Access to Algorithms

Hannah Bloch-Wehba

Drexel University Thomas R. Kline School of Law

Follow this and additional works at: https://ir.lawnet.fordham.edu/flr

Part of the Civil Rights and Discrimination Commons, and the Internet Law Commons

Recommended Citation

Available at: https://ir.lawnet.fordham.edu/flr/vol88/iss4/2

This Article is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Law Review by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact tmelnick@law.fordham.edu.
Federal, state, and local governments increasingly depend on automated systems—often procured from the private sector—to make key decisions about civil rights and liberties. When individuals affected by these decisions seek access to information about the algorithmic methodologies that produced them, governments frequently assert that this information is proprietary and cannot be disclosed.

Recognizing that opaque algorithmic governance poses a threat to civil rights and liberties, scholars have called for a renewed focus on transparency and accountability for automated decision-making. But scholars have neglected a critical avenue for promoting public accountability and transparency for automated decision-making: the law of access to government records and proceedings. This Article fills this gap in the literature, recognizing that the Freedom of Information Act, its state equivalents, and the First Amendment provide unappreciated legal support for algorithmic transparency.

The law of access performs three critical functions in promoting algorithmic accountability and transparency. First, by enabling any individual to challenge algorithmic opacity in government records and proceedings, the law of access can relieve some of the burden otherwise borne by parties who are often poor and underresourced. Second, access law calls into question government’s procurement of algorithmic decision-making technologies from private vendors, subject to contracts that include sweeping protections for trade secrets and intellectual property rights.
Finally, the law of access can promote an urgently needed public debate on algorithmic governance in the public sector.

INTRODUCTION

Government decision-making is increasingly automated. Cities use machine-learning algorithms to track gunshots, determine where to send police on patrol, and fire ineffective teachers. State agencies use algorithms

to predict criminal behavior, interpret DNA evidence, and allocate Medicaid benefits. Courts decide, using “decision-support” tools, whether a suspect poses a risk, eligibility for pretrial release, and how harsh a sentence to impose. The federal government uses algorithms to put individuals on immigrant and terrorist watchlists, make policy decisions about whether and how to change Social Security, and catch tax evaders.

How are these new technologies changing government decision-making? “Algorithmic governance” — a term this Article uses to refer to the use of automated decision-making methodologies by governments to inform the policymaking and adjudicative process — might make decision-making faster, more objective, and more reliable: in other words, more “efficient.” But increasing automation may also make government less participatory and open to public oversight and input.

This Article examines the potential role of the law of access to government proceedings and records in promoting algorithmic transparency and accountability in public sector decision-making.

Courts across the country have already had occasion to consider challenges to automated determinations arising in sectors such as health care, education, welfare, and criminal justice and have repeatedly concluded that due process requires the use of ascertainable public standards that enable those affected to challenge their determinations. In case after case, litigants have

---

16. See infra Part I.
sought—and successfully obtained—disclosure of key information about automated decision-making methodologies in the public sector.

These challenges are best interpreted as efforts to vindicate an important set of transparency interests: the right to know why and how the government reached a particular decision that affects someone. As such, these cases resonate within the broader framework of transparency law, which aims to open government decision-making to public view. Yet efforts to promote algorithmic transparency have largely overlooked the body of law that governs access to government proceedings and records: the Freedom of Information Act (FOIA), its state equivalents, and the First Amendment.

By codifying expectations regarding the government’s disclosure of information to the public, the law of transparency and access operates both to protect the balance of power between the public and the government and to ensure that key information regarding government decision-making is open to public scrutiny. While these concerns overlap somewhat with individual interests in understanding how the government has reached decisions that affect people, they are also distinct in their operation and effect. Because transparency law protects public rights of access to government, its remedies—chiefly, the disclosure of government records—can be sought by those who are unaffected by the particular decisions or policies they wish to expose.

17. See infra Part I.


20. But see Brauneis & Goodman, supra note 13, at 133; Coglianese & Lehr, supra note 14, at 22; Paul Schwartz, Data Processing and Government Administration: The Failure of the American Legal Response to the Computer, 43 HASTINGS L.J. 1321, 1376 (1991) (“The creation of transparent systems of data processing updates a traditional American belief in open government.”).

21. See, e.g., Margaret B. Kwoka, FOIA, Inc., 65 DUKE L.J. 1361, 1364 (2016) (describing how FOIA was intended to benefit newsgathering, “facilitating democratic participation and exposing potential government corruption or malfeasance”) [hereinafter Kwoka, FOIA, Inc.; see also Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 587–88 (1980) (noting that the First Amendment has a “structural role” in protecting republican governance, based on “the antecedent assumption that valuable public debate—as well as other civic behavior—must be informed”); Margaret B. Kwoka, Deferring to Secrecy, 54 B.C. L. REV. 185, 202–03 (2013) [hereinafter Kwoka, Deferring to Secrecy] (describing how FOIA’s imposition of de novo review protects the “democratic process of holding the agency accountable to the public” in the face of agency self-interest).

22. These features are somewhat controversial, in part, because they have permitted commercial requesters to reap substantial profits from gathering and reselling government records and, in part, because the onerous burdens on the administrative state tend to threaten the “capacity and legitimacy of [government] institutions.” See David E. Pozen, Transparency’s Ideological Drift, 128 YALE L.J. 100, 156, 159 (2018) (describing this feature of U.S. transparency law as the “transparency entitlement” and noting some of its deleterious
The public-facing structure of transparency law can make several important contributions to algorithmic transparency and accountability. First, it can shift the burden of challenging algorithmic opacity from those who are affected—often poor, underresourced litigants—to the press and the public, opening up new avenues to address opacity.23 Second, transparency law calls into question the legality of procurement practices that shield third-party vendors from public scrutiny entirely.24 Third, transparency law can create more enduring prospective obligations for government to disclose its policies and procedures on a proactive basis.25

Understanding how transparency law maps onto algorithmic governance sets the stage for future work that addresses the next generation of automation. As the government procures and relies upon newer, more sophisticated decision-making technologies, such as machine learning, it also makes decisions more opaque, harder to explain, and less attributable to specific causes.26 The greater the decisional power of the technology, the higher the risk that arbitrary or opaque decisions might evade explanation. And this apparent arbitrariness, in turn, has engendered potent critiques of the credibility,27 fairness,28 and due process29 implications of decision-making by algorithms significant for our understanding of how automation might jeopardize individuals’ civil rights and liberties.

These features—some might call them bugs30—have prompted calls for new mechanisms of transparency and accountability in the age of algorithms.31 The trouble is that few can agree on how, exactly, society can advance these values. Scholars have touted a range of mechanisms as

...
promoting algorithmic transparency and accountability.32 The extensive, and growing, menu of options includes reverse engineering,33 algorithmic impact statements,34 “value-centered design,”35 and audits.36 Others have concluded that machine learning poses no real threat to transparency at all.37

These contributions have in common a key assumption: simply disclosing the internal workings of many algorithmic decision-making tools—often encoded in source code or models—is insufficient to vindicate accountability and transparency interests. First, disclosure is not only ineffective, it is also legally precluded because these materials are the proper subject of trade secret protections.38 Second, simply disclosing information about how an algorithm reaches a decision is insufficient to make that information meaningful to the subjects.39 As a result, these scholars argue, entirely new mechanisms for promoting algorithmic accountability and transparency are required.40

But the rush to assess how best to promote accountability and transparency in artificial intelligence and machine learning threatens to overlook critical aspects of algorithmic governance in current use. Even though machine learning has not yet been widely deployed in government decision-making, the turn toward algorithmic governance nonetheless already poses serious

34. See, e.g., Selbst, supra note 32, at 168.
37. See generally Cary Coglianese & David Lehr, Transparency and Algorithmic Governance, 71 ADMIN. L. REV. 1 (2019) (contending that algorithmic governance generally can, although is not guaranteed to, comply with the transparency demands articulated within administrative law).
39. See Desai & Kroll, supra note 38, at 10 (“in addition, handing over code often will not enable the political accountability results those in favor of so-called algorithmic transparency desire.”); Selbst & Barocas, supra note 38, at 1107; Sandra Wachter et al., Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, 31 HARV. J.L. & TECH. 841, 862–70 (2018); see also Burrell, supra note 26, at 9.
40. See generally Joshua A. Kroll et al., Accountable Algorithms, 165 U. PA. L. REV. 633 (2017) (arguing that technological tools can promote algorithmic accountability as well as, and in some cases better than, legal and policy interventions).
obstacles to government transparency and accountability. Those obstacles are attributable, not to the sophistication of decision-making methodologies but to a more basic shift toward privatization and automation in government. Artificial intelligence and machine learning raise serious, and specific, challenges to transparency and accountability, but this Article leaves for another day the project of considering how transparency law should respond.

This Article contributes to ongoing debates about algorithmic accountability and transparency in three ways. First, by cataloging a range of proprietary algorithmic decision-support and decision-making tools relied upon in different civil, criminal, and administrative contexts, it highlights how extensively privatization and outsourcing have affected civil rights and liberties. This impact extends beyond criminal law enforcement to other cutting-edge cases arising in civil contexts that have received scant scholarly attention. Taken as a group, these cases illustrate an important pattern in challenges to algorithmic decision-making: litigants are equally motivated to seek transparency of the government decision-making process as they are to challenge the substance of algorithmic decisions.

Second, this Article rehabilitates disclosure as a remedy for algorithmic opacity in the public sector. Algorithmic governance in the public sector heightens the interest in disclosure of key information regarding how automated decision-making functions. Disclosure is the core mechanism of U.S. transparency law, which enshrines values of public access to government decision-making. But disclosure has been given short shrift as a mechanism for algorithmic accountability and transparency.

---


44. This Article relates to a growing body of work that studies how the relationship between government and technology companies affects accountability and transparency. See, e.g., Brauneis & Goodman, supra note 13; Catherine Crump, *Surveillance Policy Making by Procurement*, 91 Wash. L. Rev. 1595 (2016); David S. Levine, *The People’s Trade Secrets*, 18 Mich. Telecom. & Tech. L. Rev. 61 (2011); see also Hannah Bloch-Wehba, *Exposing Secret Searches: A First Amendment Right of Access to Electronic Surveillance Orders*, 93
The primary obstacle to transparency is the pervasive practice of invoking trade secrecy to shield the methodologies of automated decision-making from scrutiny.45 Without resources to develop automated decision-making tools in-house, governments have often turned to decision-support systems purchased from the private sector. These systems frequently come with license agreements, memoranda of understanding, or other documentation evincing claims that the contents are trade secrets.46

Viewed from the perspective of transparency law, the invocation of commercial confidentiality and trade secrecy to shield government decision-making from public view is legally suspect.47 These provisions cast doubt on the government’s ability to agree, through contract, to utilize decision-making mechanisms that are inconsistent with these broad public-serving goals. In practice, this sometimes puts government to a difficult choice: reveal a contractor’s trade secret or give up the use of an algorithmic tool altogether.48 Governments should implement transparency values throughout their contracting and procurement processes to ensure that proprietary decision-support tools are consistent with these aims.

Finally, this Article reframes the debate about algorithmic transparency from affected individuals to the affected public.49 Existing scholarship has often considered whether trade secrecy interests should yield to the interests of individuals who are affected by algorithmic decision-making—namely, individuals with a sufficient liberty or property interest at stake.50 In the criminal justice context, scholars and advocates have embraced the use of protective orders to ensure that defendants have access to the algorithms that confer risk scores or analyze DNA or breathalyzer evidence—without jeopardizing trade secrets.51

These compromises between the private vendors’ commercial interests and the liberty interests of those affected by algorithmic governance overlook the public’s separate and independent interest in oversight and monitoring of government decision-making. In the criminal context, the constitutional

---

45. Katyal, supra note 38, at 60 (“In the context of artificial intelligence, we see a world where, at times, intellectual property principles prevent civil rights from adequately addressing the challenges of technology, thus stagnating a new generation of civil rights altogether.”). See also Coglianese & Lehr, supra note 37, at 33 (citing Loomis as support for the proposition that transparency principles do not compel disclosure of source code).


47. See, e.g., Diakopoulos, supra note 33.

48. See discussion infra Part I.B.


50. See, e.g., Citron, supra note 42, at 1254–55; Roth, supra note 27, at 2028; Wexler, supra note 29, at 1349.

51. See, e.g., Wexler, supra note 29, at 1353 (“Courts may issue protective orders to limit the use and distribution of trade secrets beyond the needs of the proceeding.”).
right of access to government proceedings and records casts doubt on whether prosecutors and courts can selectively disclose proprietary algorithms to affected individuals while shielding them from the public. More broadly, selective disclosure tends to ignore the First Amendment’s “structural” role for the press and public in monitoring government proceedings.53

The Article proceeds in four parts. Part I traces the emerging use of, and challenges to, proprietary, automated decision systems in health care, criminal justice, and education. Part II unpacks how these challenges both assert the individual due process rights of litigants and also invoke the larger public interest in support of enhanced transparency. Part III explores the procedural and substantive conflicts between proprietary decision-making on the one hand and government transparency obligations under the First Amendment and FOIA on the other. Part IV briefly sketches some remedial measures that governments might take in order to alleviate concerns about the accountability and transparency of algorithmic governance.

I. THE RISE OF PUBLIC SECTOR ALGORITHMS

It is hardly groundbreaking to observe that algorithms are increasingly prevalent in the public sector. New technologies are supposed to make it easier for humans to make difficult decisions—and where is decision-making more difficult, or more important, than in government? The kinds of decisions that the public sector must make are high stakes: whether an individual who is arrested for murder, but claims he acted in self-defense, should be released from detention or stay in jail; whether a person who is profoundly disabled and requires home care in order to avoid being institutionalized should receive $70,000 or $140,000 in Medicaid waiver benefits; whether a public school teacher whose students perform worse than their peers on a statewide test should be laid off.56

These scenarios are not simply hypotheticals. They represent flash points between emerging methods of algorithmic decision-making and the rights of individuals to understand and challenge those decisions. This Part surveys these conflicts, observing that increasing automation and privatization of

57. Citron, supra note 42, at 1252.
decision-making are at the root of new challenges to algorithmic determinations.

A note about methodology: these cases and contexts were chosen because they keenly present the clash between vendors that provide algorithmic decision-making tools, governments that deploy such tools, private individuals who wish to challenge these outcomes, and the general public. Although the case law remains relatively scant, it was surprising to see the number of reported decisions that illustrate these structural dynamics prevalent in challenges to algorithmic opacity. Nonetheless, this account is not exhaustive, and other cases likely exist that illustrate these patterns.

Although this dynamic has garnered particular attention in the context of the criminal justice system, the proprietary nature of many algorithmic governance tools poses significant obstacles to individuals who seek to challenge algorithmic determinations in a variety of contexts. The precise substance of these disputes matters less than the overarching pattern: these cases frequently present a clash of interests between government’s increasing reliance on proprietary tools, procured from private contractors or vendors, and transparency requirements.

The clash between transparency and proprietary interests is particularly pronounced when individuals seek to challenge the outcomes of adjudications—whether judicial or administrative—that affect their civil rights and liberties. Notably, however, the new challenges to algorithmic governance do not rise and fall on the substance of an algorithmic decision. Rather, the most successful challenges to algorithmic decision-making reflect demands for more information regarding the ways in which government is reaching its decisions: in other words, demands for transparency and access to information about the process.

### A. Medicaid

Challenges to proprietary decision-making in the context of Medicaid are illustrative. For years, lower courts have been dealing with procedural due process claims as state Medicaid agencies privatized their decision-making

---


60. See, e.g., Brauneis & Goodman, supra note 13; Coglianese & Lehr, supra note 14; Katyal, supra note 38; Selbst & Barocas, supra note 38.
and began to use algorithmic methods to reduce recipients’ benefits. Examining these cases makes clear that the shift toward algorithmic governance goes hand-in-hand with other measures that are intended to cut costs and have the (perhaps unintended) secondary effect of reducing accountability and transparency as well. Agencies often rely on the “objectivity” or “efficiency” of their data-driven decision-making procedures to justify cost-cutting measures, such as terminating employees or cutting Medicaid benefits. But as agencies turn toward more “objective” decision-making procedures, they often rely on private contractors who use proprietary, closed-source methods to make decisions about these constitutional rights.

The privatization and automation of decision-making regarding Medicaid benefits present clear tensions with principles of procedural due process. When individuals receive Medicaid or other public assistance benefits, those benefits are “treated as a form of ‘property.’” Consequently, Medicaid benefits cannot be reduced or terminated without satisfying certain safeguards set out in the Medicaid Act and the Constitution’s procedural due process guarantees.

These statutory and constitutional protections require the government to explain why and how it decided to terminate or reduce benefits. Under federal Medicaid regulations, notices of terminations or reductions in benefits are required to contain “a clear statement of the specific reasons supporting the intended action.” Moreover, under the Medicaid Act, individuals must receive the opportunity for a “fair hearing” to challenge the denial of benefits. Any “termination, suspension, or reduction of” benefits

---

61. This move is perhaps best understood as a form of “bureaucratic disentitlement.” Michael Lipsky, *Bureaucratic Disentitlement in Social Welfare Programs*, 58 SOC. REV. 3, 3 (1984) (defining “bureaucratic disentitlement” as a mode of “retracement” in which “obligations to social welfare beneficiaries are reduced and circumscribed through largely obscure ‘bureaucratic’ actions and inactions of public authorities”); see also VIRGINIA EUBANKS, *AUTOMATING INEQUALITY* 49 (1st ed. 2018) (describing how Indiana privatized and automated its welfare systems in order to cut costs); Vicki Lens, *Bureaucratic Disentitlement After Welfare Reform: Are Fair Hearings the Cure?*, 12 GEO. J. ON POVERTY L. & POL’Y 13, 13 (2005) (“One of the few avenues for challenging bureaucratic disentitlement is the fair hearing system. However, little is known about how the fair hearing system is faring under welfare reform.”).


63. *Id.*


68. 42 U.S.C. § 1396(a)(3).
or eligibility triggers the statutory requirement for a hearing. In a separate provision of the Act, Congress also required state agencies to base Medicaid waiver budgets on a “methodology that uses valid, reliable cost data [which] is open to public inspection, and includes a calculation of the expected cost of such services.” Likewise, procedural due process requires agencies to employ “ascertainable standards” in decision-making.

These protections remain vital to prevent the wrongful termination of benefits, even as states have increasingly turned toward the private sector to provide various Medicaid services. A 2006 Government Accountability Office report investigating the protection of personal health information found that 96 percent of state Medicaid agencies used vendors to perform various administrative services, including enrollment and benefits management. As states have turned to managed care organizations to administer benefits, private companies have become the primary providers of public Medicaid benefits in many states.

In turn, vendors have adopted a range of new algorithmic tools to help make the management of Medicaid more efficient. Yet new mechanisms for administering Medicaid have created tensions with constitutional and statutory demands of openness. In 2015, a group of West Virginians with severe intellectual and developmental disabilities brought suit against the state’s Department of Health and Human Resources, challenging the state’s reliance on a proprietary algorithm to reduce critical Medicaid benefits. The plaintiffs had received Medicaid waiver benefits for decades under the state’s home and community-based care program, which supported the

69. 42 C.F.R. §§ 431.201, 431.206(c).
70. 42 U.S.C. § 1396n(j)(5)(D).
71. Lightfoot v. District of Columbia, 448 F.3d 392, 400 (D.C. Cir. 2006); Holmes v. N.Y.C. Hous. Auth., 398 F.2d 262, 265 (2d Cir. 1968); Hornsby v. Allen, 326 F.2d 605, 612 (5th Cir. 1964).
provision of key services that enabled them to live at home or in the community instead of being institutionalized.76

These benefits were administered by a “waiver administrator,” APS Healthcare Inc., a private company tasked with allocating waiver benefits and generating budgets for the benefits and care for which the recipients were eligible.77 Under its contract, APS bore responsibility for annual assessments to measure recipients’ “abilities and needs,” to ensure that recipients of waiver funds were eligible to receive funds and to come up with a budget allocating benefits to each recipient.78 It did so by gathering data through interviews and “standard assessment tools” and then applying a proprietary algorithm that generated a budget to cover authorized waiver benefits.79

The problem was that each year, the algorithm spat out a budget that appeared totally unrelated to the actual cost of providing the care which the plaintiffs required.80 APS sent letters to each recipient “notifying him or her of the budget amount without explanation as to how that number was determined.”81 In many cases, the algorithm-generated budget was slashed by tens of thousands of dollars from the year before. But the plaintiffs’ conditions were stable; most of them had not improved in functionality or ability since they were teenagers, suggesting that, year over year, they would require roughly the same benefits and hours of services.82

Nonetheless, the plaintiffs had little success in appealing to human decision makers to reverse the algorithm’s senseless, arbitrary, and unexplained reductions in benefits. In boilerplate letters, APS contended that it could not exceed the “algorithm-generated budget.”83 The plaintiffs had no further success at the “fair hearings” required by the Medicaid Act. Both the contractor and administrative judges were highly deferential to the algorithmic decision-making process, refusing to override—or even investigate—the algorithm’s conclusions.84

The results were catastrophic. One plaintiff, Tara R., a twenty-seven-year-old woman who has “cerebral palsy, a severe intellectual disability, and limited hand functioning,” functioned at an “age equivalent of nine months.”85 She lived at home with her father and her disabled stepmother until 2014 when her benefits were cut from about $130,000 to about $72,000, making it impossible to keep her in her family home. When the benefits were
slashed, Tara was moved to an emergency care facility and then to a group home, where she became “lethargic” and “unwilling to engage with others.” Due to these changes, the plaintiffs alleged, Tara was at “serious risk of being institutionalized.”

The court rightly rejected this framework, agreeing with the plaintiffs that the APS algorithm could not satisfy the Constitution’s procedural due process requirements. Noting that the government had provided “no information as to what factors are incorporated into the APS Algorithm, how each factor is weighted, or the overarching methodology APS utilizes,” the court faulted APS for failing to employ “ascertainable standards” in making their determinations. Moreover, APS had failed to even include “any individualized rationale” for the budgets allocated to the plaintiffs, making it impossible for plaintiffs to “meaningfully challenge” the budgets. Concerned that the “lack of transparency” in the algorithm rendered the determinations “potentially rudderless,” the district court concluded that the APS decision-making process created an “unacceptable risk of arbitrary and ‘erroneous deprivation[s].’”

But these problems were not irresolvable. While the court enjoined the department from continuing to use the APS algorithm, it reasoned that requiring the state to develop a decision-making methodology that actually used ascertainable standards would not impose an undue “fiscal or administrative” burden. In response, West Virginia developed a new system that replaced the proprietary APS algorithm with “matrices employing a number of clearly identified variables based on a combination of a member’s living situation and answers to specific questions during the member’s annual assessment.” The state promised that the matrix would be “publicly available” and that recipients would be able to challenge both the accuracy of the static factors that constituted inputs into the matrix and the application of the matrix itself. Concluding that the new system sufficiently remedied the due process flaws in the APS algorithm, the court lifted the injunction.

Secretive determinations about benefit eligibility have widespread implications for a range of other interests, including those of other beneficiaries, possible future beneficiaries, their attorneys and social

---

86. Id. at 32–33.
87. Id. at 34.
89. Id.
90. Id.
91. Id. at *11 (alteration in original) (quoting Town of Castle Rock v. Gonzales, 545 U.S. 748, 792 (2005) (Stevens, J., dissenting)).
92. Id.
94. Id. at *10.
95. Id. at *1.
workers, and even state and federal taxpayers. But West Virginia is hardly alone in resisting disclosure of these decision-making methods. A similar case arising in Idaho makes plain the clash between privatized and automated governance on the one hand and due process guarantees on the other. Like the West Virginia plaintiffs, the Idaho plaintiffs challenged the state’s use of a proprietary, secret methodology to determine their individual budgets for home and community-based waiver benefits. The state offered a compromise: it would disclose the methodology to the plaintiffs, but only if they assented to a confidentiality agreement that provided that the “details of the budget-setting methodology... may not be discussed or revealed to anyone, in any manner, except for purposes of administrative appeal and judicial review.”

Idaho’s position that its methodology was a “trade secret” ran headlong into its statutory obligation to use a methodology that was “open to public inspection.” The parties—and the court—ultimately rejected this attempt to shield the methodology from public disclosure. Instead, after some back-and-forth, the parties stipulated to a preliminary injunction that the agency would make the budget-calculating tool, as well as a range of supporting documents necessary to understand the tool, available to participants in the waiver program upon request. In addition, the department promised to make most of the same materials available to members of the public under Idaho public records laws.

Though Idaho’s attempt at a compromise ultimately failed, its invocation of trade secrecy exemplifies a troubling trend in approaches to algorithmic accountability. Idaho’s offer to make the information available to plaintiffs, subject to a gag order that prevented them from discussing the methodology, typifies what I call “atomized disclosure”—an approach that seeks to solve due process problems by disclosing information to the affected parties, but only on the condition that they not further disclose it. For the reasons discussed in Part IV, atomized disclosure is highly problematic: it creates serious First Amendment concerns, public policy issues, and inefficiencies.

B. Education

Proprietary algorithmic governance has invited due process challenges in other sectors as well. As school systems have attempted to become more

96. See generally K.W. ex rel. D.W. v. Armstrong, 789 F.3d 962 (9th Cir. 2015).
99. Plaintiffs’ Brief at 11, supra note 97 (requiring budgets to be based upon “a methodology that uses valid, reliable cost data, is open to public inspection, and includes a calculation of the expected cost of such services”).
101. Id.
102. Id. at 5.
accountable, they have turned toward data-driven tools to measure educational outcomes and improve educational effectiveness. These tools have altered educational practices at all levels of the school system, transforming how teachers engage students in the classroom, how states rate school performance, and how districts measure progress. As in the context of Medicaid privatization, the mechanisms of data-driven education reform are also often privately developed, further entrenching private power in classroom teaching, assessment, and data collection itself. These new practices are also occurring within the political context of a push for “free-market” reforms that map the practices of for-profit businesses onto public institutions.

“Value-added assessment” reflects this push toward data-driven education policy. Value-added assessments, or “value-added measures,” assess teacher quality by examining and tracking student test scores in order to measure the effect that teachers have on student performance over time. Value-added


106. For a discussion of HISD, see infra Part I.B.


108. RAVITCH, supra note 107, at 177–78 (“These free-market reformers advocated testing, accountability, merit pay, and charter schools, and most were notably hostile to unions. The unions objected to the reformers’ efforts to judge teachers solely by their students’ test scores, and the reformers sought to break the powers of the unions.”).

assessments are used beyond classroom teaching as well: they can also shed light on the soundness of teacher education itself.110

Like privatization in health care, value-added assessments also purport to be a more “objective” way to cut costs in a financially precarious environment. Budget shortfalls in school districts across America have prompted some districts to lay off teachers.111 Vividly invoking the language of private enterprise, a 2001 report supportive of value-added measures compared educational systems to other businesses, writing, “[M]anagers in most industries would attempt to target layoffs so as to cause as little damage as possible to productivity—less productive workers would be dismissed or furloughed before more productive workers.”112

Teachers’ unions have been at the forefront of efforts to resist these transformations and have fought against district efforts to cut costs by terminating teachers who do not measure up in “value-added” terms. A recent case from Houston, Texas—one of the largest school districts in the country113—illustrates a successful union-led effort to end the district’s reliance on “privately developed algorithms” to determine whether public school teachers were “ineffective” and should be terminated.114 Just as in the Medicaid cases, the case concerned the outsourcing of government services to a private company that employed proprietary algorithms to make critical decisions that implicated due process rights.115

The Houston Independent School District (HISD) had contracted with SAS, a private company that developed a “value-added statistical model” known as the Educational Value-Added Assessment System (EVAAS), to aid in evaluating teacher effectiveness.116 Teachers who have tenure, or who are employed under “continuing contracts,” have a “property interest in continued employment.”117 But HISD made it a goal to “exit” its


115. See generally id.

116. Id. at 1172.

“ineffective” teachers and to retain only those who showed sufficient student growth, as measured by the EVAAS.\textsuperscript{118}

The new policy resulted in the dismissal of at least twelve teachers on continuing contracts.\textsuperscript{119} But because of the proprietary nature of the EVAAS algorithm, the teachers and school district lacked sufficient information to understand how the program functioned.\textsuperscript{120} The teachers and the union who challenged the program described it as “complex and opaque.”\textsuperscript{121} Because SAS treated the software and algorithms as “trade secrets” and refused to divulge them, not even HISD had access to them.\textsuperscript{122}

Like the Medicaid cases, the HISD case presented a significant conflict between the plaintiffs’ desire to access information about how the EVAAS methodology functioned, the claimed interest in secrecy, and the public interest. In the course of discovery, the parties negotiated a framework through which SAS would disclose certain trade secrets—including the source code, models, and methodologies for the EVAAS—to the plaintiffs’ attorneys and experts on an “attorney eyes only” basis.\textsuperscript{123} The court entered a protective order that provided, in part, that none of the protected information could be disclosed to anyone outside the scope of the litigation.\textsuperscript{124} Shortly after the court entered the protective order, the plaintiffs’ expert, Dr. Jesse Rothstein, inspected the source code for EVAAS.\textsuperscript{125} He then prepared an expert report which concluded, in part, that teachers could not “meaningfully verify” their EVAAS scores.\textsuperscript{126}

The teachers’ union posted a litigation update on its website referring to Dr. Rothstein’s report.\textsuperscript{127} SAS promptly filed a motion for contempt and for sanctions, complaining that the blog post—which concededly contained none of the company’s trade secrets or other proprietary information—violated the protective order because it could only have been written based on Dr. Rothstein’s “observations [and]/or conclusions” of EVAAS.\textsuperscript{128} In SAS’s view, the protective order meant to “prevent Plaintiffs and all of Plaintiffs’

\textsuperscript{118} HISD, 251 F. Supp. 3d at 1174–75.
\textsuperscript{119} Id. at 1175.
\textsuperscript{120} Id. at 1176 (finding that teachers lack access to “the computer algorithms and data necessary to verify the accuracy of their scores”).
\textsuperscript{121} Plaintiffs’ First Amended Complaint at 14–15, HISD, 251 F. Supp. 3d 1168 (No. 4:14-cv-01189), ECF No. 23.
\textsuperscript{122} HISD, 251 F. Supp. 3d at 1176.
\textsuperscript{123} See generally Protective Order over SAS Institute Inc. Information, HISD, 251 F. Supp. 3d 1168 (No. 4:14-cv-01189), ECF No. 47-1.
\textsuperscript{124} Id.
\textsuperscript{125} Order at 3, HISD, 251 F. Supp. 3d 1168 (No. 4:14-cv-01189), ECF No. 59.
\textsuperscript{126} Id.
\textsuperscript{127} See generally Exhibit C, HISD, 251 F. Supp. 3d 1168 (No. 4:14-cv-01189), ECF No. 54-3.
\textsuperscript{128} SAS Institute Inc.’s Response to Plaintiffs’ Motion for Interpretation of Protective Order and Motion for Contempt at 5, HISD, 251 F. Supp. 3d 1168 (No. 4:14-cv-01189), ECF No. 54 (alteration in original).
experts from *continuing any public discourse against EVAAS.*" The court rejected SAS’s “overly broad interpretation,” finding that, if adopted, it would “inhibit legitimate discussion about the lawsuit” among union members and among the general public.

The court was equally suspicious of SAS’s secrecy claims on the merits and agreed that relying on a secret algorithm, the outcome of which the plaintiffs could not challenge, raised serious procedural due process concerns. Most significantly, the methodology could not establish the reason for a teacher’s dismissal “in sufficient detail so as to enable him to show any error that may exist.” Those concerns were not remediated by HISD’s effort to make available general information about the EVAAS methodology. As in the West Virginia case, the court agreed with the plaintiffs that the use of a secret, proprietary methodology would make it impossible for the affected party to raise a meaningful challenge at a hearing.

This did not mean that the court would require SAS to disclose its trade secrets—the court recognized that the plaintiffs could not constitutionally “put SAS out of business.” But if the methodology was unconstitutional, the policy likely had to be overturned. A few months after the court denied the school district’s motion for summary judgment, the district settled with the union, abandoning EVAAS and paying the union’s attorney’s fees.

C. Criminal Law Enforcement

1. Policing

Proprietary algorithmic governance is widespread in policing. Consider the example of the gunshot detection company ShotSpotter: the service, which is employed by over ninety jurisdictions across the country, uses sensors to discern the sound of gunfire and triangulate its location, pushing a notification to emergency services. Cities subscribe to ShotSpotter’s services; the company installs the sensors, and the city receives the notifications from the company’s software. But ShotSpotter has often taken the view that the data it generates about where gunshots occur is a

129. Id. at 6 (emphasis added).
130. Order, supra note 125, at 6.
132. Id. at 1176.
133. Id. at 1178.
134. Id. at 1179.
138. Id.
proprietary trade secret. In one letter, *Forbes* reported, ShotSpotter’s CEO emphasized the company’s position that its data “is not crime data” at all.

When journalists and researchers began requesting the data from police, ShotSpotter sent out a “nationwide memo” urging cities not to disclose it. ShotSpotter—and some municipalities—took the position that, pursuant to contract, the data was not a matter of public record. As a result, researchers were limited to analyzing data from the handful of jurisdictions that released it—over ShotSpotter’s objections—or purchased it directly from ShotSpotter.

2. Bail

Proprietary decision-making is also of increasing relevance in criminal prosecutions. Algorithmic governance is the topic of significant interest in the context of pretrial release determinations, partially prompted by a nationwide reckoning with the injustice of cash bail. Over the last several years, a surge in activism by community bail funds, lawsuits challenging the constitutionality of money bail, and legislative reconsideration of money bail have substantially shifted the conversation about pretrial detention. In one report, a California working group on pretrial detention reform pointedly


141. Brauneis & Goodman, supra note 13, at 155 n.197.

142. Jason Tashea, *Should the Public Have Access to Data Police Acquire Through Private Companies?*, A.B.A. J. (Dec. 1, 2016), www.abajournal.com/magazine/article/public_access_police_data_private_company [https://perma.cc/5DJ5-BQ7E] (“[B]usiness and political interests are curtailing the public’s access to the data, which could be used to improve public safety, police accountability and citizens’ understanding of the nature of crime in their communities.”).


144. See, e.g., ODonnell v. Harris County, 892 F.3d 147 (5th Cir. 2018); *In re Humphrey*, 228 Cal. Rptr. 3d 513 (Ct. App. 2018).

reminded its readers, “The United States is one of only two countries that allow for-profit bail bonding; the other is the Philippines.”

The move toward algorithmic governance builds on a long history of quantitative, actuarial measures to assess the risk that specific criminal defendants might pose to society. These “actuarial risk assessment instruments” (ARAIs) have also been deployed in the context of pretrial release decisions, sentencing, parole, and determinations of sexually violent predator status, to name a few. Contemporary ARAIs hold substantial promise to reduce overincarceration by making more accurate decisions about who poses a potential risk to society. This need is particularly pronounced in the contexts of pretrial release and bail: many pretrial detainees are at low risk of committing violent offenses if they are released. Detaining individuals simply because they cannot afford to pay bail is unjust, unconstitutional, and expensive.

In light of these realizations, cities, counties, and states are adopting new decision-making tools—building on the older generation of ARAIs—to help
determine whether a pretrial detainee actually poses a risk to public safety if released. The new generation of risk assessment tools has been heralded as providing an “unbiased, objective evaluation of the risks that defendants pose to society.”

This focus on objectivity comes as no surprise: social scientists have long argued that actuarial risk assessment is both more objective and more accurate than human decision-making. Indeed, actuarial assessments may well be more accurate than “clinical” judgment, which relies on the “professional judgment of the reviewer” to determine potential future risk. Clinical judgment is “crude and subjective” and prone to human error.

But state legislatures and court systems that adopt new risk assessment tools frequently procure them from foundations or the private sector, raising questions about transparency. The Arnold Foundation, for example, provides its “Public Safety Assessment” free of charge to jurisdictions that adopt it—but it compels them to enter into a memorandum of understanding (MOU) that stipulates that they will not treat the tool like an ordinary public record for purposes of freedom of information laws. Unlike ShotSpotter, the Arnold Foundation’s MOU expressly indicates that the foundation has no property interest in the data “provided by” these jurisdictions. But the MOU also provides that the foundation retains “all right, title and interest (including patents, copyrights, trade secrets and trademarks) in and to the Tool.”

3. Evidence

Evidence generated using proprietary methods also occupies a central role at trial. Take, for example, the common use of breathalyzer evidence to demonstrate that a DUI defendant was, indeed, under the influence. Several companies manufacture breathalyzers, or “breath test machines,” including

---

153. Mayson, supra note 59, at 2222 (describing algorithmic risk assessment as the “linchpin of the bail-reform movement”).
154. Milgram et al., supra note 150, at 219.
155. Id. at 220.
157. Id.
158. One social science paper demonstrates the dismissive attitude of many toward clinical judgment, concluding that clinical risk assessments “are often wildly inaccurate and their rationale opaque.” Berk & Hyatt, supra note 7, at 222.
160. See, e.g., No-Cost Memorandum of Understanding Between Laura and John Arnold Foundation and County of Santa Clara, Cal. (June 19, 2018) (on file with author).
161. Id.
162. See, e.g., Ram, supra note 49; Roth, supra note 27; Wexler, supra note 29; see also Aurora J. Wilson, Discovery of Breathalyzer Source Code in DUI Prosecutions, 7 WASH. J.L. TECH. & ARTS 121 (2011).
Dräger (which makes the AlcoTest 9510) and Intoxilyzer. Defendants in dozens of state courts have sought discovery of the source code of these tools, arguing that expert analysis of the source code is essential to be able to confront the evidence against them. But many courts have concluded that the prosecution does not “possess” the source code because it is owned by the private vendor.

When the vendors have disclosed the source code, it is frequently subject to an expansive protective order. For instance, Dräger has disclosed source code in multiple criminal proceedings, pursuant to a protective order. But when two defense experts who had examined the code presented a report describing its flaws at an annual convention of DUI lawyers in 2017, the company sent them a cease-and-desist letter, contending that the allegations were defamatory and violated the order—despite the fact that the report did not contain any of the source code itself. The experts ultimately settled with Dräger, although some defense attorneys believed the company was interpreting its protective order too broadly.

Defendants’ experiences with DNA evidence are equally instructive. Courts in numerous jurisdictions have admitted DNA analyses generated by proprietary software, without disclosing the source code to the defendants. In New York City, for example, the city’s crime lab—the Office of the Chief Medical Examiner (OCME)—developed its own probabilistic genotyping tool, the Forensic Statistical Tool (FST). The FST worked by generating a “likelihood ratio” to estimate the probability that a given contributor’s DNA was present in a mixed sample.

---


165. See, e.g., State v. Underdahl, 767 N.W.2d 677 (Minn. 2009); see also Wilson, supra note 162, at 123 n.3 (collecting cases).

166. Wilson, supra note 162, at 123.


168. Id. (“Draeger sent the researchers a cease and desist letter claiming defamation and alleging the two violated a protective order, designed to protect the source code from leaking.”).

169. Id.


Despite the OCME’s extensive use of the FST, the office never disclosed the source code to a single defendant until Kevin Johnson was prosecuted in federal court.\(^{173}\) Johnson was arrested in 2015 after an apartment search turned up two guns. \(^{173}\) OCME used the FST to analyze the samples of DNA obtained from the guns, concluding that it was 156 times more likely than not that one of the guns contained Johnson’s DNA. When Johnson requested access to the FST source code for expert analysis and review, the government refused to comply, arguing that the FST was “proprietary and copyrighted.”\(^{174}\) After a discovery battle, the court concluded that the source code had to be turned over to the defense expert,\(^{175}\) who reviewed the code and concluded that its accuracy should be “seriously questioned.”\(^{176}\)

Despite the significance of the expert’s conclusions—which cast doubt on the thousands of cases in which FST evidence had been used—his report remained under wraps. In order to facilitate discovery, the parties agreed to a protective order under which the source code was designated as “Highly Confidential Material.”\(^{177}\) Accordingly, the report was filed on the docket, but many of its findings remained inaccessible until a nonprofit news outlet, ProPublica, filed a motion to intervene, vacate the protective order, and unseal the source code.\(^{178}\) After ProPublica intervened, the city dropped its claim that the code was proprietary and released it to the reporter, who published it, prompting a public discussion.\(^{179}\)

4. Sentencing

Sentencing proceedings are also being transformed by algorithmic governance. In a now-infamous case, a defendant raised a due process challenge to the use at sentencing of a proprietary algorithmic risk assessment tool called the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS).\(^{180}\) COMPAS, which was developed by the

---

173. Kirchner, supra note 171 (writing that the OCME estimated it had used the tool in over 1300 cases).

180. See generally State v. Loomis, 881 N.W.2d 749 (Wis. 2016).
Northpointe Institute for Public Management, is an actuarial risk assessment tool. COMPAS weighs a number of factors, such as criminal history, education, employment, age, and substance abuse history and generates “risk scores” intended to predict the likelihood of pretrial recidivism, general recidivism, and violent recidivism.

Eric Loomis challenged the use of COMPAS at his sentencing on due process grounds, analogizing the instrument to a presentence investigation report that must be disclosed to the defendant. But Northpointe “consider[ed] COMPAS a proprietary instrument and a trade secret” and contended that its source code could not be disclosed. Without access to information about how the COMPAS tool functions, Loomis argued, its accuracy was questionable.

The court took a middle road. Loomis had an “opportunity to verify” that the inputs into COMPAS—answers to questions about his criminal history, for example—were accurate. But several studies had suggested that the tool was biased and potentially inaccurate. The court held that, because of these ambiguities about the tool’s accuracy, the sentencing court must be notified regarding both the proprietary nature of the tool and its potential inaccuracies. One judge wrote in a separate concurrence to clarify, however, that even taking these limitations into account, it would be impermissible for the court to “rely” on COMPAS at sentencing; at most, COMPAS scores could be only “one of many factors” considered.

Even the most avid supporters of risk assessment are skeptical of the use of proprietary methods for these purposes; they are concerned that vendors may not disclose important information or that the profit motive might lead them to overstate the value of their contributions. These concerns about transparency are coupled with additional substantive questions about how the tools actually function: for instance, do algorithmic decision-making mechanisms consider race or gender in ways that might violate the Constitution or principles of due process? Do evidence-generating tools like

---

182. Id. at 34 fig.1.
183. Loomis, 881 N.W.2d at 761.
184. Id.
185. Id. at 762.
186. Id. at 761.
187. Id. at 761–64.
188. Id. at 764 (“Providing information to sentencing courts on the limitations and cautions attendant with the use of COMPAS risk assessments will enable courts to better assess the accuracy of the assessment and the appropriate weight to be given to the risk score.”).
189. Id. at 774 (Roggensack, J., concurring).
190. Richard Berk, Criminal Justice Forecasts of Risk: A Machine Learning Approach 105 (2012) (“Proprietary software may be purchased easily enough, but important details may be inadequately disclosed, and performance claims may turn out to be unsubstantiated; there is usually no equivalent of peer review. It can also be difficult to alter the software, or require that changes be made by the purveyor, once the project has begun.”).
breathalyzers malfunction under certain conditions? And if so, how will defendants—or the public—know?

II. ALGORITHMIC OPAcity AND THE PUBLIC INTEREST

In 2002, Martha Minow wrote that what “American schools, prisons, welfare agencies, and social service programs have in common” is that they are the subject of expanding experiments in privatization. Seventeen years later, these seemingly disparate contexts are united not only as sites of privatization but also as experiments in automation and algorithmic governance. In important respects, these cases reflect the many ways in which outsourcing decision-making to the private sector can pose challenges to existing transparency and accountability mechanisms. Partnerships between government and the private sector in Medicaid, education, and criminal justice are transforming the way that government makes critical decisions that affect individual rights as well as the broader public.

A. Concealing Government Decision-Making

First, algorithmic governance amplifies some recurring problems for procedural due process, with widespread effects. Bureaucracy and red tape all but ensure that the reasons and procedures for government decisions are difficult to access even when humans, not machines, are in control. But by automating decision-making and resisting disclosure of its methods, algorithmic governance poses more entrenched obstacles to litigants’ abilities to “meaningfully challenge” determinations, limiting the types of information that the government could disclose to affected citizens. Thus, when government defendants assert that their decision-making methodologies cannot be disclosed because of trade secret concerns, they in turn attempt to minimize the importance of the methodology—or emphasize its objectivity—in understanding how the government reached the contested decision.

In all these cases, by contrast, the courts recognized that due process requires litigants to have access to some information about the decision-making process. But what information specifically? The courts lack a benchmark for understanding what kinds of information litigants actually require to make the possibility of a “meaningful challenge” a reality. This

191. Whittaker, supra note 167.
192. Minow, supra note 58, at 1229.
194. Cf. Lens, supra note 61, at 16–19 (describing how both the “social work” and the “legal” models of determining eligibility for welfare benefits resulted in arbitrary and discriminatory denials of aid).
determination may depend partially on the design and intended use of an algorithmic governance method. But some crosscutting questions have yet to be resolved, including whether individuals should have access to information about how the methodology functions or only to the data that constitutes an input into the system.

Accordingly, some courts have suggested that access to the “static factors” inputted into an automated system is sufficient to vindicate due process rights. Thus, in State v. Loomis, the Wisconsin Supreme Court upheld the use of COMPAS in part because the defendant had access to questions and answers regarding “static factors” such as his criminal history. But other courts have required more, recognizing that access to additional information about the decision-making process was critical to understanding how the government reached the outcomes that the plaintiffs wished to challenge. And in Houston Federation of Teachers, Local 2145 v. Houston Independent School District (HISD), the court seemed to follow this more demanding approach, reasoning that access to general information about the EVAAS methodology was insufficient to alleviate due process concerns.

In short, these decisions are uniform in holding that the law requires the disclosure of information necessary to understand whether an automated decision is accurate but differ in their determinations of what that information is. In a sense, this observation comports with the courts’ general embrace of “flexible” procedures that can accommodate different substantive contexts.

But if technology and privatization are altering decision-making methodologies in ways that cut across sectors, perhaps a more coherent and affirmative approach is needed to determine what kinds of information about algorithmic systems ought to be disclosed. Litigation that is fact-specific, occurs on a case-by-case basis and ultimately advances the interests of (and strikes compromises among) private parties may not be the most efficient, or effective, strategy for advancing algorithmic accountability. The “flexibility” of the due process inquiry, in other words, may undermine

---

196. See, e.g., Brauneis & Goodman, supra note 13, at 120–22 (describing the importance of understanding the risk of false positives and negatives, particularly in criminal justice contexts).
197. 881 N.W.2d 749 (Wis. 2016).
198. Id. at 761.
199. Thus, in Michael T. v. Crouch, the revised approach to determining eligibility for Medicaid waiver benefits allowed beneficiaries to challenge not only the accuracy of the inputs but also the application of the decision-making methodology itself. See generally No. 2:15-CV-09655, 2018 WL 1513295 (S.D.W. Va. Mar. 26, 2018).
201. Id. at 1178.
203. See, e.g., Brauneis & Goodman, supra note 13, at 166 (“Governments should consciously generate—or demand that their vendors generate—records that will further public understanding of algorithmic processes.”).
efforts to shed light on the extent to which decision-making across agencies is shifting from public toward private governance.204

B. The Role of Human Judgment

These cases also raise significant questions about the role of deference and human judgment in considering—and potentially reversing—algorithmic decisions. Courts appear more skeptical of algorithmic determinations when proprietary tools are accepted and relied upon as the primary or exclusive factor in decision-making.205 By contrast, courts appear more likely to bless proprietary algorithmic governance where an algorithmic determination is only one of many factors to be considered.206

The relationship between human discretion and technological tools is of central concern because reliance on technology might change the ways in which decision makers give reasons for their decisions as well as the outcomes themselves.207 As Danielle Citron has demonstrated, “automation bias” suggests that “workers will likely adopt a computer’s suggested eligibility determinations and benefit calculations.”208 These cases tend to support Citron’s observation, confirming that “fair hearings” are less than fair when hearing officers defer unthinkingly to algorithmic determinations. As the HISD court wrote, it “beggers belief that any HISD hearing officer would (or could) freely disregard the very score used by HISD to identify ‘ineffective’ teachers.”209 Likewise, the court in Michael T. v. Crouch210 found that, despite West Virginia’s “stated policy” to increase benefits beyond the budget allocated by the APS algorithm, it had “eschew[ed] this policy in favor of affirming” the outcome of the algorithmic determination.211

Nonetheless, some studies show more complex interactions between human decision makers and algorithmic determinations. For instance,

204. See, e.g., Laura A. Dickinson, Privatization and Accountability, 7 ANN. REV. L. & SOC. SCI. 101 (2011); Jody Freeman, The Private Role in Public Governance, 75 N.Y.U. L. REV. 543, 576 (2000) (“[M]any scholars have argued that, in certain contexts, private actors ought to submit to oversight by agencies, courts, and the legislature, and to be constrained by the Constitution in the same manner as traditional public agencies are.”); Margaret H. Lemos, Privatizing Public Litigation, 104 GEO. L.J. 515 (2016) (describing public sector reliance on private attorneys); Metzger, supra note 58 (analyzing the extent of privatization in nondelegation terms).

205. See, e.g., State v. Loomis, 881 N.W.2d 749, 769–71 (Wis. 2016) (upholding the use of proprietary risk assessment because the state’s practices did not give the risk scores “undue weight”).

206. See, e.g., id. at 772–74 (Roggensack, J., concurring) (supporting the use of algorithmic determinations in contexts in which decision makers are already required to weigh multiple factors).


208. Citron, supra note 42, at 1272.


211. Id. at *3.
algorithmic decisions on “human tasks” such as hiring are perceived as less “fair” and less “trustworthy” than human judgment, suggesting that some decision makers might ignore or discount them. One study of judicial attitudes toward risk assessment in sentencing found that a minority of judges believed risk assessment to be more accurate than human judgment. In a recent study of pretrial risk assessment in Kentucky, Megan Stevenson found that the use of an actuarial risk assessment tool did not markedly increase efficiency. One potential reason, she found, was that “judicial discretion was used not to correct the risk assessment when it erred, but to override the risk assessment when it was correct.” As one scholar recently predicted with regard to criminal law enforcement, negative media coverage might also lead to more public resistance to algorithmic outcomes “since the general public will inevitably see the failures of predictive algorithms along with their successes.”

These factors complicate, rather than clarify, the role of decision-maker discretion. They make it more difficult to attribute an outcome to a specific decision maker or process and to understand the basis of government decisions. One potential result is that the advent of algorithmic decision-making—while promising enhanced objectivity and efficiency—actually introduces more, not less, uncertainty into the logic of governing. This uncertainty is material not only to the individuals who seek to understand why they have been denied important rights and benefits but also to the public as a whole.

C. Process and Results

Perhaps the greatest question raised by these challenges to algorithmic governance concerns the relationship between process and outcomes. Numerous scholars have raised pressing concerns that algorithmic...
governance—in the private as well as the public sector—can lead to faulty, discriminatory, or biased outcomes.218

Notably, however, these successful challenges to proprietary algorithmic governance in the public sector have not concerned bias or unfairness in the outcomes of automated processes but rather interests in a fair process. In several cases, these courts explicitly refused to consider whether an algorithm itself was “systematically biased.”219 Rather, to the extent that litigants have been successful in efforts to curb algorithmic decision-making, these successes are not about degrees of bias or fairness embedded within a tool. They reflect interests in the kinds of transparency and access that due process requires. Of course, transparency is also a prerequisite for understanding whether algorithmic governance indeed offends substantive rights.

But transparency is as important for reasons of process as for substance. In fact, these cases may be better viewed through the lens of procedural values such as transparency, participation, and democratic accountability than through the lens of discrimination or bias. This is not just because the resolution of these cases rises or falls on judgments about the quality and kind of information required to be disclosed to affected parties but rather that the cases can be seen as advancing procedural justice.220 As scholars of procedural justice acknowledge, the substantive fairness of government decision-making matters as much as the appearance of fairness in promoting public trust and legitimacy.221

As governments adopt automated decision-making systems, they ought to consider not only the substance of those decisions but also how those transformations in governance affect public control, trust, and democratic oversight. This observation comports with the general understanding that governmental processes ought to be transparent, comprehensible, and predictable.222 The interests in “predictability, transparency, and rationality”

218. See, e.g., Rachel Courtland, *Bias Detectives: The Researchers Striving to Make Algorithms Fair*, NATURE (June 20, 2018), https://www.nature.com/articles/d41586-018-05469-3 [https://perma.cc/AW8W-RW3H]; see also Barocas & Selbst, supra note 28; Citron, supra note 42; Citron & Pasquale, supra note 29; Huq, supra note 59; Katyal, supra note 38; Mayson, supra note 59; Starr, supra note 59.

219. HISD, 251 F. Supp. 3d 1168, 1180 (S.D. Tex. 2017) (dismissing the plaintiffs’ substantive due process argument that EVAAS was not “rational” because it was “systematically biased”), see also State v. Loomis, 881 N.W.2d 749, 764 (Wis. 2016) (endorsing “cautions” on the use of risk assessment without explicitly finding that the tools encoded bias).


221. Tracey L. Meares & Tom R. Tyler, *Justice Sotomayor and the Jurisprudence of Procedural Justice*, 123 YALE L.J. FORUM 525, 535 (2014) (“Many judges devote their attention to being fair, i.e., to correctly applying the law to the facts of each case, but do not think about how they can communicate that they are being fair to the parties in the case or to the public more generally.”).

222. See Mashaw, supra note 18; Redish & Marshall, supra note 18; Saphire, supra note 18, at 116 (“A purely piecemeal, incremental definition of fairness would be at odds with the view that fairness can or should have some guiding influence on the way in which persons or institutions should be expected to act.”).
are not only essential for vindicating individuals’ interest in understanding the legal rules that bind them but also for informing society about the laws that exist and how they are applied.223

III.  ACCESS LAW FOR AN OPAQUE AGE

Challenges to algorithmic decision-making teach a valuable lesson: knowledge is power. In efforts to confront algorithmic decision-making, the first step is nearly always an arduous journey to shed light on why, and how, the decision was reached in the first instance. Even within a traditional procedural due process framework, litigants have repeatedly raised issues regarding transparency of government decision-making that affect the public.224

New challenges to transparency and accountability also resonate within the broader framework of the law of access to government proceedings and records, which is preoccupied with opening government decision-making to public view. This Article now turns toward the law of access itself to examine how the guarantees of public records statutes and the constitutional right of access to government proceedings might advance efforts to bring algorithmic governance into public view. Critically, neither mechanism provides clear solutions to the challenge of proprietary algorithmic governance. Nonetheless, both sources call into question the adoption of proprietary tools to shield government decision-making from public view.225

A.  Why Access Law?

These cases raise a conceptual question: when ought the methodology of government decision-making be public? This question has deep practical implications. If the processes for government decision-making were already public, litigants would not have to fight tooth and nail to gain access to an explanation of why their benefits were slashed, their employment was terminated, or their release from prison was delayed.

The challenges to algorithmic opacity surveyed in the preceding sections are efforts to facilitate access to information critical to individuals affected by algorithmic governance. In light of these modest successes for the interests of algorithmic justice, what more could the law of access add?

The law of access makes a critical contribution in shifting the burden to force disclosure from those who are directly affected to the general public. To date, most of the challenges to algorithmic opacity have been brought by

224. See supra Part I.A (describing the Idaho plaintiffs’ rejection of a protective order); supra Part I.B (describing the HISD protective order).
225. See, e.g., DIAKOPOULOS, supra note 33, at 12.
litigants who are typically underresourced: criminal defendants, the poor and disabled, and public servants.

Nowhere is this dynamic more obvious than in the context of Medicaid waiver determinations. Although these cases have received hardly any scholarly attention, they have deep significance for the study of algorithmic governance. The Medicaid cases reflect how algorithmic governance often affects the least privileged, least empowered members of society, who are often represented by overstretched and underresourced legal aid organizations: in this case, the disabled.

Yet implicit in these cases is an acknowledgment that this information also has broader implications for the public’s right to know. In *K.W. ex rel. D.W. v. Armstrong*, that claim was made explicit: the decision-making methodology had to be disclosed not only to the plaintiffs but also to any other interested person using the mechanism of Idaho’s public records law. The reasons are clear: although there were only a few plaintiffs, the methodology should be available to all beneficiaries and their guardians, regardless of whether they were represented in the case. Moreover, *K.W.* reflects a broader understanding: in all of these cases, even if individual litigants had sufficient information to challenge the individual determinations that affected their rights, the public would still be largely in the dark.

This public interest in understanding how proprietary algorithmic governance works is precisely what is protected by laws requiring public access to government records and proceedings. This interest is independent from that of the litigants. Indeed, in many cases seeking to vindicate the right of access to government proceedings, the public intervenes in an ongoing case notwithstanding the opposition of both parties. Under open records

---

226. *See, e.g.*, Petition for a Writ of Certiorari & Motion for Leave to Proceed in Forma Pauperis, Loomis v. Wisconsin, 137 S. Ct. 2290 (2017) (mem.) (No. 16-6387) (establishing that Loomis was represented by pro bono counsel Michael D. Rosenberg of Community Justice, Inc.).


230. 789 F.3d 962 (9th Cir. 2015).

231. *See, e.g.*, United States v. Aref, 533 F.3d 72, 81 (2d Cir. 2008) (“[A] motion to intervene to assert the public’s First Amendment right of access to criminal proceedings is proper.” (emphasis added)); United States v. Soussoudis (*In re Wash. Post Co.*), 807 F.2d 383, 386–87 (4th Cir. 1986) (permitting the *Washington Post* to intervene for purposes of challenging the closure of a sentencing hearing to which defendant had not objected); United
statutes, transparency advocates frequently seek records that implicate
individual privacy rights. This public-oriented framework acknowledges
that, at times, the public’s interests in transparency and openness may
contradict the preferences of the parties in litigation.

This disjunction between the interests of private litigants and the public
interest has practical roots. Private litigants often lack a reason to push for
public disclosure of records concerning algorithmic decision-making.
Sometimes secrecy redounds to a litigant’s benefit by protecting key privacy
interests. In the criminal context, pushing for public disclosure might
heighten the possibility that others would learn of a criminal proceeding, thus
creating more significant collateral consequences by tipping off future
employers, landlords, or business associates or by revealing cooperation with
law enforcement investigations. In the civil context, pushing for public
disclosure also runs counter to statutes that protect individual medical
privacy or that shield against disclosure of employment records.

More important, as a normative matter, individual litigants should not have
to shoulder the burden of ensuring that algorithmic governance comports
with constitutional and statutory requirements vis-à-vis the public. Litigating
these issues requires time and money that many litigants do not have.

Nonetheless, asserting the public interest in transparency is not to diminish
the importance and the value of individual challenges to opacity. As Frank
Michelman has described it in a different context, these two perspectives are
neither “mutually exclusive [nor] competitive” but rather give a “binocular
view” of algorithmic transparency. As this Article describes below,
transparency’s legal mechanisms can meaningfully contribute to the project
of algorithmic transparency along a parallel track without undermining or
jeopardizing the due process arguments presented in the cases surveyed
above.

---

to intervene and unseal evidence even though the defendant had not moved to unseal).
233. See generally U.S. Dep’t of Justice v. Reporters Comm. for Freedom of the Press, 489
234. Id. at 784; see also D. Brock Hornby, Can Federal Sentencing Remain Transparent?,
Judicature, Spring 2019, at 46 (describing efforts to conceal sentencing memoranda that
would reveal a defendant’s cooperation with law enforcement).
235. See, e.g., Al Baker & Benjamin Mueller, Records Leak in Eric Garner Case Renews
22/nyregion/nypd-eric-garner-daniel-pantaleo-disciplinary-records.html [https://perma.cc/
RAX8-QDTF] (describing the conflict between confidentiality of police records and the New
York open records statute); see also State ex rel. Cincinnati Enquirer v. Daniels, 844 N.E.2d
1181, 1187 (Ohio 2006) (addressing the conflict between the Health Insurance Portability
and Accountability Act and Ohio’s public records statute).
236. Frank I. Michelman, Formal and Associational Aims in Procedural Due Process, in
B. Transparency’s Statute: FOIA

Might FOIA or its state equivalents directly constrain the use of proprietary algorithmic governance? Efforts to leverage the guarantees of open records litigation in support of algorithmic transparency confront several doctrinal hurdles. Although FOIA’s requirements are intended to open government decision-making to public view, the law does not, itself, impose obstacles to the use of private decision-making authority.237 Instead, it creates an administrative process for a member of the public to request government records and confers federal jurisdiction on district courts, which can enjoin agencies from withholding records or order them to produce records which have been “improperly withheld.”238

But the interests protected by FOIA and its state counterparts—enhancing “public knowledge of Government operations”239—suggest some limits on the government’s use of proprietary, secret decision-making methods. The extensive body of FOIA case law emphasizes the necessity of understanding both the mechanisms and outcomes of decision-making. Moreover, the broad principles of open government embodied in FOIA suggest that shielding government decisions by using proprietary means is inappropriate.

Congress enacted FOIA in response to an administrative state that had become increasingly secretive.240 The purpose of the statute was to “pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny.”241 The statutory structure reflects its purpose, allowing “any person” to submit a request for agency records and requiring agencies to respond—unless the material falls within one of nine enumerated exemptions.242 In addition, FOIA requires agencies to affirmatively publish several categories of rules, procedures, and statements of policy, either in the Federal Register or in electronic “reading rooms.”243 In contrast to the legacy

---

237. See Paul R. Verkuil, Outsourcing and the Duty to Govern, in GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY, supra note 193, at 310, 316–17 (contending that FOIA’s transparency obligations, while not imposing substantive obstacles, would “help condition the President’s transfer of civilian policymaking authority to private hands”).

238. See Kenneth Culp Davis, The Information Act: A Preliminary Analysis, 34 U. CHI. L. REV. 761, 767 (1967) (“The court has jurisdiction to enforce; it is not commanded to enforce.”).


240. See generally Kwoka, Deferring to Secrecy, supra note 21, at 197; see also EPA v. Mink, 410 U.S. 73, 79 (1973) (explaining how, prior to FOIA’s enactment, section 3 of the Administrative Procedure Act had come to be “looked upon more as a withholding statute than a disclosure statute”).


of administrative secrecy, FOIA instead embraced a philosophy of “maximum access.”

An initial obstacle to efforts to promote algorithmic transparency concerns FOIA’s limitation that it applies only to those records which an agency “controls.” To determine whether an agency “controls” a record, courts apply a multifactor test that examines the intent of the creator, the agency’s ability to “use and dispose of” the record, and its use and integration of the document within its own system. The “decisive factor” in establishing whether a document is a government record is whether an agency has used, read, or relied upon it, because only if it has done so would disclosure vindicate FOIA’s fundamental values by helping the public learn about government decision-making.

FOIA’s “control” requirement reflects its goal of shedding light on records that actually reflect government decision-making. This statutory purpose suggests that when agencies adopt and rely upon proprietary materials or software in making decisions, those materials should generally be considered matters of public record—regardless of the licensing or contractual provisions that govern. Indeed, allowing contracts between the government and its vendors to remove the infrastructure of decision-making from public control reflects a formalistic approach that privileges the private sector’s economic and political power while virtually eviscerating the purposes of the statutory protections. As Justice William J. Brennan put it in a scathing dissent in 1980, secret governance is equally “destructive of democracy” regardless of the formal contractual means by which it is accomplished.

While courts have rarely had the opportunity to consider FOIA requests for proprietary records that are at the core of the government’s decision-making functions, the emergence of algorithmic governance puts this balance to the test. But courts ought to look askance at efforts to hamper public access in ways that would permit the government “to insulate itself from public scrutiny of its operations and regulatory decisions.” Where governments

250. See Pozen, supra note 43, at 1114 (describing the private sector’s “privileged position” under FOIA).
251. Forsham v. Harris, 445 U.S. 169, 190 n.8 (1980) (Brennan, J., dissenting) (“Certainly the agency cannot control the legal consequences simply by the label it attaches to a relationship.”).
252. Tax Analysts, 913 F. Supp. at 607. In Tax Analysts, the district court ruled that JURIS, an electronic legal research database, was not an “agency record” subject to the FOIA. Id. West, a legal publisher, had entered into a contract with the Department of Justice through
adopt proprietary decision-making methodologies that impact their “structure, operation, or decision-making procedures,” those records ought to become public.\textsuperscript{253} In other words, although not every item that the government procures or licenses from the private sector becomes a “public record,” those that are at the core of the government’s decision-making functions—the transparency of which is the primary interest protected by FOIA—are likely to be covered by the statute’s disclosure regime.

1. Exemption 4

Even assuming that the records are controlled by an agency, however, FOIA’s exemptions may also impede efforts to obtain access to proprietary decision-making tools. FOIA’s “Exemption 4” provides that “trade secrets and commercial or financial information obtained from a person and privileged or confidential” are exempt from disclosure.\textsuperscript{254} For example, courts have denied FOIA requests for proprietary videoconferencing software, reasoning that even assuming the records were “agency records,” they would be protected under Exemption 4.\textsuperscript{255}

Like the control requirement, FOIA’s broad exemption for trade secrets and confidential business information was intended to stimulate information sharing with the government, not to shield government decision-making from public scrutiny. The statute’s legislative history confirms that the exemption was meant to protect “information which is obtained by the government through questionnaires or other inquiries, but which would customarily not be released to the public by the person from whom it was obtained.”\textsuperscript{256} Congress anticipated that information such as “business sales statistics, inventories, customer lists, and manufacturing processes” submitted to an agency would be kept confidential.\textsuperscript{257}

But Exemption 4’s protections extend beyond trade secrets to protect confidential commercial information as well. In an influential 1974 decision, the D.C. Circuit held that, in order to satisfy the requirements of Exemption 4, courts must not only determine whether information is “confidential” but also that “non-disclosure is justified by the legislative purpose which underlies the exemption.”\textsuperscript{258} Under this approach, Exemption 4 recognizes that information can be withheld if disclosure is likely “(1) to impair the Government’s ability to obtain necessary information in the future; or (2) to

\begin{thebibliography}{99}
\bibitem{Exemption4} Id. at 607.
\bibitem{ Innocent} 111 Cong. Rec. 26,823 (1965).
\bibitem{Control} Id. at 607–04. The district court found that the database was not under the department’s “control,” reasoning that disclosure would not serve the broader values of FOIA. Id. at 607.
\bibitem{TradeSecrets} Id. at 607; see also SDC Dev. Corp. v. Mathews, 542 F.2d 1116, 1119 (9th Cir. 1976).
\bibitem{Information} Id.
\bibitem{Exemption4} Id. at 607.
\bibitem{Information} Nat’l Parks & Conservation Ass’n v. Morton, 498 F.2d 765, 767 (D.C. Cir. 1974).
\bibitem{Control} Id. at 607–04. The district court found that the database was not under the department’s “control,” reasoning that disclosure would not serve the broader values of FOIA. Id. at 607.
\bibitem{TradeSecrets} Id. at 607; see also SDC Dev. Corp. v. Mathews, 542 F.2d 1116, 1119 (9th Cir. 1976).
\bibitem{Information} Id. at 607.
\bibitem{Exemption4} Id. at 607–04. The district court found that the database was not under the department’s “control,” reasoning that disclosure would not serve the broader values of FOIA. Id. at 607.
\bibitem{TradeSecrets} Id. at 607; see also SDC Dev. Corp. v. Mathews, 542 F.2d 1116, 1119 (9th Cir. 1976).
\bibitem{Information} Id. at 607.
\bibitem{Exemption4} Id. at 607–04. The district court found that the database was not under the department’s “control,” reasoning that disclosure would not serve the broader values of FOIA. Id. at 607.
\bibitem{TradeSecrets} Id. at 607; see also SDC Dev. Corp. v. Mathews, 542 F.2d 1116, 1119 (9th Cir. 1976).
\bibitem{Information} Id. at 607.
\bibitem{Exemption4} Id. at 607–04. The district court found that the database was not under the department’s “control,” reasoning that disclosure would not serve the broader values of FOIA. Id. at 607.
\bibitem{TradeSecrets} Id. at 607; see also SDC Dev. Corp. v. Mathews, 542 F.2d 1116, 1119 (9th Cir. 1976).
\bibitem{Information} Id. at 607.
\bibitem{Exemption4} Id. at 607–04. The district court found that the database was not under the department’s “control,” reasoning that disclosure would not serve the broader values of FOIA. Id. at 607.
\bibitem{TradeSecrets} Id. at 607; see also SDC Dev. Corp. v. Mathews, 542 F.2d 1116, 1119 (9th Cir. 1976).
\bibitem{Information} Id. at 607.
\bibitem{Exemption4} Id. at 607–04. The district court found that the database was not under the department’s “control,” reasoning that disclosure would not serve the broader values of FOIA. Id. at 607.
cause substantial harm to the competitive position of the person from whom the information was obtained.”

In June 2019, however, the U.S. Supreme Court found the “substantial competitive harm” requirement “inconsistent with the terms of the statute.” Instead, the Court reasoned that, in order to shield commercial or proprietary information from disclosure, FOIA required only that the owner of that information “customarily and actually” treat it as secret and that the government promise to keep the information secret as well. The result is to expand the scope of plausible Exemption 4 claims.

Agencies may be even less likely to comply with FOIA requests when they expect that a vendor or contractor would not want to comply. Agencies normally notify government contractors when information that may be confidential is sought under FOIA. Those who submit confidential information to the government can file a “reverse FOIA” suit seeking to enjoin an agency from releasing that information. As one commentator has observed, “even the threat of a reverse-FOIA action creates an environment where agencies are more likely to work with contractors” to prevent disclosure.

Nonetheless, there is some room for optimism that Exemption 4 might not shield the methodologies of government decision-making from disclosure. First, there is little evidence that Exemption 4 was intended to cover decision-making methodologies employed by the government in making determinations about constitutional rights. Although the federal courts have repeatedly held that even organizations that are delegated fairly extensive authority by the executive branch are not subject to FOIA, that conclusion is questionable where those organizations make determinations about constitutional rights. Although the government does have an interest in ensuring the “continued availability” of information and materials that are

---

259. Id. at 770 (footnote omitted).
261. Id. at 2366.
262. Id. at 2368 (Breyer, J., concurring in part and dissenting in part) (“[G]iven the temptation, common across the private and public sectors, to regard as secret all information that need not be disclosed, I fear the majority’s reading will deprive the public of information for reasons no better than convenience, skittishness, or bureaucratic inertia.”); see also Tom Susman & Lisa Rosenberg, Will Corporations Decide What Information the Public Gets?, HILL (June 3, 2019, 5:00 PM), https://thehill.com/opinion/civil-rights/446699-will-corporations-decide-what-information-the-public-gets [https://perma.cc/H8HR-J2ZH].
266. See, e.g., Forsham v. Harris, 445 U.S. 169, 171 (1980) (holding that “written data generated, owned, and possessed by a privately controlled organization receiving federal study grants are not ‘agency records’” under FOIA); see also Guttman, supra note 58.
voluntarily provided to it by the private sector, this does not suggest that the private sector should be able to condition its services on confidentiality.267

2. Exemption 5

FOIA’s “Exemption 5” may also pose a hurdle to disclosure of proprietary decision-making software. FOIA exempts from disclosure information that is subject to the deliberative process privilege.268 This exemption is intended to protect the integrity of the formulation of government decisions and policy by shielding them from outside interference and scrutiny.269 Facts are not exempt; only those materials that would “expose the deliberative process” can be withheld.270 And because the privilege only protects “predecisional” material, it cannot be asserted after an agency accepts or relies upon it.271

No court has upheld a claim that automated decision systems should be considered “deliberative.” Indeed, many automated decision systems are likely to contain more unprivileged “facts” than privileged “deliberation.”272 And acceptance of a decision made by an automated tool would extinguish any privilege in any event.273

In a 2006 case, the attorney general of Massachusetts sought access to EPA records related to the use of a “proprietary computerized model . . . to prepare forecasts utilized in evaluating the relative costs and benefits of alternative proposed regulatory approaches to pollution control.”274 The court rejected EPA’s invocation of the deliberative process exemption, reasoning that the model was essentially an “investigative technique utilized to generate raw data.”275 While the data undoubtedly would reflect, to some extent, the agency’s thought process, the court went on, “This is true of any investigation by which an agency seeks facts—knowing what questions are asked or which witnesses are interviewed reveals aspects of what the investigator deemed important or worthy of consideration.”276

Nonetheless, this reasoning has not stopped government agencies from claiming that the deliberative process exemption shields reasoning that was aided or developed by automated means. In one recent case under Illinois’s Freedom of Information Act, a newspaper sought access to records related to

269. See Grand Cent. P’ship, Inc. v. Cuomo, 166 F.3d 473, 482 (2d Cir. 2009).
272. Mead Data Cent., 575 F.2d at 935.
273. Brennan Ctr., 697 F.3d at 200.
275. Id. at 352–53.
276. Id. at 352.
the Cook County Assessor’s Office’s methodology for valuing property for the purposes of assessing property taxes.277 The methodology involved using a computerized regression model to compare properties to other similar properties, after which analysts examined the results, made adjustments, and finalized the values. The court rejected the office’s invocation of the deliberative process exemption, recognizing that the requested records were “not ones in which opinions are expressed or in which policies or actions are formulated—they are factual.”278

Although open records laws have gone fairly untested as means to compel the disclosure of proprietary decision-making tools used by government, they call into question the legitimacy of government contracts that require secrecy in decision-making. It is axiomatic that public records laws ought to be “liberally construed” to promote public access to government records.279 Some state open records laws explicitly prevent the government from entering into contracts that would “impair[] the right of the public” to access public records.280 Other state courts have simply found that certain secret actions taken by government are inconsistent with state open records laws.281 As such, public records laws provide critical support for opponents of algorithmic opacity.

C. Transparency’s Constitution: The First Amendment

The First Amendment is equally hostile to secret government decision-making.282 This hostility stems, in part, from a central observation of First Amendment theory that an inextricable link binds together democracy, self-governance, and free expression.283 The understanding that free expression

278. Id. at 879.
280. CONN. GEN. STAT. § 1-211(b) (2020); see also Office of Health Care Access v. Freedom of Info. Comm’n, No. CV0305215738, 2005 WL 1095361, at *8 (Conn. Super. Ct. Apr. 19, 2005) (upholding the decision that the agency violated Connecticut’s FOIA by acquiring a new computer system from a contractor that impeded compliance with public records requests).
281. See, e.g., S-P Drug Co. v. Smith, 409 N.Y.S.2d 161, 164–65 (Sup. Ct. 1978) (“The State cannot evade the obligations of the law by agreeing not to disclose the drug price data and documentation, requiring any interested member of the public to purchase that information from a private party at a price.”).
283. ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT 26 (1960); see also Robert H. Bork, Neutral Principles and Some First Amendment Problems, 47 IND. L.J. 1, 20 (1971) (“Constitutional protection should be accorded only to speech that is explicitly political.”); Alexander Meiklejohn, The First Amendment Is an Absolute, 1961 SUP. CT. REV. 245, 254.
is “indispensable to the operation of a democratic form of government” is at the heart of several accounts of the “meaning” of the First Amendment.284 And while many theorists would extend the meaning of the First Amendment much farther, at a minimum, the “political speech” that lies at the core of First Amendment interests would appear to include speech regarding government decision-making.285 These interests cut against secretive government proceedings that cannot be monitored or scrutinized by the press or public.

Reflecting the prevailing view that information about government decision-making is critical both to democracy and to public debate, the Supreme Court has recognized that the public has a constitutional right of access to government proceedings and records rooted in the First Amendment.286 In 1978, the Supreme Court explicitly recognized “a general right to inspect and copy public records and documents” under common law.287 In 1979, the Supreme Court—while holding that the Sixth Amendment did not guarantee a public right of access to criminal trials—indicated that there might be a right of access to criminal trials couched in the First and Fourteenth Amendments.288 In following years, the Court broadened its interpretation, finding that the public must be able to attend a variety of criminal proceedings—including trials,289 voir dire,290 and preliminary hearings.291

In its 1980 opinion in Richmond Newspapers, Inc. v. Virginia,292 the Court explicitly linked the right to attend criminal trials to broader First Amendment values, reasoning that, “without the freedom to attend such trials, which people have exercised for centuries, important aspects of freedom of speech and ‘of the press could be eviscerated.’”293 And in his influential concurring opinion, Justice Brennan also emphasized the functional importance of the right of access, identifying open government proceedings as a critical feature of the First Amendment’s “structural role . . . in securing and fostering our republican system of self-government.”294

286. See Bloch-Wehba, supra note 44, at 153–58 (canvassing the right of access case law).
293. Id. at 580 (quoting Branzburg v. Hayes, 408 U.S. 665, 681 (1972)).
294. Id. at 587 (Brennan, J., concurring).
The First Amendment right of access to government proceedings requires that preliminary criminal hearings be held in open court.295 Press-Enterprise Co. v. Superior Court296 (Press-Enterprise II) set forth a two-pronged test for determining whether the public must have access to a given proceeding and held that a court considering an access claim must assess both “whether public access plays a significant positive role in the functioning of the particular process in question” and “whether the place and process have historically been open to the press and general public.”297 If the First Amendment right attaches, proponents of closure must meet a demanding standard.298

Importantly for the enterprise of algorithmic risk assessment, Press-Enterprise II and its progeny established a presumption of openness regarding bail hearings. Numerous courts have recognized that the functional benefits of public access, which serves as “a check on judicial conduct and tends to improve the performance both of the parties and of the judiciary,” are as apparent in pretrial release proceedings as in other judicial proceedings.299 Perhaps even more so: “The decision to hold a person presumed innocent of any crime without bail is one of major importance to the administration of justice,” and the community is “directly affected” by these decisions.300

By the same token, the press and the public have a constitutional right to attend sentencing and have access to sentencing-related documents. This right is integrally related to the court’s duties in sentencing, which are independent from those of the jury.301 At sentencing, public access is particularly important because it “operates to check any temptation that might be felt by either the prosecutor or the court to obtain a guilty plea by coercion or trick, or to seek or impose an arbitrary or disproportionate sentence.”302 Likewise, sentencing is socially significant to numerous audiences: to “friends and family members of the defendant being sentenced,” to “victims of crimes, to family members of victims, and to members of the community in which the crime occurred.”303 Sentencing is also a particularly “solemn occasion at which the judge has the weighty duty of determining the fate of another human being.”304 These perspectives have

297. Id. at 8.
298. Press-Enterprise I, 464 U.S. 501, 510 (1984) (“The presumption of openness may be overcome only by an overriding interest based on findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest.”).
299. United States v. Chagra, 701 F.2d 354, 363–64 (5th Cir. 1983) (citing United States v. Criden, 675 F.2d 550, 556 (3d Cir. 1982)).
301. United States v. Carpenter, 526 F. Supp. 292, 295 (E.D.N.Y. 1981) (“In sentencing, unlike other aspects of criminal proceedings, it is the distinct province of the court to determine what constitutes proper sentence.”).
304. Id. at 199.
remained part of the logic of holding open sentencing hearings despite the increasingly transactional nature of sentencing, which today includes “precious little discussion of the human qualities of the victim or the defendant, of the inherently unquantifiable moral aspects of the defendant’s crime, or of the type of sanction that would best achieve any of the purposes of sentencing.”


The First Amendment interests in open government proceedings suggest that proprietary algorithmic governance mechanisms may violate the Constitution. As one commentator has put it, “once a computerized algorithm is used by the government, constitutional rights may attach.”

306. See Eidelman, supra note 52, at 918.

When the government relies upon an automated decision system to generate evidence at trial, to set bail, or to determine a sentence, the public’s First Amendment rights demand that those proceedings be held in an open and transparent manner. By shielding the methodology of decision-making from public view, the government undermines critical assumptions of the First Amendment.

IV. TRANSPARENCY REMEDIES FOR ALGORITHMIC OPAcity

Time and again, litigants directly confront black box procedures that result from the outsourcing or privatization of government decision-making. This opacity often flouts constitutional or statutory requirements of openness. In short, these challenges can be understood as efforts to obtain access to key information needed to understand government decisions that affect people directly.

Reframing algorithmic decision-making as reflecting a public interest in disclosure, rather than a purely private interest in due process, brings to the fore a central dynamic. When courts find that the Constitution or a statute requires the disclosure of how the government reaches its decisions, we should understand that that requirement is not a relic of procedural due process alone. Rather, it reflects fundamental values of open government that are codified in the Freedom of Information Act, its state equivalents, and the First Amendment. Those mechanisms—the fabric of the law of access—are hostile to privatized, proprietary decision-making.

Viewing algorithmic governance through the lens of access law introduces a new perspective into the discussion of accountability and transparency for automated decision systems. Not only should algorithmic governance be accountable to those whom it affects, it should also satisfy, or at least not violate, fundamental values of open government that are core to our democratic system. These values cast doubt on the viability of the frameworks that have developed to limit the flow of critical information about algorithmic governance.
A. Secrecy by Contract

At bottom, the transparency problem raised by algorithmic governance as it is presented today results largely from procurement practices that fail to foreground the public interest. As Catherine Crump has documented, this problem is particularly pronounced in the context of criminal law enforcement and surveillance. As State and local government agencies seeking to secretly procure surveillance technologies can often either face a lack of awareness and interest by legislative officials or avoid legislative oversight entirely.

From the perspective of intellectual property law, the dueling interests between vendors’ trade secrecy claims and plaintiffs’ challenges seem unremarkable. But from the perspective of procurement law, this need not be so. States differ widely with regard to how public contracts should treat intellectual property rights. Some states generally treat these contracts as conferring licenses upon state actors, while others, by default, allocate full ownership of intellectual property to the state. Some have criticized this allocation of intellectual property ownership to the state, writing that conveying such ownership to a public purchaser simply is not necessary for “the efficient and cost-effective delivery of supplies and services.” In the mine-run of cases, this observation is likely correct.

But where intellectual property rights are likely to clash with governments’ obligations under transparency laws, perhaps different contract terms should be anticipated. Procurement law anticipates a distinction between items that are used for “governmental purposes” and those that are not. Surely, the allocation of government benefits and decisions regarding critical civil rights and liberties are “governmental purposes.” This suggests that these tools are not generally “commercial” systems. Indeed, many vendors of automated decision systems have government agencies as their primary, or sole, customer base.

307. See generally Crump, supra note 44.
308. Id. at 1617.
309. See, e.g., Katyal, supra note 38.
313. Federal Acquisition Regulation, 48 C.F.R. § 2.101 (2019) (defining “commercial” items as items that are “of a type customarily used by the general public or by non-governmental entities for purposes other than governmental purposes”).
314. Id.
Acting as consumers, governments can therefore require more demanding contract terms that bring their procurement processes into alignment with due process and transparency requirements. A draft bill recently introduced by the Washington State Legislature exemplifies this approach. The draft bill requires that automated decision systems have several transparency and accountability-enhancing features, including that they be open to audit and inspection by state agencies and third parties and that they be capable of giving intelligible explanations for the decisions they reach. In terms of procurement, the Washington bill also requires that procurement contracts for automated decision systems cannot contain nondisclosure provisions or other obstacles to transparency. Washington’s approach provides sound guidance for other jurisdictions to follow in reforming their procurement policies for algorithmic governance.

B. Transparency for Me, but Not for Thee

In an atmosphere of increasing automation and privatization, these cases pit proprietary interests in trade secrecy against individual interests in transparency. Faced with demands for more transparency, courts and litigants have sometimes reached an apparent compromise: protective orders, coupled with nondisclosure orders, that permit disclosure to the parties while preventing disclosure to the general public.

In this vein, numerous commentators have suggested that vendors’ claims of trade secrecy cannot simply surmount the rights of affected individuals to understand and challenge decisions that affect them. The scholarly consensus appears uniform: simply privileging vendors’ assertions of trade secrecy over the affected parties’ rights is inappropriate. Faced with concerns about how to balance proprietary interests against those of individuals who seek to challenge algorithmic determinations, however, many have suggested that courts could employ protective orders to ensure that vendors could be compelled to disclose proprietary information to individual litigants while shielding the same information from public view.

From this perspective, the chief problem with algorithmic opacity is that the individuals who are affected should have sufficient information to understand how they are assessed, judged, and scored. Only by enabling

316. Id.
317. Id.
318. See supra Part I.A (describing the Idaho plaintiffs’ rejection of a protective order);
319. supra Part I.B (describing the HISD protective order).
320. See, e.g., Brenda Reddix-Smalls, Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market, 12 U.C. DAVIS BUS. L.J. 87 (2011); see also Barocas & Selbst, supra note 28; Ram, supra note 49; Wachter et al., supra note 39; Wexler, supra note 29.
321. See Ram, supra note 49, at 717–18; Wexler, supra note 29, at 1410.
322. See Citron, supra note 42, at 30; Citron & Pasquale, supra note 29, at 5.
the disclosure of this information can we vindicate individuals’ dignity, autonomy, and due process rights. Within this paradigm, striking a bargain with vendors that facilitates these important disclosures is often worth some cost to public knowledge. And although some scholars have expressed some unease with the impact that this solution might have on broader interests in transparency, they have not critiqued it on these terms.

This assumption that protective orders can appropriately balance the interest in disclosure against intrusion into the proprietary interests of the developer overlooks, however, the importance of information about algorithmic governance to the public as a whole. Viewing algorithmic decision-making through the lens of the law of access makes clear that these new tools impact not only those who are directly affected by algorithmic decision-making but also the general public. Extensive reliance on proprietary decision-making methods runs headlong into the principles that underpin transparency protections embedded in the First Amendment’s right of access to government proceedings and open government statutes such as FOIA.

As a procedural “fix” for problems of algorithmic opacity, protective orders raise serious problems of their own. First, this framework makes explicit an assumption that the methodologies of proprietary decision-making in government need only be disclosed to the individual plaintiffs who choose to bring challenges. This assumption overlooks the resonance of calls for more transparency and accountability for broader populations who are not represented before the courts. Yet the implications of these cases for unrepresented parties are clear: each of the algorithmic tools described in the foregoing sections makes decisions that affect thousands of individuals. Bringing these cases as class actions, as in the health-care context, or on behalf of institutional plaintiffs, as in HISD, can partially solve the problem of representing the interests of all, or as many as possible, of the affected individuals. But protective orders, by design, impede the flow of information to those individuals, as well as to the press and the public. This issue was presented in sharp relief in the Idaho case, in which the plaintiffs rejected the state’s offer to enter into a protective order, instead insisting that the information they sought be disclosed not only to the named plaintiffs but also to every participant in the budget waiver program.

In fact, relying on individual plaintiffs to challenge—and gain access to—proprietary decision-making tools on an ad hoc basis has serious social costs


324. See, e.g., Wexler, supra note 29, at 1353 n.46 (raising a “potential conflict between protective orders and Sixth Amendment public trial rights”).

325. This Article leaves for another day an exploration of how social movements’ calls for algorithmic accountability also complicate these legal paradigms. Cf. Amna Akbar, Toward a Radical Imagination of Law, 93 N.Y.U. L. Rev. 405, 476 (2018) (calling for legal scholars to consider ‘movements’ visions for the world beyond what law can readily recognize or through the lens of what the state adopts”).

326. See supra Part I.A.
because the parties to these cases will be unlikely to push back on overly broad assertions of trade secrecy or other proprietary interests. As the HISD case demonstrates, in civil cases, the incentives to consent to a protective order are typically high. Litigants who are challenging opaque algorithmic decisions often settle, plead guilty, or accept disclosure of key information regarding the challenged methodology subject to a protective order that prevents the public from gaining access. 327 This dynamic is all the more pronounced when the litigants are poor individuals or underresourced organizational parties. 328 Although criminal defendants have been on the front lines of efforts to compel disclosure of vital information related to black box tools, many more have simply pleaded guilty when faced with inculpatory evidence from algorithmic tools. 329 It is hardly surprising that individuals of limited means—such as Kevin Johnson, the defendant in the FST case who was represented by the Federal Defenders of the Eastern District of New York—would accept these tradeoffs. 330

The result is that, by employing protective orders to make records available to the parties but shielded from the public, the courts create a framework of “information silos.” 331 The silo vividly symbolizes the problem of isolated decision-making within impermeable walls, unmoored from relevant outside experience or expertise. 332

Protective orders create silos by making disclosure to individuals contingent on their silence to a broader audience. In essence, each individual recipient of the information exists in his or her own silo, unable to communicate that information to others who might want or need it. This is precisely the issue raised by the disclosure of source code by Dräger, one of

---

327. See discussion supra Part I.C.
329. See ProPublica Memorandum, supra note 178.
330. Kirchner, supra note 171.
331. See Richard E. Levy & Robert L. Glicksman, Agency-Specific Precedents, 89 TEX. L. REV. 499, 510 (2011). The term “silos” typically refers to barriers—whether formal or informal—that prevent the flow of information, data, or managerial responsibility from one area to another. The term is frequently used in the managerial literature to describe difficulties coordinating across different areas of a business. See, e.g., James G. Bohn, Development and Exploratory Validation of an Organizational Efficacy Scale, 21 HUM. RESOURCE DEV. Q. 227, 235 (2010) (“What are often called ‘silos’ represent a lack of coordination between teams in an organization, and they are a recipe for disaster.”); Ron Ashkenas, Jack Welch’s Approach to Breaking Down Silos Still Works, HARV. BUS. REV. (Sept. 9, 2015), https://hbr.org/2015/09/jack-welchs-approach-to-breaking-down-silos-still-works [https://perma.cc/5RVW-GX6G] (describing how, despite advances in information technology, “many organizations still have hierarchical, siloed, and fragmented processes and cultures”).
332. See, e.g., Levy & Glicksman, supra note 331, at 510; see also Edgar H. Schein, Organizational Psychology Then and Now: Some Observations, 2 ANN. REV. ORGANIZATIONAL PSYCHOL. & ORGANIZATIONAL BEHAV. 1, 4 (2015) (describing the fragmentation of an intellectual field into “many sub-cultures each with its own jargon and preferred research methods and each evolving an intellectual silo disconnected from either central theory and/or other silos”).
the breathalyzer vendors. As a matter of policy, Dräger will disclose its source code in any criminal proceeding, subject to a protective order. The protective order makes clear the devil’s bargain: even though Dräger’s source code is material to hundreds, if not thousands, of cases, the broader public is permitted to know very little about how it functions. Indeed, when two defense experts presented a report describing flaws in the code to an annual convention of DUI lawyers—many of whom had worked on cases involving Dräger source code—the company claimed it had been defamed. The same issue would be confronted by Legal Aid attorneys who represented individuals seeking to challenge their Medicaid waiver benefit determinations or lawyers for the Houston teachers’ union who represented teachers seeking to challenge their terminations.

There might be good reasons, in some cases, to limit disclosure of information to individual litigants instead of to the general public. For instance, it is easy to imagine that certain medical information, key to the outcome of a hearing on eligibility for Medicaid benefits, is private and not subject to disclosure. In some settings, there might also be legitimate concerns that automated systems could be “gamed” if they were too open. But when the information regards the methodology for how government decisions are made, it is much harder to understand what interests could possibly support secrecy. The entire framework of the law of access to government proceedings and records is intended to ensure that information critical to public debate and oversight is available to all, not just to a few. When information is sufficiently important to be disclosed to individuals, making that disclosure contingent on a broader silence makes clear that the compromise in fact comes at a significant cost to the public interest.

New legislation may advance the interests of both defendants and the public. In September 2019, Representative Mark Takano introduced the Justice in Forensic Algorithms Act of 2019, a bill designed to promote defense access to evidence in criminal proceedings. The bill, which was influenced by the work of Rebecca Wexler and Andrea Roth, would amend the Federal Rules of Evidence to forbid using the trade secret privilege alone

333. See discussion supra Part I.C.3.
334. See discussion supra Part I.C.3.
335. See discussion supra Part I.C.3.
336. Whittaker, supra note 167 (“Dräger sent the researchers a cease and desist letter claiming defamation and alleging the two violated a protective order, designed to protect the source code from leaking.”).
337. See discussion supra Parts I.A–B.
339. See supra Part III.
340. See Helen Hershkoff, Poverty Law and Civil Procedure: Rethinking the First-Year Course, 34 FORDHAM URB. L.J. 1325, 1328 (2007) (“Litigation is not just a contest between two opposing private parties. It also is a state-sanctioned process that uses public money and is subject to constitutional constraints.”).
342. Id. pmbl.
to shield evidence from disclosure to defendants. In addition, the bill would task the National Institute of Standards and Technology with setting standards for forensic software, including standardizing requirements for “publicly available documentation” of the software, its training data, and its testing methodology.

The Justice in Forensic Algorithms Act does not address protective orders, but it nevertheless reflects a powerful endorsement of public standard-setting, documentation, and testing of forensic algorithms. In doing so, the Act partially responds to Ellen Goodman and Robert Brauneis’s call for government agencies to require more documentation of algorithmic systems to render them transparent. But while the due process and Brady issues in the context of forensic evidence are pronounced, there is no reason that the Act’s approach should be limited to forensic algorithms alone. Indeed, the other applications of algorithmic governance described in Part I reflect the same need for standardization, validation, and public documentation of algorithmic decision-making systems to render them transparent and accountable. If anything, the use of proprietary algorithmic decision-making in contexts that deprive individuals of their civil rights has gone relatively underreported and unnoticed by Congress. Congress should therefore advance a similar approach in considering the use of algorithmic decision-making systems in civil contexts, including (if necessary) by amending the Medicaid Act and by limiting the provision of federal funding in contexts where state agencies rely on black box proprietary decision-making systems.

C. The Challenge to Transparency Values

More generally, algorithmic tools sometimes appear to defy the traditional logic of government oversight—that “sunlight is said to be the best of disinfectants,” that the public’s presence can benefit proceedings, and that public oversight can benefit the operations and structure of governance. If we accept the premise that algorithmic governance is more “efficient, valuable, powerful, and objective” than its human counterparts, then why

343. Id. § 2(b).
344. Id. § 2(a)(2). In addition, the bill would require the National Institute of Standards and Technology to set standards for crime labs’ validation of forensic software and their public reporting about their validation studies. Id. § 2(a)(2)(D).
345. Brauneis & Goodman, supra note 13, at 166 (calling for additional documentation).
value transparency at all?\textsuperscript{348} Maybe we can look toward a future in which government-by-machine need not bother with the administrative headache and “burden” of responding to FOIA requests and producing documents.\textsuperscript{349} Indeed, the value of public observation and participation in the democratic process looks a lot like the kind of subjective, “clinical” judgment at which advocates of actuarial measures look askance. If actuarial measures are already accurate and fair, it’s difficult to understand how “[p]ublic scrutiny of a criminal trial enhances the quality and safeguards the integrity of the factfinding process” or “fosters an appearance of fairness, thereby heightening public respect for the judicial process.”\textsuperscript{350}

In other words, algorithmic governance resists the straightforward application of existing transparency mechanisms, but not only because of practical obstacles. The major threat to government transparency in an algorithmic age is not simply that processes have become obscure, automated, and outsourced. Rather, it is easy to see how the promise of “objectivity”—even if it is false—can undermine the core assumptions of transparency law. When government decision makers can disclaim responsibility because they have simply adopted an ostensibly neutral recommendation generated by a technological tool, it diminishes the public’s ability to hold the government accountable.

As such, algorithmic governance also lays bare the need for enhanced—not minimized—transparency and accountability measures. The public-oriented perspective on government oversight evinced in the transparency case law helps to inform judgments about when accountability is necessary, why transparency is helpful, and how we might want to approach algorithmic decision-making in law and in government.\textsuperscript{351} While current research (perhaps rightly) focuses on the individuals and institutions who are directly affected by algorithmic governance, the adoption of these methodologies also creates a ripple effect, shielding the decision-making process from scrutiny by affected parties and by the public.\textsuperscript{352}

Updating transparency law for the algorithmic age will take work. To begin, courts should critically examine the application of trade secrets protections to shield government decision-making processes from scrutiny. As articulated in Part II.A, this practice lacks any basis in FOIA’s case law and is in substantial tension with the fundamental values of FOIA. These fundamental values also suggest some potential changes in government procurement and contracting processes. Informed by the principles of open government, agencies and courts should avoid contracting for proprietary decision-making tools with vendors who require broad secrecy provisions.


\textsuperscript{349} See generally Pozen, supra note 43.

\textsuperscript{350} Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 606 (1982).

\textsuperscript{351} See supra Part III.

\textsuperscript{352} See supra Part III.
The emergence of algorithmic governance also suggests a more vital role for affirmative—rather than reactive—disclosure of key information about how the government functions. FOIA and the First Amendment do not require the government to create new records or interpret existing policies—they only require the production of existing records in response to an individual request. But affirmative disclosure of key information about how algorithmic governance works would vindicate values of open government, even though it is not required by existing law. New York City has adopted this approach in its pivotal algorithmic accountability bill, which requires a new task force to develop a “process for making information publicly available that, for each agency automated decision system, will allow the public to meaningfully assess how such system functions and is used by the city, including making technical information about such system publicly available where appropriate.”

This affirmative approach to transparency is preferable to a framework that relies on individual claimants to challenge opacity on an ad hoc basis. Individual due process challenges are insufficient to guarantee meaningful public oversight and accountability for algorithmic tools.

**CONCLUSION**

True algorithmic transparency goes far beyond an explanation of a challenged action to the individual who is affected. Rather, as challenges to opacity illustrate, algorithmic governance implicates core values of transparency law: access to government records and to key information necessary to understand government decision-making. Viewing algorithmic governance through the lens of access law makes clear that automation and privatization pose a serious threat to the existing framework, which privileges reactive disclosure of existing government records to individual requesters. Rather, just as algorithmic governance portends a new era in government decision-making, it must be accompanied by new forms of transparency to protect the vital role of public oversight in our democratic system.

---
