption of machine learning tools).

The constitutional law of equality takes intent and classification as central analytic terms.[182] Since the mid 1970s, the Supreme Court has defined "the basic equal protection principle" under the Fourteenth Amendment to mean that "the invidious quality of a law claimed to be racially discriminatory must ultimately be traced to a racially discriminatory purpose."[183] It has also held that any occasion upon which "the government distributes burdens or benefits on the basis of individual racial classifications," will lead to the application of strict scrutiny.[184] To survive constitutional scrutiny, a classification's use must be narrowly tailored to serve a compelling state interest.[185] This anticlassification strand of the doctrine is justified on the grounds that racial lines are "divisive" and purportedly rarely relevant to a legitimate state purpose.[186]

The concept of an impermissible "purpose" or intent, however, has not been defined with clarity. It can be construed in several different ways.[187] Consider, for example, a recent racial gerrymandering decision in which the Supreme Court affirmed that "a state law . . . enacted with discriminatory intent" presented a constitutional problem.[188] The Court's reference to "discriminatory intent" might mean several different things: Does it require a showing that legislators responsible for redistricting despised or feared African Americans? What if they simply embraced negative racial stereotypes and hence viewed minorities as less worthy of political influence? Or what if they simply viewed Blacks as 'not our people' in a partisan sense? The Court does not say which of these count as "discriminatory intent." Indeed, it is a remarkable feature of Equal Protection jurisprudence that its central term—intent—remains clouded in uncertainty after almost fifty years of service.

Putting this uncertainty to one side, it seems clear is that in the modal Equal Protection case, the terms "intent" and "purpose" are typically used to describe the interior psychological disposition or beliefs of a particular individual.[189] To be sure, there are cases in which courts have drawn inferences about the intentions of collective bodies such as legislatures,[190] including racial gerrymandering challenges. But these cases are generally recognized as presenting difficult problems of aggregation

---

[182] Statutory antidiscrimination law, in contrast, also includes questions of disparate impact and reasonable accommodation. Noah D. Zatz, *Managing the Macaw: Third-Party Harassers, Accommodation, and the Disaggregation of Discriminatory Intent*, 109 COLUM. L. REV. 1357, 1368–69 (2009). For analyses of how disparate impact liability can be re-articulated for a machine learning context, *see e.g.*, Barocas & Selbst, *Big Data's Disparate Impact*, *supra* note 157, at 701-12 (arguing that the disparate impact doctrine should look for discrimination in data mining); Huq, *Racial Equity*, *supra* note 9, at 1128-33 (arguing for a bifurcated classification rule in algorithmic criminal justice tools).

[183] Washington v. Davis, 426 U.S. 229, 240 (1976). Although the intent requirement is now perceived as a conservative formulation, Katie Eyer has persuasively documented how racial progressives advocated for an intent rule through much of the twentieth century as a way to defeat southern states' efforts to circumvent desegregation rulings. Katie R. Eyer, *Ideological Drift and the Forgotten History of Intent*, 51 HARV. CR-CLL REV. 1, 4-5 (2016).

[184] Parents Involved in Cmty. Sch. v. Seattle Sch. Dist. No. 1, 551 U.S. 701, 720 (2007); *see also* Gratz v. Bollinger, 539 U.S. 244, 270 (2003) (describing the use of such classifications as "pernicious" (internal quotation marks omitted)); Jack M. Balkin & Reva B. Siegel, *The American Civil Rights Tradition: Anticlassification or Antisubordination?*, 58 U. MIAMI L. REV. 9, 10 (2003) ("[T]he anticlassification . . . principle holds that the government may not classify people either overtly or surreptitiously on the basis of a forbidden category: for example, their race.").

[185] Adarand Constructors, Inc. v. Pena, 515 U.S. 200, 235 (1995) ("Federal racial classifications, like those of a State, must serve a compelling governmental interest, and must be narrowly tailored to further that interest.").

[186] Fisher v. Univ. of Texas at Austin, 136 S. Ct. 2198, 2210 (2016).

[187] Aziz Z. Huq, *What is Discriminatory Intent?*, 103 CORNELL L. REV. 1211, 1240–63 (2018) (exploring the divergent potential meanings of intent in the constitutional context of antidiscrimination law).

[188] Abbott v. Perez, 138 S. Ct. 2305, 2324 (2018).

[189] *See, e.g.,* Foster v. Chatman, 136 S. Ct. 1737, 1754 (2016) (invalidating a criminal conviction on Sixth Amendment grounds and citing to the prosecutor's "racial animosity" (internal quotation marks omitted)).

[190] For a rare example, see Hunter v. Underwood, 471 U.S. 222, 229 (1985).

and inference because collective bodies do not themselves have intents—only their members do.[191] Even challenges to collective bodies' decisions do not deviate from the baseline psychological model of "intent" as individual belief or disposition insofar as they presuppose the possibility of aggregating individual intents.

2. Applying Equal Protections Doctrine to Machine Learning:

Difficulties arise in transposing equality doctrine to the machine learning context. In part, these difficulties track ambiguities in extant applications of that law; in part, they are distinct to this new technology. I consider here how application of anticlassification norms and intent-related rules generate difficulties. In the following section, I argue that the principle ways in which machine learning tools raise equality-related concerns are not well captured by anticlassification and intent-focused rules.

Consider first the application of anticlassification rules to the use of race labels in training data. At first blush, the doctrine might be read to suggest that any state use of individuals' race as "an input to the system" triggers constitutional concern.[192] The use of race as a "feature" might be seen as analogous to its use as a factor in college applications. In the latter context, the use of race as one factor among many generates strict judicial scrutiny.[193] But this conclusion may move too fast. For the use of race as a label in machine learning is arguably distinct from its use in college admissions. The latter is public and "divisive"[194] in the way that the technical, often practically indiscernible, use of race in machine learning systems is not. Moreover, there is a gap between race awareness and impermissible racial classification. Human decision-makers employed by the state (such as a police officer or a case worker) are often, inevitably aware of race in the sense of being immediately presented with phenotypical evidence in the majority of cases. It follows that an official's mere awareness of race raises no constitutional problem. By analogy, it may also be that mere inclusion of race as a feature of training data should not be per se problematic. Rather, such inclusion should be construed to be analogous to the visual accounting for race in quotidian human interactions.[195] Race as a feature is constitutionally problematic only if it influences ultimate decisions in a constitutionally relevant way. In the intent context, the Court has applied a but-for causation rule.[196] Logically, this should also apply to anticlassification challenges. Applying the but-for causation rule to the machine learning context requires courts to determine whether race's inclusion as a feature was a but-for cause of a specific decision. That is, application of a colorblindness rule would lead to a potentially complex technical inquiry into the counterfactual relevance of the race or gender feature.

A race-aware classifier that met this causation requirement, nevertheless, would likely implicate the anticlassification doctrine's concern with "protecting individuals from the harm of categorization by race."[197] As such, it would trigger strict scrutiny. But how would this standard work, and in

---

191 Richard H. Fallon, Jr., *Constitutionally Forbidden Legislative Intent*, 130 HARV. L. REV. 523, 527 (2016).
192 Barocas & Selbst, *Big Data's Disparate Impact, supra* note 157, at 695.
193 *Fisher*, 136 S.Ct. at 2208.
194. *Id.* at 2210.
195 For a similar observation in respect to the reliance element of a securities fraud action, see Yavar Bathaee, *The artificial intelligence black box and the failure of intent and causation* 31 HARV. J. L. & TECH. 889, 925-26 (2017).
196 Personnel Adm'r. v. Feeney, 442 U.S. 256, 279 (1979) (proof of discriminatory purpose requires showing that government decision-maker "selected or reaffirmed a particular course of action at least in part 'because of,' not merely 'in spite of,' its adverse effects upon an identifiable group").
197 Reva B. Siegel, *From Colorblindness to Antibalkanization: An Emerging Ground of Decision in Race Equality Cases*, 120 YALE L.J. 1278, 1287 (2011) [hereinafter "Siegel, *From Colorblindness to Antibalkanization*"].

particular what would be entail for a racially aware classifier to be narrowly tailored? Because of a statistical phenomenon called "subgroup validity," it is often the case that a failure to include a feature with real-world effects leads to substantial accuracy losses.[198] Excluding race from a learner might have accuracy costs. At some point, the scale of that accuracy loss might be so great that a racial classifier would be (on some view) necessary. It is quite unclear, however, what kind of accuracy loss would be required in order to demonstrate that race's use in a classifier was "narrowly tailored" in a constitutionally adequate way.[199] The Court has never defined clearly what "narrowly tailored" means, nor provided any kind of numerical guidance for its application.[200] This ambiguity already leads to uncertainty in non-algorithmic contexts, where the Court has resolved by failing to provide a precise definition and eliding the definitional question. The leading precedent on point, which concerns the use of race to propagate diversity in admissions, rather evasively states that narrow tailoring is "simply not susceptible to precise metrics."[201] This solution, though, is not available in the machine learning context, where an algorithm's designer can assign a numerical value to the accuracy or welfare loss due to making her classifier race- or gender-blind.

Compounding the difficulty in applying the doctrine further, it may well be that the very exercise of placing a numerical accuracy or welfare-related value on the anticlassification norm will strike judges as so inimical to the ethos of constitutional law—so close to a quota—that they would baulk at the whole enterprise. In this way, the application of anticlassification rules to machine learning would generate quite novel difficulty.

Application of an intent standard to machine-learning tools can also raise complications.[202] To be sure, it is possible that the designer of a machine learning tool acts with discriminatory purpose as that term is used in Equal Protection law. But I am unaware of any instance in which animus on the part of an instrument's designers has been credibly alleged. Discrimination challenges by racial or ethnic minorities based on intent rather than classification are notoriously difficult to prove or win.[203] This is so when the official in question openly and repeatedly endorses an illicit motive.[204] Assuming there is no 'smoking gun' obtained through discovery or depositions, the task of proving unconstitutional intent will be especially challenging. In particular, when the choice of a certain technical form or a particular set of training data is the basis of the challenge, plaintiffs (especially

---

198 *See* Sam Corbett-Davies and Sharad Goel, *The Measure and Mismeasure of Fairness: A Critical Review of Fair Machine-Learning* 10 (Aug. 14, 2018) (providing examples).

199 Adarand Constructors, Inc. v. Pena, 515 U.S. 200, 235 (1995).

200 Richard H. Fallon, Jr., *Strict Judicial Scrutiny*, 54 UCLA L. REV. 1267, 1271 (2007) ("[T]he Supreme Court has never given analytical clarity to the strict scrutiny formula's central concepts of compelling governmental interests and narrow tailoring.").

201 David A. Strauss, Fisher v. University of Texas *and the Conservative Case for Affirmative Action*, 2016 SUP. CT. REV. 1, 16.

202 Huq, *Racial Equity*, *supra* note 9, at 1088–94.

203 *See* Russell K. Robinson, *Unequal Protection*, 68 STAN. L. REV. 151, 154 (2016) (contending that "the Supreme Court has steadily diminished the vigor of the Equal Protection Clause in most respects"); Reva B. Siegel, *Foreword: Equality Divided*, 127 HARV. L. REV. 1, 1–2 (2013). Indeed, given how easy it is to discriminate against racial minorities under existing law, there is little or no litigation-related incentive to resort to complex algorithms to cover up impermissible hostility to racial minorities. In contrast, members of racial majorities do not need to demonstrate an illegitimate purpose in affirmative action cases, making the claims more likely to succeed. *See* Siegel, *supra* note 207, at 1–2.

204 *See, e.g.*, Trump v. Hawaii, 138 S. Ct. 2392, 2421 (2018) (upholding President Trump's travel ban, despite discriminatory rhetoric, because the ban served legitimate national security purposes); *see also* Aziz Z. Huq, *Article II and Antidiscrimination Norms*, 118 MICH. L. REV. 47, 68–76 (2019) (offering a comprehensive account and critique of that decision).

members of a racial minority) will face an uphill battle .[205] Absent the use of an impermissible classification, plaintiffs alleging intent might argue that a feature was selected because it was "insufficiently rich . . . to assess members of a protected class."[206] Alternatively, they might seek to prove that certain features alone or in juxtaposition have been deliberated selected "as proxies for class membership."[207] But I suspect that these argument will be rarely be persuasive in the effort to demonstrate intent.

Further, in many contexts in which the state deploys machine learning, including public benefits and criminal justice domains, race and gender are likely to correlate tightly with other likely features used in training data (such as zip code or socioeconomic outcomes).[208] When there are ready proxies for race or gender effects, a discriminatory state entity can ensure that disfavored groups receive more negative outcomes by including those features in the training data.[209] In criminal justice applications, for example, there are likely to be "plenty of opportunities to associate certain social categories with statistical regularities, stereotypes, and past discrimination."[210] As a result of such collinearity, even a classifier that does not leverage race as a training-data feature is likely to learn "negative associations for certain social labels," including race.[211] That is, discriminatory and nondiscriminatory classifiers may look similar. With the exercise of moderate foresight, therefore an intentional discriminator can easily skirt liability. Again, this problem is not distinct to the machine-learning context. But the sheer diversity of available features may make it more pronounced.

In short, the application of anticlassification and intent doctrines (absent a 'smoking gun') are likely to generate difficult questions of proof, battles between experts about the purpose of various technical decisions, and few easy resolutions.

3. Equality and Machine Learning Reconsidered

Many of the equality-related concerns raised about machine learning, however, do not sound in the register of anticlassification or intent. They instead suggest the need for an alternative normative approach.

A common concern with machine learning classifiers is their capacity to encode human biases, blind spots, or otherwise normatively troubling assumptions or regularities derived from training data, outcome variables, or other design margins.[212] For example, in 2013, it was shown that a search on Google for typically African-Americans names produced advertisements for arrest records in roughly 90 percent of cases, while a search for typically white names produced the same sorts of advertisements

---

[205] *Cf.* Bathaee, *supra* note 195, at 923-25 (suggesting difficulties in attributing specific outcomes from an algorithm to its designer).
[206] Kroll et al., *supra* 117, at 681.
[207] *Id.*
[208] Barocas & Selbst, *Big Data's Disparate Impact, supra* note 157, at 692.
[209] A recent paper argues that "proving discrimination will be easier" if algorithms replace human decision-makers. Jon Kleinberg et al., *Discrimination in the Age of Algorithms*, 10 J. LEG. ANALYSIS 113, 114 (2019). Where an algorithmic designer shapes a model or selects features out of a discriminatory motive, though, this conclusion does not follow.
[210] Betsy Anne Williams, Catherine F. Brooks, and Yotam Shmargad, *How algorithms discriminate based on data they lack: Challenges, solutions, and policy implications*." 8 J. INFO. POL. 78, 89 (2018).
[211] *Id.*
[212] There are several competing and inconsistent accounts of nondiscrimination in the literature. *See* Huq, *Racial Equity*, *supra* note 9, at 1115-23 (collecting models of fairness).

in less than 25 percent of cases.[213] In 2019, a different study of a widely used commercial instrument used to recommend care regimes for high-risk patients was flagging equally at-risk African-Americans and whites at divergent rates.[217a] Black patients, as a result, received fewer interventions despite high morbidity risk. The divergence arose, the study found, because of the instrument's reliance on health care costs as an outcome variable. Recall also some facial recognition tools have errors rates for black women 34.7 percent higher than those for white men.[214] None of these equality-related concerns is well understood as a worry about either classification or a designer's intent. Perhaps unsurprisingly, the large technical literature on algorithmic bias also eschews a focus on those concepts.[215]

It is possible to generalize from these examples to identify equality-related errors that predictably arise in the machine-learning context but that cannot be easily fit within existing intent-based or anticlassification doctrine. Three examples are sample bias, feature bias, and label bias.[216] *Sample bias* results from nonrandom sampling to create training data. For example, training data for the Allegheny County AFST score arguably reflected bias on the part of members of the public reporting a risk, with Black families coming under state supervision for more minor infractions than white families.[217] As a result, there were more African-American families identified as problematic than white families, leading to distortion in the sample. *Feature bias* occurs if a particular feature assigned to the training data is systematically erroneous because features are mislabeled at different rates across different groups.[222a] This might occur in a labor market analysis, for instance, if women are erroneously labeled as less productive as a consequence of biased appraisals. Finally, *label bias* arises if the designated outcome variable fails to track ground truth equally well for different groups.[222b] An outcome variable may evince bias in respect to a specific subgroup where the label is assigned to different social groups at different thresholds. Consider a bail algorithm that is trained using data for which arrest rates are available. If police are more willing to arrest some racial groups rather than others based on the same predicate behavior, then using race as an outcome variable will introduce bias into the data.

None of these problems are well captured by existing Equal Protection doctrine.[218] At a minimum, this suggests that the normative concerns animating the latter are not necessarily identical

---

213 Latanya Sweeney, *Discrimination in online ad delivery*, arXiv preprint arXiv:1301.6822, at 1-2 (2013); *see also* SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 66-80 (2018) (providing examples or race-specific searches that generated derogatory results for black but not white-associated terms).

217a Zaid Obermeyer et al., *Racial Bias in Health Algorithms*, 366 SCIENCE 447, 447 (2019).

214 Buolamwini & Gebru, *supra* note 117, at 77-78 (2018).

215 For a useful recent summary, see Deirdre K. Mulligan et al. *This Thing Called Fairness: Disciplinary Confusion Realizing a Value in Technology*, 3 PROCEEDINGS OF THE ACM ON HUMAN-COMPUTER INTERACTION 119, 119:24–26 (2019).

216 These terms are adopted, with some changes, from Corbett-Davies and Goel, *supra* note 198, at 17-19.

217 EUBANKS, *supra* note 65, at 153-54.

222a *See* SingleStone, *Combatting Data Bias: Goal, Data, Feature and Model Bias*, MEDIUM (July 23, 2019), https://medium.com/@SingleStoneCX/combatting-data-bias-goal-data-feature-and-model-bias-5aeaf19b83fe [https://perma.cc/PDC6-KAYH].

222b *See* Corbett-Davies and Goel, *supra* note 202, at 3.

218 One reason for this is a mismatch with the standard conceptions of discrimination may be a bad fit for the machine learning context. Leading philosophical accounts of discrimination hinge on the notion that certain actions are discriminatory insofar as they manifest disrespect toward a person because they fail to "recognize certain features of . . . persons *qua* persons, such as the intrinsic value of their well-being or the character of their individual autonomy." BENJAMIN EIDELSON, DISCRIMINATION AND DISRESPECT 6 (2015); *see also* DEBORAH HELLMAN, WHEN IS DISCRIMINATION WRONG? 7-8 (2008) (focusing on the how "demeaning" action impinges on the "equal worth" of persons). These accounts take as a modal case an interpersonal encounter between individuals in which respect or disdain can be simultaneously manifested and experienced. This is not characteristic of the machine-learning state.

to the equality-related concerns raised by machine classification. In my view, it is better to recognize that invidious intent and anticlassification do not provide a comprehensive or perspicuous lens to analyze the equality concerns raised by machine learning tools. While the fashioning of a fully developed alternative to existing equality law is a task that falls beyond my project here, I offer here a very preliminary sketch of what that a reconceptualized approach to equality concerns, at some distance from the current constitutional regime, might look like.

The precise nature of "race" remains contested, even among natural and social scientists.[219] Without resolving that disagreement here, it is still possible to observe that race is normatively relevant because it is deployed as a "social fact" by individuals and institutions responsible for critical distributive decisions.[220] As a result of this social usage, race (like gender and disability) has come to be closely correlated with other indicia of disadvantage and exclusion. Thanks to this redundant encoding of race with other measures of exclusion, overt reliance on race or correlated traits (e.g., educational outcomes, residential zip code) often have the effect of strengthening the tendency of resources and opportunities to be distributed in predictably asymmetrical ways. It is the ensuing asymmetric diminishment in life chances and material goods for historical marginalized groups comprises the harm against which equality norms should insulate. A plausible alternative reconceptualization of equality norms for machine-learning instruments therefore focuses on the risk that prediction-driven allocations of benefits or harms amplify the stratifying social function of race (or, for that matter, kindred classifications such as gender, sexual identity, disability, and ethnicity).

Accounting for such harms in the machine-learning context cannot be done by a mechanical rule against race-consciousness, or a categorical presumption against prediction. Indeed, it seems to me unlikely, given extant levels of racial stratification, that predictive instruments will be able to avoid such harms without conscientious consideration of the specific mechanisms whereby disadvantage is transmitted over time and space, and (at times) race conscious interventions to disrupt these mechanisms' operation. Where such interventions have social costs (say, by increasing error rates across whole populations), an algorithmic designer must make decisions about how to trade-off between equity and other goals. Of course, such trade-offs are politically and normatively controversial. The rise of machine prediction, though, places them in clear relief. Advances in computational prediction, in other words, are likely to sharpen the conflict between colorblindness and the goal of a social order in which race (or kindred properties) does not define an individual's life course and opportunity set.

C. Privacy

Privacy is a plural not a monolithic concept. It is "complex, . . . entangled in competing and contradictory dimensions, [and] engorged with various and distinct meanings."[221] I focus here on one

---

[219] For a documenting of such disagreements, see ANN MORNING, THE NATURE OF RACE: HOW SCIENTISTS THINK AND TEACH ABOUT HUMAN DIFFERENCE 3–8 (2011). For an illuminating debate among philosophers, see WHAT IS RACE?. (Joshua Glasgow, ed., 2019).

[220] See Eduardo Bonilla-Silva, *The Essential Social Fact of Race*, 64 AM. SOC. REV. 899, 899 (1999) (internal quotation marks omitted); and Mara Loveman, *Is "Race" Essential?*, 64 AM. SOC. REV. 891, 891 (1999).

[221] Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001). For a useful taxonomy of the various margins of contestation over privacy, see Deirdre K. Mulligan, Colin Koopman, and Nick Doty, *Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy*, 374 PHIL. TRANS. ROYAL SOC. A: MATH., PHYS. & ENGINEERING SCI. 1, 11 (2016) (distinguishing contests over privacy's foundation, the scope of its protections, the nature of harms involved, and its scope in time and space).

strand: privacy in respect to information, in the sense of an instrumental ability to determine how, and to whom, information held closely by a person is disclosed.[222] In the United States,[223] jurisprudence on informational privacy is far less developed than due process or equality case-law. I set forth briefly the doctrinal landscape. I then explore the ways in which machine learning can impose distinct harms to informational privacy, and ask how a more expansive constitutional or subconstitutional privacy regime might be articulated in response.

1. Constitutional Privacy Norms

The Supreme Court has never recognized a free-standing right to informational privacy. In the 1977 case of *Whalen v. Roe*, it assumed arguendo a constitutional entitlement against the state's improper collection, aggregation, or disclosure of an individual's private information.[224] Although the Supreme Court has never extended *Whalen* into a full-fledged constitutional right, some circuit courts have built on its foundation. A few have suggested that no such right obtains, while others have crafted a cautious doctrinal test for the right.[225] A 2010 precedent appears to read *Whalen* narrowly but conspicuously declined to reject the possibility of a constitutional right to informational privacy.[226] *Carpenter v. United States*,[227] which narrowed the third-party doctrine in the Fourth Amendment context, also recognized a right against government acquisition of private information held by third parties. But third-party doctrine under the Fourth Amendment is analytically distinct from the idea of a free-standing right to control private inferences from data that would otherwise not have been illuminating.

Given the weakness of constitutional law on information privacy, it is worth looking beyond it to federal and state statutes or regulations. Subconstitutional law, however, is a patchwork. Some federal statutory and regulatory privacy protections generally extend to private, but not to federal or state actors.[228] At the subnational level, states such as California, New York, and Massachusetts have imposed data security obligations on large companies, but not state actors.[229] Further, a "sizeable

---

[222] Helen Nissenbaum, has usefully introduced a distinction between norms of "appropriateness" and "distribution" or "flow," that illuminate "whether [information's] distribution, or *flow*, respects contextual norms of information flow" in a given social sphere. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE 123 (2008).

[223] This is slightly different from the idea of "data privacy" in European law, which is "compromised whenever a data controller processes personal information in a manner that is irrelevant or no longer relevant for the specified purposes for which the information has been acquired." Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981, 998 (2018).

[224] Whalen v. Roe, 429 U.S. 589, 599 (1977) (describing an interest in "avoiding disclosure of personal matters"); *see also* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457 (1977) (citing the quoted language in *Whalen*).

[225] For a discussion of the conflicting lower court precedent on this point, see Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CAL. L. REV. 2007, 2016 (2010).

[226] *See* Nat'l Aeronautics & Space Admin. v. Nelson, 562 U.S. 134, 147-48 (2011) ("As was our approach in *Whalen*, we will assume for present purposes that the Government's challenged inquiries implicate a privacy interest of constitutional significance.").

[227] 138 S. Ct. 2206, 2219 (2018) (rejecting application of the third-party doctrine to cell-site locational data).

[228] For instance, acting under the Health Insurance Portability and Affordability Act of 1996, the U.S. Department of Health and Human Services has created by regulation a duty to "[[p]rotect against any reasonably anticipated threats or hazards to the security or integrity" of information covered by the statute. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (Feb. 20, 2003) (codified at 45 C.F.R. 164.306(a) (2016). Since 1995, the Federal Trade Commission has used its statutory authority to police "deceptive" or "unfair" trade practices to enforce the terms of companies' privacy policies. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 599 (2014) (internal quotation marks omitted).

[229] William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1153–54 (2019).

majority of states have been engaged in privacy enforcement," albeit largely against private actors.[230] State law, and state officials, therefore, may fill some on the gaps left by federal law. But it would be wrong to assume that its coverage is comprehensive and systemic, rather than patchy and haphazard. As Lior Strahilevitz has explained in a careful synoptic analysis, this heterogenous approach at both the state and the federal level means that there may be instances in which a state or federal employee a common-law tort claim of invasion of privacy against an unauthorized governmental disclosure—but whether she can will depend on a complex interaction of federal tort liability, immunity doctrines, and state law.[231] Only careful analysis of a particular jurisdiction's applicable federal and state law will reveal whether an action counts as a wrong under either federal or state privacy law.

2. Privacy Risks from Machine Learning

The operation of machine learning creates two distinctive information privacy-related risks. The first involves the power of the state to draw inferences of private information from otherwise data that would otherwise not reveal a given private fact. This means 'private' information can be acquired without the usual predicate of a constitutionally regulated "search or seizure." Machine learning can implicate different privacy-ousting inferences. One possibility involves "category jumping" inferences to "reveal attributes or conditions an individual has specifically withheld from other."[232] Examples include the inference of health conditions from spending-related information, or the inference of behaviors or dispositions from health-related data. A second possibility concerns the leveraging of data on one person to draw inferences about an individual who is not present in the dataset. Consider, for example, the genetic databases maintained by both federal government and all fifty states.[233] Those databases may be searched not only to match those samples, but also to match against "close genetic relatives."[234] Hence, they permit 'out of sample' inferences concerning the behavior and location of people who have not come into contract with the criminal justice system. Similarly, consumer genetic platforms, such as GEDmatch and FamilyTreeDNA, contain larger pools of genetic data.[239a] Some voluntarily allow law enforcement access. It is likely that the inferential potential of genetic data will increase in the near term. In 2018, researchers used a measure of allele differentiation across the whole genome, called a polygenic risk score, to make impressive population-level predictions of educational and cognitive performance.[235]

A second and distinct form of potential privacy-related harm emerges from a different source. Machine learning depends on the exploitation of large pools of training data. Often held by the state, such pools create a risk of data breaches that impose substantial privacy and pecuniary costs upon individual subjects. In states such as Pennsylvania, officials have even created new data warehouses that collect and house information flows from several, otherwise disparate state agencies, to leverage

---

[230] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 758 (2016) [hereinafter, "Citron, *Privacy Policymaking*"].
[231] Strahilevitz, *supra* note 225, at 2017-18.
[232] Eric Horvitz & Deirdre Mulligan, *Data, privacy, and the greater good*, 349 SCIENCE 253, 253 (2015).
[233] Natalie Ram, *DNA by the Entirety*, 115 COLUM. L. REV. 873, 881 (2015).
[234] *Id.* at 882-83.
[239a] Natalie Ram, *The U.S. May Soon Have a De Facto National DNA Database*, SLATE, March 19, 2019, https://slate.com/technology/2019/03/national-dna-database-law-enforcement-genetic-genealogy.html [https://perma.cc/7L79-3XCG].
[235] James J. Lee et al., *Gene discovery and polygenic prediction from a genome-wide association study of educational attainment in 1.1 million individuals*, 50 NATURE GENETICS 1112, 1112 (2018) (using polygenic risk scores to explain 11–13% of the variance in educational attainment and 7–10% of the variance in cognitive performance).

for predictive ends.[236] Data breaches can result from either negligent or malicious action, and come from inside or outside an entity. Studies find a substantial risk of large breaches with the risk rising for any given entity as the amount of data it holds grows.[237] Breach yields not only an unanticipated and socially in appropriate disclosure,. As a result of a breach, it is argued, individuals suffer "an increased risk of identity theft, fraud, and reputational damage," and immediate "[e]motional distress."[238] It is only because "reliable information regarding the cause, severity and volume of privacy violations is lacking," that there remains uncertainty about both the scale of the problem and the adequacy of legal responses.[239] It seems likely that the diffusion of machine learning across state functions increases the risk of such privacy-related losses above and beyond the risks created by private efforts to collect and analyze individuals' data.

3. Privacy Rights in the Machine Learning State

The range and variation in information privacy harms that can emerge from machine learning obviates the possibility of a single 'right to privacy' in that context. Rather than a single right, privacy is better conceptualized as a congeries of entitlements linked by a joint concern with maintaining the appropriate flow of data. Privacy in this context, however, should not be reduced to a measure of individuated control;[240] the latter is merely one component of a larger repertoire of appropriate responses. I explore three pathways—prohibitions, retail control rights, and privacy "by design"—concluding that the latter is likely most promising despite its shortfalls and limitations.

A first option for responding to machine learning's privacy risks is exemplified by San Francisco's prophylactic bar on facial recognition tools. This is a simple prohibition on the gathering and use of certain kinds of data.[246a] I am skeptical, however, that constraints on information acquisition are tenable in the facial-recognition context. Consider the privacy concerns raised by such tools. These are unlikely to be addressed successfully by banning public surveillance alone when private surveillance persists. The video surveillance throughout the Americas was valued at $3.9 billion in 2016.[241] By the same year, roughly 60 percent of cameras sold was network-ready, and 40 percent of those featured embedded video analytics "as a means to automate the monitoring process[, they] can be particularly effective in proactively identifying events as they happen or extracting information from recorded video."[242] Even if the state eschews such tools, as in San Francisco, private actors will build databases and pursue recognition-based inferences aggressively. Once private use of these tools is sufficiently

---

236 EUBANKS, *supra* note 65, at 135.

237 Benjamin Edwards, Steven Hofmeyr, and Stephanie Forrest, *Hype and heavy tails: A closer look at data breaches* 2 J. CYBERSECURITY 3, 4 (2016) (reporting findings of an empirical survey of data breaches in the private sector).

238 Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 745 (2018)

239 Sasha Romanosky and Alessandro Acquisti, *Privacy costs and personal data protection: Economic and legal perspectives*, 24 BERKELEY TECH. L. J. 1061, 1101 (2009). For a study of the resulting litigation (which is perforce an unreliable guide to the actual incidence of data breaches), see Sasha Romanosky, David Hoffman, and Alessandro Acquisti, *Empirical analysis of data breach litigation* 11 J. EMP. L. STUD. 74, 74-75 (2014) (identifying and analyzing more than 230 data breach suits in federal court between 2000 and 2010).

240 *Cf.* Cynthia Dwork & Deirdre K. Mulligan, *It's Not Privacy, and It's Not Fair*, 66 STAN. L. REV. ONLINE 35, 36 (2013) ("[P]rivacy controls and increased transparency fail to address concerns with the classifications and segmentation produced by big data analysis.").

246a *See* Conger, *supra* note 131.

241 HIS Markit, *Video Surveillance: How Technology and the Cloud Are Disrupting the Marketplace* 5 (2019), https://cdn.ihs.com/www/pdf/IHS-Markit-Technology-Video-surveillance.pdf [https://perma.cc/4FC7-3PK4].

242 *Id.* at 4, 6.

pervasive, I am skeptical that it will be feasible to maintain a prohibition on state usage of a technology in the face of pervasive private usage. To the public, the latter are likely to seem perverse and otiose—especially in the wake of high profile crimes or violent crises.

Categorical prohibitions on collection or inference may be more effective, however, in other domains. Since 2008, the Genetic Information Nondiscrimination Act ("GINA") has prohibited insurers and employers from relying on genetic data in making coverage or hiring decisions.[243] Because "the paradigmatic GINA claim" arises when an insurer "either drops coverage or hikes up premiums based on a genetic test that reveals a previously unknown health risk," the statute is best understood as a prophylaxis against inferential exploitation of data that, standing on its own, is unilluminating.[244] Bans on certain kinds of machine-learning inference might be justified on privacy grounds, or on the ground that certain kinds of predictions are not properly within the state's authority. GINA, for example, might be justified by the view that biology should not be treated by the state as destiny.[245] On the other hand, it is hard to see a similar prohibition being extended to state action, since there is some evidence that the creation of DNA databases is associated with meaningful declines in serious crimes, such as murder and rape.[246] Where there are competing social goods that might offset privacy losses, a ban might be implemented with sunset clauses. Temporary measures of this kind would allow regulators to learn how a technology is applied, whether it has greater benefits than costs, and how those costs can be mitigated.

Another alternative is a more narrowly tailored retail right to challenge specific inferences. Use regulation of this sort can be observed in the foreign intelligence context,[247] and has been urged by scholars more broadly in relation to government databases.[248] Yet there is a case for caution before embracing a regulatory reform predicated on dispersed lawsuits by uncoordinated individuals, each challenging a particular use of a machine learning tool. For one thing, a system of individualized permissions for machine inferences does not account for the possibility that an official will be able to aggregate insights across several different searches in ways that create new privacy violations. For example, searching video data for a specific person's movements might constitute a serious privacy invasion only if the officer also has access to that person's internet metadata. A granular system of warrants may miss important aggregation-enabled effects.[249] More generally, in the criminal justice domain, ex ante screens have not proven consistently effectual checks on official discretion.[250] The sheer breadth of the modern criminal law lowers the cost of obtaining warrants in the criminal justice context. Similarly, the regulation of machine-learning inferences would be subject to substantive

---

[243] 42 U.S.C. §§ 300gg-53(a)-(b)& § 2000ff-1(a).
[244] Bradley A. Areheart & Jessica L. Roberts, *GINA, Big Data, and the Future of Employee Privacy*, 128 YALE L.J. 710, 723–24 (2019).
[245] *Cf. id.* at 723 (noting concerns about adverse selection in health insurance markets with genetic testing).
[246] Jennifer L. Doleac, *The effects of DNA databases on crime*, 9 AM. ECON. J.: APP. ECON. 165, 166-67 (2017).
[247] Queries of the bulk metadata collected under Section 215 of the Patriot Act must be supported by "reasonable articulable suspicion." *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-80, 7 (FISA Ct., Apr. 25, 2013).
[248] Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 579–80 (2017) ("[W]hen a database query returns information that the government could otherwise collect only through a Fourth Amendment-regulated means, the Fourth Amendment should regulate that query.").
[249] On the other hand, warrants do now impose forward-looking minimization requirements. And in an academic context, institutional review boards can and do place constraints on the combination of empirical data. Enforcing a rule against combinatory actions, however, would require a good deal of tweaking of the present warrant system.
[250] Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609, 1610–11 (2012) ("[W]hat was once a 'warrant requirement' is now a rule so laden with exceptions that it best resembles a piece of Swiss cheese . . . .").

inflation of the justificatory grounds upon which government action is allowed. Given the imperfect performance of the Fourth Amendment's warrant rule in the face of substantive criminal law's inflation,[251] there is no reason for optimism about a parallel ex ante screening rule in the less salient context of machine learning. Instead, the weakness of the present individualized ex ante screening system for criminal searches may a reason for a more systemic approach in the machine learning context.

A further problem with retail articulation of privacy rights is that individuals seem to be highly imperfect users of protective tools. One of the distinctive characteristics of privacy harms is the fact that they can arise long after a specific disclosure is made. Retail instantiation of a privacy right assumes that individuals will be able to anticipate and account for temporally distinct harms. It is not clear this is so. Several studies have identified divergent valuations of privacy rights in contractual settings, with variance seemingly motivated by the endowment effects[252] or by an irrational willingness to trade privacy to create a "possibly permanent negative annuity in the future."[253] Cognitive failures of this emerge even though the data acquired by platforms and vendors through on-line transactions has considerable economic value: One estimate suggests that American internet platforms derived $63.8 billion in value from consumers' personal information in 2017 and $76 billion in 2018.[254]

A third possibility beyond bans and retail control rights focuses on building privacy concerns directly into the architecture of a machine learning instrument. There is a range of loosely defined 'best practices' for "privacy by design."[255] These require privacy to be "embedded into the design and architecture" of informational systems.[256] Government can implement privacy by design solutions directly, or can delegate the tasks to private-sector actors who handle sensitive data.[257] Privacy by design operates, as its name suggests, at a system-wide level. One analysis of network security, for example, underscores the need for a "flexible and modular" architecture for holding data.[258] Another

---

[251] Of course, there are conceivable reforms to make warrants more effective. *See, e.g., id.* at 1610-15 (advocating for a clear, revitalized warrant requirement that requires a warrant whenever it is feasible to obtain one). But if those reforms have not taken hold in the ordinary criminal justice domain, should we expect them to take hold in the machine learning domain?

[252] Alessandro Acquisti, Leslie K. John, and George Loewenstein, *What is privacy worth?*, 42 J. LEG. STUD. 249, 249-51 (2013).

[253] Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, 3 ECON. INFO. SECURITY 26, 31 (2005). For similar results, see Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online*, 34 J. PUB. POL'Y & MARKETING 210, 219–21 (2015).

[254] Robert Shapiro & Siddhartha Aneja, *Future Majority, Who Owns Americans' Personal Information and What Is It* Worth? 3 (2019), https://www.futuremajority.org/pages/who-owns-americans-personal-information [https://perma.cc/EHA5-B7BX]; *see also* Matthew Crain, *The limits of transparency: Data brokers and commodification*, 20 NEW MEDIA & SOC. 88, 90 (2018) (describing data brokerage as a $200 billion industry). Empirical studies suggest that "[w]hen consumers learn that their data is a tradable asset, they value their data significantly more." Sarah Spiekermann & Jana Korunovska, *Towards a Value Theory for Personal Data*, 32 J. INFO. TECH. 62, 74 (2017).

[255] Seda Gürses, Carmela Troncoso, & Claudia Diaz, *Engineering privacy by design*, 14 COMP., PRIV. & DATA PROTECTION 25, 27-28 (2011). The seminal work is Ann Cavoukian, *Privacy by Design: The Seven Foundational Principles* (2009), http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf [https://perma.cc/5U2X-B3WH]. The Federal Trade Commission has endorsed privacy-by-design principles. Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses & Policymakers*, at iii (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [https://perma.cc/TK9B-X9BL].

[256] Cavoukian, *supra* note 255, at 3.

[257] Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377, 380–81 (2006).

[258] Simon Liu and Rick Kuhn, *Data loss prevention*, 12 IT PROF'L 10, 13 (2010).

catalogs a number of "system[s] . . . to detect and prevent the unauthorized access, use, or transmission of confidential information."[259] Data can be classified according to its sensitivity, access can be regulated directly and through encryption, and especially sensitive data can be stored in distributed silos, so no one breach will generate too much damage.[260] Where information is dispersed across numerous physical devices, such as surveillance cameras or the Rapid-DNA "swab in - profile out" box,[261] security against hacks is hard or impossible to achieve through patching, and instead must be integrated in the design and construction stage.[262] The core point is again that privacy, whether a matter of a centralized database or a network of distributed devices, must be hardwired at the design stage. It cannot be effectively supplied at the back end. It is more akin to constitutional structures such as the separation of powers than to a discrete individual right.[263]

To be sure, all is not well with privacy by design. In a recent survey, Deirdre Mulligan and Kenneth Bamberger stress the difficulty of "intentionally translating values into design requirements" given cognitive biases and unintended consequences.[264] This, they argue, is a result of deficiencies in the governmental processes through which privacy by design is realized:

> [E]xisting institutions and processes of democratic and administrative governance have proven to be defective design-war battlefields. They are structurally unsuited to the deliberative decisionmaking [sic] necessary for governance-by-design. No domestic venue exists for the broad conversation about which values to embed in which circumstances. Administrative process frequently fails even to recognize technology design choices as matters of public policy, rather than private choice or government procurement. Agencies generally lack both the technical expertise and the mandate to consider fully the implications of embedding values in design. . . . [A]gency-by-agency decisionmaking [sic] creates downstream ripple effects, prioritizing certain values and precluding reasoned deliberation over others. First movers, particularly those that exercise the greatest sway over the private sector, may co-opt technology to their agencies' particular missions.[265]

---

[259] ASAF SHABTAI, YUVAL ELOVICI, AND LIOR ROKACH, A SURVEY OF DATA LEAKAGE DETECTION AND PREVENTION SOLUTIONS 10 (2012) (emphasis omitted).

[260] Faheem Ullah et al., *Data exfiltration: A review of external attack vectors and countermeasure*s, 101 J. NETWORK AND COM. APP. 18, 26–27 (2018); *see also* Lior Arbel, *Data loss prevention: the business case*, 5 COMP. FRAUD & SEC. 13, 14-15 (2015) (emphasizing the creation of systems for constraining and tracking data access).

[261] Rapid DNA analysis is a new technology that allows for DNA testing of buccal swabs to be done at police stations, rather than at a centralized facility. Jacklyn Buscaino, et al., *Evaluation of a rapid DNA process with the RapidHIT® ID system using a specialized cartridge for extracted and quantified human DNA*, 34 FORENSIC SCI. INT'L GENETICS 116, 116-17 (2018).

[262] Bruce Schneier, *Internet Hacking is About to Get Much Worse*, N.Y. TIMES, Oct. 11, 2018, https://www.nytimes.com/2018/10/11/opinion/internet-hacking-cybersecurity-iot.html [https://perma.cc/JC8Y-ELKX].

[263] *Cf.* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1608 (2007 (arguing that if policymakers adhere to the view that privacy rights are coextensive with explicit privacy laws, they may be omitting a significant source of privacy interests).

[264] Deirdre K. Mulligan and Kenneth A. Bamberger, *Saving Governance-by-Design*, 106 CAL. L. REV. 697, 710 (2018).

[265] *Id.* at 701-02. For criticism of 'privacy by design' as ambiguous and an inappropriate delegation of authority to (unrepresentative) engineers, see Ari Ezra Waldman, *Privacy's Law of Design*, 9 UC IRVINE L. REV. 1239, 1273 & n.229 (2019).

In response to these concerns, they offer a series of best practices to mitigate institutional pathologies.[266] Their careful analysis suggests the need for careful institutional design of agencies and departments tasks with the implementation of privacy by design.

In sum, information privacy, like due process and equality, is promoted through the careful design and maintenance of institutional systems: It is a property of the overall informational architecture in which machine learning tools are operated, not of any individual act of classification or prediction. No doubt the specific instruments that best tailored to privacy's production in this context will change as technology shifts, and as we move from PC-based applications to phone-based tools to the internet of things (and perhaps thence to mind-AI integration[267]). But it seems probable that the system-level locus of privacy-responsive policy-making will persist.

D. Constitutional Norms For Machine Learning: A Summary

My aim in this Part has been to examine how important constitutional values of due process, equality, or privacy are raised by the machine-learning state. Application of those norms raises both challenges encountered in the non-algorithmic context and new problems. In respect to each right, I have suggested a recalibrated account of the relevant norm. In closing, I want to draw attention to a common thread tying these analyses together: When humans interact with algorithmic systems, normative concerns tend to arise because of structural or design decisions that affect many or all users, and not because of the specifics of particular interactions. Constitutional norms of procedural due process, equality or privacy, that is, pervasively operate at the system rather than the individual level. Although thus is true in some non-algorithmic contexts, the systematicity of constitutional norms in the machine-learning state creates a strong reason to break from the 'liability in tort' model that otherwise dominates adjudication of constitutional rights.

The justifications for adopting a systematic and wholesale, rather than a retail and individualistic, perspective to algorithmic constitutionalism sound in terms of diagnosis, causation, and (relevant to the following Part) remedy. First, from a diagnostic perspective, the identification of individual cases of erroneous decisions provides limited evidence that a particular algorithmic classification system has deviated from due process norms. Nor does the fact that a classification rules tends to rank members of a protected class differently from nonmembers alone bespeak an equality-related problem.[268] Second, the causes of due process, equality, and privacy violations tend to lie at the level of system design and operation, not the discrete and isolated action of a street-level official. Without taking a systemic perspective that attends to the suite of human design decisions embedded in the algorithm's training data, outcome variable, and method, it will often not be possible to identify how or why inaccuracies or systemic biases occur. In a like vein, data-breach risk tends to emerge from weaknesses in an information system's architecture. Finally, remedies for due process, equality, or privacy concerns are likely incomplete without a systemic perspective. Human appeals from algorithmic decisions may provide due process in the individual case but are likely to increase the

---

[266] Mulligan & Bamberger, *supra* note 240. at 742-80.

[267] *Cf.* Alex Knapp, *Elon Musk Sees His Neuralink Merging Your Brain With A.I.*, FORBES, July 7, 2019, https://www.forbes.com/sites/alexknapp/2019/07/17/elon-musk-sees-his-neuralink-merging-your-brain-with-ai/#1b69a8f74b07 [https://perma.cc/C42P-EX44] (detailing Elon Musk's plan to develop implants to connect human brains with computers).

[268] *See* Huq, *Racial Equity*, *supra* note 9, at 1125-32.

overall error rate.[269] Eliminating race from the feature set for an algorithmic tool can lead error rates to spike.[270]

This system-level location of due process, equality, and privacy concerns channels attention to human decisions and elements of algorithmic design remote in time from the immediate contact between a machine and a regulated human subject. As a result, it invites new questions about how, in practice, those norms are to be realized given the dominant "liability in tort" model of constitutional enforcement[271]--questions that are taken up more fully in the next Part.

III. Constitutional Remediation in the Machine Learning State

A well-calibrated remedial architecture for the machine-learning state has two elements. It first requires ex ante rules to force disclosures and generate transparency on the one hand, and to impose accuracy, privacy, and equality-enhancing mandates on the other. Second, it entails the availability of aggregate, rather than individual, litigation remedies after the fact. In other work, I have argued against the idea that a right to a human appeal is an appropriate response to constitutional flaws in a predictive tool.[272] Building on the arguments developed in that article, I posit that aggregate remedies that focus on system-level characteristics of predictive tools provide a more effective means of identifying and correcting design choices that elicit constitutional errors.

The analytic framework employed here draws on a familiar distinction between rules (whose content is established ex ante) and standards (given substance after the fact).[273] This ex ante/ex post distinction in practice is correlated, somewhat imperfectly, with the choice between regulation by administrative agency and regulation through the common-law system of tort liability.[274] I assume here that ex ante regulation is done by agency, while courts undertake ex post review. Both forms of intervention have familiar strengths. Ex ante regulation trades on the virtues of bureaucratic expertise, predictability, and consistency.[275] Ex post intervention enables private choice by forcing the internalization of potential damage payments and allowing the "parties to calibrate their anticipatory remedial measures."[276] While some scholarship treats these strategies as alternatives, in practice "ex ante and ex post policies are very frequently used jointly."[277] Uncertainty among ex post actors, in

---

[269] *See* Huq, Human Decision, *supra* note 149, at 38–43 (developing this argument).
[270] *See supra* text accompanying note 155.
[271] *See supra* text accompanying note 24.
[272] *See* Huq, *Human Decision*, *supra* note 149, at 53.
[273] Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557, 559-63 (1992); *see also* STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW 572-74 (2004). A standard is partially specified ex ante, but the full range of relevant considerations, and its precise specification are determined only ex post.
[274] Richard A. Posner, *Regulation (Agencies) Versus Litigation (Courts): An Analytical Framework*, *in* REGULATION VERSUS LITIGATION: PERSPECTIVES FROM ECONOMICS AND LAW 11, 13–19 (Daniel P. Kessler ed., 2010).
[275] Susan Rose-Ackerman, *Regulation and the Law of Torts*, 81 AM. ECON. REV. 54, 54 (1991) (ex ante regulation requires that an agency "decide individual cases instead of judges and juries; resolves some generic issues in rulemakings not linked to individual cases; uses nonjudicialized procedures to evaluate technocratic information; affects behavior *ex ante* without waiting for harm to occur, and minimizes the inconsistent and unequal coverage arising from individual adjudication").
[276] Samuel Issacharoff, *Regulating After the Fact*, 56 DEPAUL L. REV. 375, 380 (2007).
[277] Charles D. Kolstad, Thomas S. Ulen, and Gary V. Johnson, *Ex post liability for harm vs. ex ante safety regulation: substitutes or complements?*, 80 AM. ECON. REV. 888, 888 (1990) (emphasis omitted).

particular, can be mitigated by the promulgation of ex ante rules.[278] In the machine learning context, ex ante regulation can provide off-the-rack templates for disclosure, transparency standards, and design mandates for privacy and equality norms. All these mitigate ex post uncertainty, as well facilitating diagnosis after the fact. But ex post exposition and review to ensure that constitutional design decisions have been taken, and that an instrument has not diminished in accuracy because of brittleness remains a necessary complement.

Even assuming this need for ex post enforcement through litigation, questions remain about the form of litigated oversight. I emphasize here the virtues of aggregate litigation over retail challenges to outcomes in specific cases. Aggregate challenges (such as class actions, facial challenges, and the like) usefully direct attention to system-wide causes of constitutional harm. They invite remedies fashioned to account for the interests of all regulated subjects—and not, say, instruments that improve on accuracy for a subset of the regulated population while increasing errors for a majority. This aggregate/retail distinction is not the sole important question of remedial decision choice (and is surely not important *only* in this context). But I focus on it because of its singular importance in the machine learning context.

A. Regulating Algorithms

Administrative agencies have long been "key actors responsible for implementing congressional commands contained in statutes."[279] In comparison to courts, agencies boast comparative institutional advantages in expertise and responsiveness.[280] Ex ante regulation is possible by both federal and subnational agencies. States such as California are enacting statutory protections of privacy that will impinge on the way in which private actors can deploy machine learning.[281] Municipalities such as Seattle and Santa Clara have enacted regulations covering not only the collection but also analysis of surveillance data.[282] These examples are unlikely to prove isolated. To the contrary, interjurisdictional diffusion, imitation, and competition likely will generate healthy rates of regulatory innovation even absent federal action.

---

[278] *Id.* at 889; *see also* Steven Shavell, *A model of the optimal use of liability and safety regulation*, 15 RAND J. ECON. 271, 272 (1984) ("[I]t is often socially advantageous for the two means of controlling risk to be jointly employed—for parties to be required to satisfy a regulatory standard and also to face possible liability.").

[279] Bertrall L. Ross II, *Embracing Administrative Constitutionalism*, 95 B.U. L. REV. 519, 527 (2015); *see also* Sophia Z. Lee, *Race, Sex, and Rulemaking: Administrative Constitutionalism and the Workplace*, 96 VA. L. REV. 799, 801 (2010) (defining administrative constitutionalism as "regulatory agencies' interpretation and implementation of constitutional law"); Gillian E. Metzger, *Administrative Constitutionalism*, 91 TEX. L. REV. 1897, 1900 (2013) (describing administrative constitutionalism as "encompass[ing] the elaboration of new constitutional understandings by administrative actors"). Of course, this might change if constitutional doctrine changes. *Cf.* Gundy v. United States, 139 S.Ct. 2116, 2131(2019) (Gorsuch, J., dissenting) (casting doubt on rule-making delegations to federal agencies).

[280] Margaret H. Lemos, *Special Incentives to Sue*, 95 MINN. L. REV. 782, 786–87 (2011).

[281] *See, e.g.,* Assembly Bill No. 375, Ch. 55, "An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy," June 28, 2018 ("[G]rant[ing] [] consumer[s] a right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of 3rd parties with which the information is shared."); Dipayan Ghost, *What you need to know about California's new data privacy law*, HARV. BUS. REV., JULY 11, 2018, https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law [https://perma.cc/49DF-ADV4] (summarizing the background and effects of California's Consumer Privacy Act).

[282] Seattle, Wash. Mun. Code § 14.18.010 (regulating "any electronic data collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology acquired by the City or operated at the direction of the City"). Similar measures include Santa Clara County, Cal., Code of Ordinances div. A40, § A40-7(c) (2018).

Ex ante regulation can be used to create substantive standards or to create a disclosure regimes. I address each of these possibilities in turn.

1. Substantive Regulatory Interventions

The most common ex ante regulatory intervention relevant to machine learning in nonpublic hands is privacy by design. Both the European Union and the federal government had adopted mandates of that kind.[283] Scholars have devoted considerable attention to refining privacy-by-design principles.[284] I will focus here on regulating for equality. This is useful because the regulatory focus on privacy to date has made equality values more costly to enforce because it has deprived regulators and private parties of information necessary to identify discriminatory phenomena.[285] For example, a 2019 Illinois statute regulating the use of machine learning in hiring decisions mandates the destruction of video data within thirty days of an interview upon an interviewee's request—a measure that likely makes it more difficult to ascertain ex post whether unlawful discrimination may have occurred in the hiring process.[286] As legislators and agencies consider how public uses of machine learning are managed, greater attention to computational infrastructure conducive to equality norms is thus useful. In that spirit, this section outlines an equality-related regulatory interventions: a mandate to adopt the 'best feasible' nondiscriminatory algorithm. This idea, I should note in advance, need not be limited to equality norms, but might also have due process and privacy applications.

One regulatory mandate worth exploring works by analogy to the "best available technology" ("BAT") rules employed in several federal environmental statutes.[287] The gist of the idea is that regulating agencies would mandate a BAT requirement for nondiscriminatory (fair) algorithms (although it is possible to engage the same mandate in respect to security against data breaches). Under the Clean Water Act, for example the EPA determine the "best practicable control technology" by accounting, *inter alia*, for "the total cost of application of technology in relation to the effluent reduction benefits to be achieved from such application, . . . the age of equipment and facilities involved, the process employed, the engineering aspects of the application of various types of control techniques, process changes, [and] environmental impact."[288] BAT mandates of this ilk allow the agency to derive an appropriate regulatory standard from the observed distribution of industry

---

[283] *See* Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 22-34 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [https://perma.cc/TK9B-X9BL]; Council Regulation 2016/679, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Dir 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1

[284] *See, e.g.,* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 12 (2018) (offering a framework for law and policy that uses privacy by design to regulate consumer protection and surveillance); Mulligan & Bamberger, *supra* note 264, at 740-80 (proposing a new institutional, technological, and conceptual framework to preserve privacy-by-design); Waldman, *supra* note 265, at 1266-85 (using products liability to answer privacy-by-design's open questions).

[285] Mulligan & Bamberger, *supra* note 264, at 728 ("Limiting the availability of attributes like race, gender, and nationality can limit blatantly intentional discrimination but confounds efforts such as this to root out more invidious forms of discriminatory profiling."); *accord* Dwork & Mulligan, *supra* note 240, at 37.

[286] Artificial Intelligence Video Interview Act, 820 Ill. Comp. Stat. Ann. 42/1.

[287] *See, e.g.,* 33 U.S.C. § 1311(b)(2) (requiring Best Available Technology economically achievable for toxic pollutants under the Clean Water Act).

[288] *Id.* § 1314(b)(1)(B).

practices.[289] Closer to the context at hand, they have been proposed as a liability rule for website's responsibilities respecting copyright enforcement.[290]

BAT rules might be implemented in a number of different ways. For example, they might be framed in general terms so as to impose a burden on regulated actors to select or develop instruments that minimize a set of race- or gender-related costs and benefits, or to maximize certain outcomes. Rather than directing those actors to employ a preselected instrument, the mandate would leave it to courts to ascertain what counted as a BAT through after-the-fact litigation. This leverages the possibility that regulated actors are better positioned than agencies to identify and develop mechanisms for optimizing over costs and benefits. Alternatively, an agency might simply promulgate an openended "list of best available technologies be determined ex ante" from which regulated entities would select.[291] This pathway would place a burden on the regulating agency to identify equality-favoring innovations ex ante. The agency might derive this information from observation of private market behavior, or alternatively, through an information-revelation mechanism such as a system of prizes or research grants.[292] Finally, a BAT for constraining discriminatory effects might entail the crafting of an equality term that can be included in a classifier equation.[293] Of course, any of these regulatory approaches requires the agency to define ex ante the form of (racial or gender) equality it deems important.

BAT mandates of this form, in sum, illustrate the kinds of substantive mandates that can be used to elicit ex ante salutary forms of algorithmic action. The example, though, is not meant to be exhaustive. To the contrary, I offer them it to suggest the potential of regulatory mandates, with the expectations that others can and should be imagined.[294]

2. Transparency and Disclosure Mandates

Another pathway for ex ante regulation focuses on disclosure of various sorts—or forms of what has come to known as transparency and explainability in algorithmic design. I begin by offering a cautious note about the ambiguous meaning and potential costs of transparency. I then explore specific ways in which these difficulties can be resolved. Finally, I identify some specific disclosure

---

[289] Jonathan S. Masur and Eric A. Posner, *Norming in Administrative Law*, 68 DUKE L.J. 1383, 1396–97 (2019); *see also* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 2024-25 (2017) (offering this suggestion in respect to machine-based testimony).

[290] Lital Helman and Gideon Parchomovsky, *The Best Available Technology Standard*, 111 COLUM. L. REV. 1194, 1217-18 (2011).

[291] Helman & Parchomovsky, *supra* note 290, at 1224.

[292] For the relative merits of prize mechanisms, see Brian D. Wright, *The Economics of Invention Incentives: Patents, Prizes , and Research Contracts*, 73 AM. ECON. REV. 691, 696-700 (1983).

[293] This is suggested in an unpublished paper. Michele Samorani et al., *Overbooked and Overlooked: Machine Learning and Racial Bias in Medical Appointment Scheduling*, at 15–16 (October 9, 2019), available at SSRN: https://ssrn.com/abstract=3467047 [https://perma.cc/E8E5-YRJP]. The proposal, however, is novel and should be regarded as only a possibility absent further scrutiny.

[294] In the privacy context for example, one mandate might focus on minimizing the risk of deanonymization. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1716 (2010). While a 2011 comprehensive metastudy of health-related data acknowledged reidentification risk and concluded that it was "insufficient" to draw strong conclusions about the magnitude of such risk, Khaled El Emam, et al., *A systematic review of re-identification attacks on health data*, 6 PLOS ONE 6.12, at 1 (2011),. More recent work underscores the possibility of embedding privacy-protective design features into data to prevent reidentification, including the exclusion of certain features and perturbation of the data, *see* Khaled El Emam, Sam Rodgers, and Bradley Malin, *Anonymizing and sharing individual patient data*, 350 BRIT. MED. J. *h1130, at* 2015): h1139.

mandates that facilitate important ex post judgments about constitutional norms, even though these are not well described as 'transparency' mandates.

Despite a "resurgence" of interest on "explainable artificial intelligence," the precise meanings of that term and its cognate "transparency" remain contested.[295] The former term has even been criticized as a "suitcase word[]" that "pack[s] together a variety of meanings" but that "holds no universally agreed-upon meaning."[296] A threshold, and critical, ambiguity concerns the threshold object of the exercise. A disclosure mandate might focus either on "the mechanism by which the model works" or, alternatively, on a justification or an explanation of a specific classification decision.[297] This is the difference between a request for a global explanation (i.e., providing a covering law that characterizes the algorithm's work) and a local explanation (focused on a specific instance).[298]

Popular writing often seems to assume that machine learning is by necessity inscrutable.[299] And indeed, it is the case that many forms of machine learning architectures are so complicated that their manner of computing outcomes, or their design, cannot be easier conveyed in a nontechnical form. This is acutely so for deep learning instruments.[300] In 2015, for example, Microsoft developed a prize-winning CNN called ResNet.[306a] Not only did ResNet have 152 layers of neurons in its network, it also used a device called skip-connections, which allow neurons in an 'outer' layer to feed directly into neuron layers much deeper in the network's architecture. Accounts of ResNet suggest that there is no easy way to 'explain' how the network operates to a nonspecialist, or to retrace the computational steps needful to reach a particular outcome. If 'transparency' is understood to demand an account of how ResNet works in its particular that is legible to a lay person, it may well be a fool's errand.

But ResNet is not necessary typical of the models currently in common state use. The assumption that all machine learning models are impenetrable is also flawed. For there are other methods, such as decision trees and linear models, that are far more "easily understandable and interpretable for humans."[301] At the global level, therefore, the available scope for explanation is a function of the choice of algorithmic method. The most sophisticated (and hence effective) algorithms in usage now, deep learning instruments, tend to be the most difficult to represent because of their scale, their use of distributed representations, and the iterative nature of their computations.[302] While

---

[295] Tim Miller, *Explanation in artificial intelligence: Insights from the social sciences*. 267 ARTIFICIAL INTEL. 1, 1-2 (2019) (emphasis omitted). Another survey that underscores breadth of the term is Michael Gleicher, *A Framework for Considering Comprehensibility Modeling*, 4 BIG DATA 75, 77–84 (2016).

[296] Zachary C. Lipton and Jacob Steinhardt, *Troubling trends in machine learning scholarship*, *ARXIV PREPRINT arXiv:1807.03341* at 6 (2018).

[297] Zachary C. Lipton, *The mythos of model interpretability*, ARXIV PREPRINT:1606.03490, at 5 (2016); *cf.* Coglianese & Lehr, *Transparency and Algorithmic Governance*, *supra* note 63, at 20-22 (distinguishing "fishbowl" transparency into what government has done, from "reasoned" transparency, which focuses on the reasons for action). Selbst and Barocas distinguish between inscrutability (pertaining to how something works) and nonintuitiveness (why it works that way). Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1089–91 (2018). These margins both concern the choice of method, and not the result.

[298] Amina Adadi and Mohammed Berrada, *Peeking inside the black-box: A survey on Explainable Artificial Intelligence (XAI)*, 6 IEEE ACCESS 52138, 52147-48 (2018) (drawing the global/local distinction).

[299] *See, e.g.,* Knight, *supra* note 14 ("We've never before built machines that operate in ways their creators don't understand. How well can we expect to communicate—and get along with—intelligent machines that could be unpredictable and inscrutable?"). Knight, to be sure, recognizes that he is discussing only a subset of machine learning.

[300] Marcus, *supra* note 51, at 10-11.

[306a] KELLEHER, *supra* note 35, at 170.

[301] Riccardo Guidotti et al. *A survey of methods for explaining black box models*, 51 ACM COMP. SUR. 93, 100 (2019).

[302] KELLEHER, *supra* note 35, at 243-44; Adadi & Berrada, *supra* note 298, at 52145.

there is research ongoing on rendering deep learning instruments more intuitive through a combination of expository tools,[303] global-level transparency mandates focused on how a specific method operates are likely to require a trade-off between competing normative ends of transparency and accuracy. At times this trade-off can be avoided. One way to mitigate it, for example, is to seek "simple rules" that perform (almost) as well as complex instruments, yet are more readily comprehensible.[304]

Within these constraints, an explanation of a classification outcome—why was this person jailed, or that benefit denied?—might proceed in a number of different ways. Like global explanations, outcome-specific explanations can be more or less feasible depending on how they are conceptualized. An outcome could be explained in terms of its designer's goals: *x* result was reached because the algorithm was deigned to do *p*. It could alternatively index the specifics of an instrument's technical architecture (say, the manner in hyperparameters were calibrated).[305] A third form of explanation focuses on causality: To 'explain' a specific outcome might thus be to offer a causal explanation—a formulation that might elide with a method-focused definition of transparency, or that might run into difficulty because of the noncausal quality of much machine-learning inference. In contrast to these approaches—each of which raises technical or conceptual difficulties—recent studies of explanation in the machine learning context instead suggest that the most commonly observed demand from human users is one for "contrastive" explanations. These do not explain the causes for an event per se, but explain the cause of an event relative to some other event that did not occur [306] That is, they give an answer to the question "why *x* and not *y*." A demand for contrastive explanation entails the identification of counterfactuals in which a minimal number of features are changed to reach a different classification; or a justification that links that outcome to some underlying policy judgment or latent variable.[307] Transparency of this kind is a tractable design option in many cases. But which of these implementation mechanism is appropriate will demand on the specific normative questions raised by algorithmic decision-making in a given context.[308]

In addition to these decision-specific options, there is a range of more specific disclosure mandates to facilitate ex post accounting. I offer three examples of these. First, an algorithmic decision should be accompanied by a "datasheet" that records the choices and manipulations of training data, and the "composition, collection process, recommended uses, and so on" of the raiding data.[309] Second, an algorithm should be designed for "auditability . . . to enable third parties to probe and

---

[303] Chris Olah and colleagues, for example, have suggested that "disparate techniques now come together in a unified grammar, fulfilling complementary roles in the resulting interfaces . . . [that] allows us to systematically explore the space of interpretability interfaces, enabling us to evaluate whether they meet particular goals." Chris Olah et al. *The building blocks of interpretability*, 3 DISTILL, e10 (2018). They use this composite method to offer explanations of deep learning tools. *Id.*

[304] *See, e.g.,* Jongbin Jung et al. *Simple rules for complex decisions* 2 (2007), http://www.rshroff.com/uploads/6/2/3/5/62359383/simple-rules.pdf [https://perma.cc/ZW2Q-MR2W] (exploring the availability of "fast, frugal, and clear" decision procedures across a range of domains).

[305] I.e., terms set by human judgment rather than being computed by the machine itself.

[306] Miller, *supra* note 295, at 9 (emphases omitted).

[307] CHRISTOPH MOLNER, INTERPRETABLE MACHINE LEARNING 21–22, 129–30 (2019).

[308] Menaka Narayanan et al., *How do Humans Understand Explanations from Machine Learning Systems? An Evaluation of the Human-Interpretability of Explanation*, ARXIV PREPRINT:1802.00682, at 1–3, 15 (2018) (discussing why different kinds of explanation differ, and how to craft effective responses).

[309] Timnit Gebru et al., *Datasheets for datasets*, ARXIV PREPRINT ARXIV:1803.09010, at 2 (2018).

review the behavior of an algorithm."[310] At a most basic level, this might be done through inclusion of an application programming interface ("API") that facilitates downstream review even without access to the underlying algorithm.[311] Finally, cryptographic commitments embedded in an algorithm's code are a way of ensuring that the same, known decision rules are applied to all regulated subjects.[312] A related possibility, developed by the Open Algorithms project of Imperial College London and the MIT Media Lab, is the use of blockchain as a record to log the manner in which an algorithm is used across particular cases.[313] A similar possible design mandate with the ambition of enabling proof of ex post would require an algorithm to produce "a tamper-evident record that provides non-repudiable evidence of all nodes' actions."[314]

None of these options ought to be impeded by trade secrecy claims on behalf of algorithms' creators.[315] A regulatory agency should mandate that certain parameters and hyperparameters be disclosed alongside a machine's operation. For due process purposes, this might include the nature and origins of the training data; any constraints imposed upon rules that could be learned from that data; the outcome variable; and the latent construct. It is difficult to see how any of these disclosure obligations would impinge upon intellectual property interests in algorithmic design, even on the assumption that such an interest was a substantial one, given the availability of a protective order. Even where a vendor who has sold the state an algorithmic system does claim intellectual property protection, a regulatory could compel the vendor to make public sufficient detail to understand how historical data is translated into prediction or prescription. Agencies not only have clear power to condition access to state contracts on such disclosure, but can appeal to the publicity-oriented justification of intellectual property law itself.[316]

* * *

Because the decisions relevant to those norms are often embedded in the threshold development and design of a machine learning system, regulators are well positioned to generate mandates and constrains conduce to constitutional compliance. There is a wide array of ex ante tools available to regulators wishing to promote constitutional norms in the machine learning state. The taxonomy offered here is not an exhaustive guide to how such regulation should be framed. It rather

---

310 Nicholas Diakopoulos & Sorelle Friedler, *How to Hold Algorithms Accountable*, MIT TECH. REV. (Nov. 17, 2016), https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/ [https://perma.cc/N7H6-7ESV] (emphasis omitted).

311 It is possible to access a black-boxed algorithm via an API to test how certain features (e.g., protected class membership) influences outcomes without disclosing the algorithm's operating rules. Philip Adler et al.. *Auditing black-box models for indirect influence*, 54 KNOW. & INFO. SYS. 95, 96-97 (2018).

312 Kroll et al., *supra* note 117, at 665-67 ("cryptographic commitment," a digitally generated, tamper-proof certification, that assures that "(1) [a] particular decision policy was used and (2) . . . particular data were used as input to the decision policy"). Another precommitment device is the zero-knowledge proof, which can be used to prove that a certain decision policy was actually used without revealing its contents. *Id.* at 668.

313 Bruno Lepri, et al., *Fair, transparent, and accountable algorithmic decision-making processes*, 31 PHIL. & TECH. 611, 622-24 (2018) (describing the implementation of the Open Algorithm project).

314 Andreas Haeberlen, Petr Kuznetsov & Peter Druschel, *PeerReview: Practical Accountability for Distributed Systems*, 41 ACM SIGOPS OPERATING SYS. REV. 175, 175 (2007); *accord* Deven R. Desai & Joshua A. Kroll, *Trust but Verify: A Guide to Algorithms and the Law*, 31 HARV. J.L. & TECH. 1, 10-11(2017) (same).

315 *See* Wexler, *supra* note 121, at 1349–53 (describing the problem with creators protecting their algorithms with trade secrecy claims).

316 Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets As IP Rights*, 61 STAN. L. REV. 311, 332-33 (2008).

presents a first step in developing needful regulatory frameworks for promoting a machine learning state under the rule of law.

B. Litigating the Constitutionality of Algorithms

Ex ante regulation is necessary, but is not sufficient, to promote constitutionalism in the machine learning state. Designers of a machine learning system cannot be certain before the fact of how their instrument will perform across all conceivable circumstances. Learned rules can and do prove brittle in the teeth of unexpected phenomenon.[317] Designers of a machine-learning system, even if subject to robust an ante regulation, may also fail to install or maintain appropriate protections for constitutional norms. Privacy-protective software patches, for example, might not be timely installed. Hardware obsolescence may not be mitigated. A loose fit between the outcome variable and the latent construct of interest may slip into the design. As a result, some form of ex post litigation is necessary even with ex ante regulation in place.

The optimal litigation form for enforcing constitutional norms in the machine-learning state is wholesale and not retail It takes the algorithmic system's operation as the relevant transactional frame. It offers injunctive relief aimed at correction and improvement of that system's operation as a remedy. It should not aim to generate damages or even negative injunctions against machine learning—opt-outs for specific plaintiffs without regard to how the body of regulated subjects are treated.[318] Litigation's ambition, therefore, should be understood in terms of systemic amelioration in line with the wholesale nature of due process, equality, and privacy norms.

A suit to enforce constitutional norms against an algorithmic governance tool will perforce focus on the tool's system-level operation. Due process challenges under *Mathews* will usually turn on one of the ways (discussed above) in which algorithmic architecture can generate substantial numbers of false positives or false negatives.[319] Equality challenges hinging on either intent or classification will centrally concern the choices of training data, features and outcome variable (although the way in which those parameters are analyzed remains up in the air).[320] And privacy litigation will tend to focus similarly on system-level vulnerabilities of software or hardware, and failures to implement privacy by design.[321] Regulatory mandates along certain design margins, such as transparency requirements, cryptographic commitments, and zero-day proofs can facilitate litigation by rendering predictable litigants' access to important empirical and technical details. And a burden shifting mechanism, akin to that used in disparate impact litigation,[322] can be used to weed out insufficiently robust design choices along all three margins.

Constitutional litigation in this vein can be filed either by private or public plaintiffs. A public agency would file suit against a coordinate body within government. Such suits can be observed at

317 *See supra* text accompanying notes 86 to 87.
318 *See* Huq, *Human Decision*, *supra* note 149, at 14.
319 *See supra* Part II.A.2.
320 *See supra* Part II.B.2.
321 *See supra* Part II.C.
322 *See* 42 U.S.C. § 2000e-2(k)(1)(A)(i) (setting forth burden shifting test for Title VII).

both the federal[323] and the state level.[324] States also have "parens patriae" standing to vindicate "quasi-sovereign" interests, which is understood to include a "general interest" in the welfare of its citizens of the sort that a state might try "to address through its sovereign lawmaking powers."[325] The latter might be relevant when constitutional interests are vindicated best through a suit against a private party acting in coordination with the state. A parens patriae suit might be brought, for example, against the supplier of algorithmic software or the hardware on the ground that it (say) created an improper risk to state residents' privacy interests. Such suits are to date unknown. Even if they emerge, it seems likely that public enforcement of constitutional norms in the machine learning context will remain at suboptimal levels. Agencies operating under a state or federal aegis have strong incentives to settle their disputes internally rather than in the court. At present, the necessary institutional infrastructure for the robust enforcement of due process, equality and privacy norms detailed in Part II simply does not exist. In its absence, it seems likely that private litigation will continue to play a role in trying to vindicate constitutional norms in the machine learning state.[326]

The obvious form that private enforcement could take is the class action suit in state or federal court. The Supreme Court has recently restricted state courts' jurisdiction to adjudicate national class actions.[327] But state courts remain able to resolve challenges to state-level policies implemented by state officials. Such suits have been lodged, for example, to challenge deficiencies in the funding of public defense offices and other criminal justice dysfunctionalities.[328] And as noted, there is already a scattering of suits challenging the use of machine learning and similar tools in public benefits, teacher evaluation, and bail contexts.[329] A thousand more flowers, so to speak, should bloom.

Suits challenging algorithmic governance have yielded a range of reforms. In Houston, the challenge to the EVAAS teacher evaluation system led to the school district abandoning algorithmic assessment.[330] In the challenge to the Arkansas benefits system described earlier, litigation revealed that "a third-party software vendor implementing the system [had] mistakenly used a version of the algorithm that didn't account for diabetes issues," and forced the state to correct the flaw.[331] And in an Idaho suit challenging a benefits algorithm, plaintiffs "work[ed] with the Idaho Department of

---

323 Daniel A. Farber & Anne Joseph O'Connell, *Agencies As Adversaries*, 105 CAL. L. REV. 1375, 1415 (2017) (documenting cases).

324 *See, e.g.,* Va. Office for Prot. & Advocacy v. Stewart, 563 U.S. 247, 261 (2011) (permitting *Ex Parte Young* action by an independent state agency against a coordinate agency) .

325 Alfred L. Snapp & Son, Inc. v. Puerto Rico, 458 U.S. 592, 607 & n.14 (1982).

326 For an analogous argument in the antitrust context, see HERBERT HOVENKAMP, THE ANTITRUST ENTERPRISE 58-63 (2005).

327 *See* Bristol-Myers Squibb Co. v. Superior Court, 137 S. Ct. 1773, 1783–84 (2017). For a useful discussion of the case's effects, see Andrew D. Bradt & D. Theodore Rave, *Aggregation on Defendants' Terms: Bristol-Myers Squibb and the Federalization of Mass-Tort Litigation*, 59 B.C. L. REV. 1251, 1281–1306 (2018).

328 *See, e.g.*, Phan v. State, 723 S.E.2d 876, 880–81 (Ga. 2012) (challenging that the state's public defender's system had a systematic breakdown which violated the defendant's Speedy Trial right); Hurrell-Harring v. State, 930 N.E.2d 217, 219 (N.Y. 2010) (challenging that the state's underfunded public defenders deprive indigent defendants the right to Assistance of Counsel); Kuren v. Luzerne County, 146 A.3d 715, 718 (Pa. 2016) (same); *see also* Pub. Def., 11th Judicial Circuit v. State, 115 So. 3d 261, 264-66 (Fla. 2013) (public defenders successfully moved to withdraw from nonfelony cases, citing a lack of resources.).

329 *See supra* text accompanying notes 16 to 19

330 Shelby Webb and John D. Harden, *Houston ISD settles with union over controversial teacher evaluations*, HOUSTON CHRON., Oct . 12, 2017, https://www.chron.com/news/education/article/Houston-ISD-settles-with-union-over-teacher-12267893.php [https://perma.cc/Y4C6-8UCK].

331 Lecher, *supra* note 13.

Health and Welfare to develop a new model."[332] The settlement ultimately accepted by the Idaho district court contained a 24-step process for evaluating and recalibrating the benefits process.[333] None of the cases I have identified ultimately led to a damages award. This militates against the concern that legal challenge will generate disabling liabilities for state and municipal actors out of proportion to their fault.[334] These examples suggest that class-action challenges to algorithmic governance techniques could be successful both in the sense of foreclosing the use of machine learning tools in the absence of appropriate data, and also catalyzing processes of analysis and reconstruction whereby the algorithm is not abandoned but improved. In this fashion, litigation supplies in part the necessary spur to check continuously for deviations from ground truth, to eliminate brittleness, and to account for distortions such as discrimination.

* * *

Regulation and litigation, as in many domains, are complementary partners in the catalysis of constitutional norms for the machine-learning state. Both are in their infancy now. There is almost no regulatory architecture in place at either the state or the federal level at the moment. There are a handful of suits challenging machine-learning tools. They provide useful proofs of concept. But neither the regulatory nor the litigation system is prepared, in sophistication or capacity, for the ongoing diffusion of algorithmic governance. As machine learning tools spread across both the coercive, criminal justice state as well as its regulatory and welfare counterparts, there will be increasing cause to find an effectual regulatory architecture for the algorithmic state. This Part has begun that task by sketching the basic elements of the network of regulation and litigation necessary to ensuring that our algorithmic state is also a constitutional state.

Conclusion

Liberal constitutionalism entails a commitment to maintaining bounds on state power. That commitment is tested when "the technological and military character of governments and the productive relationships" of society change.[335] The "powerful and highly generalizable"[336] technology of machine learning poses a challenge to our constitutional system because it has the capability to transform the relationship between the state and its citizens. I have suggested a suite of responses to that concern here. But more generally, I worry that new computational tools will tend to increase the capability of the state to analyze, predict, and control its subjects behavior. They are also likely to decrease citizens' ability to understand and raises objections to coercive projections of state power. At the limit, the use of those technologies may cast doubt on the necessary conditions for the meaningful play of democratic control.

---

[332] AI Now Institute, *Litigating Algorithms: Challenging Government Use of Algorithmic Decision Systems* 9 (Sept. 20-2018), https://ainowinstitute.org/litigatingalgorithms.pdf [https://perma.cc/9EKU-2AHZ].

[333] Settlement in *K.W. v. Armstrong*, No. 1:12-cv-00022-BLW, at 9-10 (D. Id. Sept. 15, 2016).

[334] The risk of disproportionate liability has led some district courts to limit liability in cases of data breach. *Cf.* Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 368 (M.D. Pa. 2015) ("[F]or a court to require companies to pay damages to thousands of customers, when there is yet to be a single case of identity theft proven, strikes us as overzealous and unduly burdensome to businesses."). While an injunction might also impose costs on a public entity, it creates no perverse incentive to file socially negative value suits.

[335] Shklar, *supra* note 1, at 23-24.

[336] GREENFIELD, *supra* note 8, at 226.

This potential asymmetry in power between the machine learning state and its subjects (formerly citizens) presents a formidable challenge in the medium term. That challenge is most acute and most visible in China, where a range of surveillance and analytic technologies are deployed to suppress political dissent and leash ethnic and religious identity. But we should be under no illusions that the same technologies (and more) cannot find parallel uses in liberal democracies. Nor should we be under any illusion that steps explored here will on their own be sufficient to check the progress of a technocratic illiberalism. Far from it. Legal countermeasures of this ilk to the totalizing shadow of the state are always only adjuncts to larger, democratic efforts to keep the balance between state and citizen from capsizal. They will be effective only if conjoined with popular pressure, of the kind seen most recently in San Francisco's facial recognition ban, to check the machine learning state when doing so remains within reach. It is the scale and passion of such public movements that will determine whether state algorithms comply with the rule of law, or whether instead they will be deployed to temper the democratic project.