A PUBLIC TECHNOLOGY OPTION

HANNAH BLOCH-WEHBA*

I
INTRODUCTION

Private technology is increasingly driving public governance. Government agencies buy software and data from the private sector, adapting commercial technologies for public use. At every level of government, agencies eager to realize cost savings and efficiency gains are turning to private vendors who promise to modernize their informational infrastructure and move them to the cloud. Networks of software companies, implementation partners, and management consultants help to mediate and instantiate these new developments in governance. The drive toward government modernization, datafication, and digitization rests on extensive and growing partnerships between state agencies and the private firms that develop new governance tools.[1] The government explains and justifies its rollout of digitization efforts, cloud infrastructure, artificial intelligence, and automated decision making by pointing to industry's technological superiority. In turn, private vendors supply the technological infrastructure necessary for state transformation.

This article examines datafication and digitalization as core mechanisms through which regulatory managerialism operates.[2] Decisions to take up new technological infrastructure for governance reflect—in both pragmatic and ideological ways—familiar inclinations toward privatization, flexibility, and efficiency. I trace efforts to digitize and modernize government back to the movement to "reinvent" government in the 1990s, remaking it in the image of corporate America.[3] Under the banner of technological transformation, the state has imported products and methodologies engineered by and for the private sector and deployed them in public contexts.

These transformations are both substantive and substantial. With discretion,

---

This Article is also available online at http://lcp.law.duke.edu/

* Associate Professor of Law, Texas A&M University School of Law; Affiliate Fellow, Yale Law School Information Society Project; Affiliate Fellow, NYU School of Law Policing Project. I am grateful to Julie Cohen and Ari Ezra Waldman, as well as participants at the IP Scholars Roundtable and the Information Law Institute Fellows Workshop, for thoughtful and generous feedback on this Article.

1. Kate Crawford & Jason Schultz, *AI Systems as State Actors*, 119 COLUM. L. REV. 1941, 1941 (2019).

2. Julie E. Cohen & Ari Ezra Waldman, *Introduction: Framing Regulatory Managerialism as an Object of Study and Strategic Displacement*, 86 LAW & CONTEMP. PROBS. no. 3, 2023, at i, vi, ix–x (overviewing digital information technologies and data-driven systems employed by regulatory managerialism).

3. *See generally* DAVID OSBORNE & TED GAEBLER, REINVENTING GOVERNMENT: HOW THE ENTREPRENEURIAL SPIRIT IS TRANSFORMING THE PUBLIC SECTOR (1992).

authority, and competency increasingly vested in technology firms, the levers of policy are moving away from democratic governance and into the private sector.[4] Information technology contracts are no longer simply about providing distinct and relatively static record management tools to government users.[5] Vendors promise to break down data silos and make information more widely accessible to governing bodies, with potentially radical implications for privacy.[6] New forms of analysis and surveillance create novel due process and distributive justice concerns.[7] Often billed as technocratic efforts to "modernize" state infrastructure, these moves create a variety of new opportunities for the private technology sector to embed itself in public governance while routing around safeguards that could ensure private vendors operate with democratic legitimacy.[8] Efforts to modernize the state reflect the prioritization of innovation over accountability and invite co-optation by the private vendors increasingly responsible for building, maintaining, and managing government technology.[9]

Collectively, these shifts—automation, digitalization, datafication, and privatization—render new forms of governance less visible to the public and less amenable to democratic oversight. Technological transformations supported by private partners promise a variety of efficiency gains for state actors, but they also threaten to diminish the efficacy of transparency and accountability mechanisms oriented toward public agencies. The private vendors that are increasingly providing state actors with informational infrastructure adhere to a very different set of norms: instead of openness by default, their records are presumptively private. Beyond mere disclosure requirements, private companies also exert broader forms of control over information-sharing, retaining extensive control over employees and documents through contract and corporate policy.[10] Counterposed against private-sector norms, the kinds of rigorous transparency, accountability, and public oversight requirements that have historically ensured that public governance remains democratically accountable are both expensive and inefficient.

I focus on transparency in particular because transparency law—however

4. Deirdre K. Mulligan & Kenneth A. Bamberger, *Procurement as Policy: Administrative Process for Machine Learning*, 34 BERKELEY TECH. L.J. 773, 778 (2019).

5. *See generally* Marion Fourcade & Jeffrey Gordon, *Learning Like a State: Statecraft in the Digital Age*, 1 J.L. & POL. ECON. 1 (2020); Louise Amoore, *Machine Learning Political Orders*, 49 REV. INT'L STUD. 20 (2022) (examining the implications of new governance technologies).

6. LOUISE AMOORE, CLOUD ETHICS 33 (2020).

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

8. CHIARA CORDELLI, THE PRIVATIZED STATE 142–43 (2020).

9. *Id.* at 38 (describing privatization as "embedded in an overarching culture that valorizes market values and efficiency above everything else").

10. Hannah Bloch-Wehba, *The Promise and Perils of Tech Whistleblowing*, 118 NW. U. L. REV. (forthcoming 2024) (manuscript at 13), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4377064 [https://perma.cc/Q8VD-NQ8D] [hereinafter Bloch-Wehba, *The Promise and Perils of Tech Whistleblowing*].

flawed—provides a crucial foundation for democratic accountability.[11] Indeed, by all accounts, public transparency norms are ill-equipped to keep pace with these shifts. As Margaret Kwoka ably captures in her contribution to this symposium, the erosion of public transparency norms requires more than just rethinking the structure and substance of transparency law.[12] More foundationally, law ought to intervene to protect meaningful oversight of novel forms of governance by reducing private control of information. Doing so will require rethinking—and in some cases abandoning—legal structures and doctrinal commitments that insulate private vendors from meaningful transparency and accountability obligations.

I offer up three suggestions for realigning the use of technology in public governance with democratic values. First, I argue that we ought to do away with, or at least radically shrink, existing protections for trade secrecy in public contracting. Second, I explore routes toward additional protections for whistleblowers to help provide a release valve to overzealous corporate secrecy. Finally, I point the way toward a potentially fuller role for public development of technology: a public option to compete with private domination. Understanding the relationships between law, public administration, and technological modernization helps to uncover potential pathways toward non-reformist reforms.[13]

II

TECHNOLOGIES OF GOVERNANCE AS DRIVER AND SYMPTOM OF REGULATORY MANAGERIALISM

Today's efforts to modernize and digitize the state take up the mantle of an earlier strand of regulatory reforms that sought to "reinvent" government, promoting efficiency and "customer satisfaction," in large part through privatization.[14] In both form and substance, the "datafied state" shares this ideological pedigree, reflecting a belief that government ought to operate more like the private sector.[15]

Across a variety of domains, government actors are adopting sophisticated

11. *See* Margaret Kwoka, *Scoping an Information Commission*, 86 LAW. & CONTEMP. PROBS. no. 3, 2023, at 197, 205 ("Access to government information under FOIA is a foundational, structural necessity in our democracy . . . . [T]he larger managerial trends in modern governance have unsurprisingly also taken hold in FOIA administration and have worked to the detriment of transparency and government accountability.").

12. *See id.* ("Any response to the current failures in FOIA administration has to take account not just of managerialism's reality, but the new framework of the information economy in which FOIA operates. An information commission—models of which can be seen around the world—is an institution that can take on both challenges.").

13. Cohen and Waldman, *supra* note 2, at iii–iv.

14. K. SABEEL RAHMAN & HOLLIE RUSSON GILMAN, CIVIC POWER: REBUILDING AMERICAN DEMOCRACY IN AN ERA OF CRISIS 121 (2019).

15. *The Datafied State*, DATA & SOC'Y (Mar. 10, 2022), https://points.datasociety.net/the-datafied-state-a2a7101ba573 [https://perma.cc/BT5Q-ZPFS].

new mechanisms in support of data-driven decision-making. These transformations in governance have created new opportunities for private contractors and vendors. Law enforcement agencies buy predictive policing, gunshot detection, and probabilistic genotyping software.[16] The Department of Veterans Affairs partners with Deepmind to predict patient deterioration.[17] State and local agencies swamped by applications for public benefits turn to Google Cloud to process claims and predict whether claims are fraudulent.[18] The IRS pays $1.6 million for a company to build a chatbot to answer taxpayer questions.[19]

Technology's ascent as a mechanism for governing reflects broader reorientations of the regulatory state toward flexible institutional arrangements, privatization, and participation.[20] Under the banner of the New Public Management ("NPM"), a term denoting a broad perceived "shift in public management styles," the public sector assumed new techniques and approaches that reoriented legacy regulatory strategies toward managerial techniques.[21] Among NPM's core doctrines were the shift toward private-sector-style management practices, increasing emphasis on "discipline and parsimony in resource use and on active search for finding alternative, less costly ways to deliver public services," and increased competition both within the public sector and between government and the private sector.[22] In legal scholarship, these ideas found a footing in new governance frameworks that welcomed participation by a broad array of actors and stakeholders as part of a "dynamic, reflexive, and flexible regime" of regulation.[23]

In the United States, the outsourcing of government infrastructure had its roots in the Reagan Administration's embrace of privatization as a cost-cutting

16. Farhang Heydari, *The Private Role in Public Safety*, 90 GEO. WASH. L. REV. 696, 703 (2022).

17. Evan Sweeney, *VA Taps Google's DeepMind to Predict Patient Deterioration*, FIERCE HEALTHCARE (Feb. 26, 2018).

18. Mike Daniels, *New Google Cloud Public Benefit Solutions Power Rental and Housing Assistance Efforts Nationwide*, GOOGLE CLOUD BLOG (Nov. 3, 2021), https://cloud.google.com/blog/topics/public-sector/new-google-cloud-public-benefit-solutions-power-rental-and-housing-assistance-efforts-nationwide/ [https://perma.cc/42NX-8RVJ].

19. *IRS Unveils Voice and Chat Bots to Assist Taxpayers with Simple Collection Questions and Tasks; Provides Faster Service, Reduced Wait Times*, INTERNAL REVENUE SERV., https://www.irs.gov/newsroom/irs-unveils-voice-and-chat-bots-to-assist-taxpayers-with-simple-collection-questions-and-tasks-provides-faster-service-reduced-wait-times [https://perma.cc/KNZ7-HNSZ]; *IRS Contract Award for Chatbot System*, FED. PROCUREMENT DATA SYS., https://www.fpds.gov/fpdsng_cms/index.php/en/ [https://perma.cc/3JEJ-T93K] (enter "2032H521F00814" into the search field; find the result with "date signed" listed as Sept. 22, 2021; click "view").

20. Hannah Bloch-Wehba, *Algorithmic Governance from the Bottom Up*, 48 BYU L. REV. 69, 81–82 (2022).

21. Christopher Hood, *The "New Public Management" in the 1980s: Variations on a Theme*, 20 ACCT. ORGS. & SOC'Y 93, 95 (Feb. 1995).

22. *Id*.

23. Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342, 365 (2004); Jodi L. Short, *The Paranoid Style in Regulatory Reform*, 63 HASTINGS L.J. 633, 667 (2012).

mechanism.[24] But the "infusion of market principles into the political world" proved appealing across partisan divides.[25] President Clinton's National Performance Review drew on NPM thinking in both style and substance, rebranding governance as a management challenge.[26] In lieu of a new social contract, the National Performance Review envisioned a "new customer service contract with the American people, a new guarantee of effective, efficient, and responsive government."[27] These political projects put managerial goals such as customer service, public-private partnerships, and broader commitments to market-style measurements of governmental programs at the center of successive administrations' policy agendas.[28]

The metaphor of government-as-business draws on the rebranding of the citizen as a customer.[29] The Clinton Administration's efforts to reinvent government explicitly invoked "customer service" as the key to government success. Accordingly, Executive Order 12862 required government agencies "to establish and implement customer service standards" that would facilitate "customer service equal to the best in business."[30] Alongside the Government Performance and Results Act of 1993, the Act that brought "managing for results" into the federal government, the Clinton Administration's commitment to NPM doctrine was solidly established.[31] Nor did the Bush Administration stray from this commitment to managerialism.[32] Soon, however, ostensible commitments to customer service began to seem more of a mirage.[33] Indeed, from the citizen's perspective, NPM may have reduced faith in government effectiveness by failing to prioritize—and sometimes even undermining—

24. JON MICHAELS, CONSTITUTIONAL COUP: PRIVATIZATION'S THREAT TO THE AMERICAN PUBLIC 80 (2017).

25. E.S. Savas, *Privatization and the New Public Management*, 28 FORDHAM URB. L.J. 1731, 1736 (2001).

26. OFF. OF THE VICE PRESIDENT, FROM RED TAPE TO RESULTS: CREATING A GOVERNMENT THAT WORKS BETTER & COSTS LESS (1993).

27. *Id.*

28. *See* Jodi Short, *Regulatory Managerialism as Gaslighting Government*, 86 LAW & CONTEMP. PROBS. no. 3, 2023, at 1, 13 ("Customer-driven government is a touchstone of managerial regulation.").

29. Jane E. Fountain, *Paradoxes of Public Sector Customer Service*, 14 GOVERNANCE 55, 55 (2001).

30. Exec. Order No. 12862, 58 Fed. Reg. 176 (Sept. 11, 1993); *see also* Memorandum on Customer Service (Mar. 22 1995), *in* 1 PUBLIC PAPERS OF THE PRESIDENTS OF THE UNITED STATES: WILLIAM J. CLINTON 384, 384–85 (1995) (tasking agencies with continuing to measure results and match them up against customer service standards); Donald P. Moynihan, *Managing for Results in State Government: Evaluating a Decade of Reform*, 66 PUB. ADMIN. REV. 77, 84 (2006) ("[S]tate governments have lurched headlong into the pursuit of results-based government, hoping for improved efficiency and results-based accountability while only partially implementing the reforms necessary to achieve these goals.").

31. Government Performance and Results Act of 1993 § 2(b), 107 Stat. 285 (1993); Edward Long & Aimee L. Franklin, *The Paradox of Implementing the Government Performance and Results Act: Top-Down Direction for Bottom-Up Implementation*, 64 PUB. ADMIN. REV. 309, 315 (2004).

32. David H. Rosenbloom & Susanne J. Piotrowski, *Reflections on New Public Management-Style Reform in U.S. National Administration and Public Trust in Government, 1993–2003*, 4 CHINESE PUB. ADMIN. REV. 1, 3–4 (Sep. 2007); Dru Stevenson, *Privatization of Welfare Services: Delegation by Commercial Contract*, 45 ARIZ. L. REV. 83, 83 (2003).

33. Short, *supra* note 28, at 13–14.

transparency.[34]

The Obama Administration both extended the effort to reinvent government and sought to bring this remodeled state into the 21st century. With it came an expanded rhetoric of customer service. Executive Order 13571 furthered the existing vision of government-as-customer-service and combined it with commitments to technological progress: "with advances in technology and service delivery systems in other sectors, the public's expectations of the Government have continued to rise. The Government must keep pace with and even exceed those expectations."[35] The 2012 Federal Digital Government Strategy likewise emphasized how consumer expectations were changing expectations of what the state could do. It envisioned a customer-centric principle for digital government, "whether our customers are internal (e.g. the civilian and military federal workforce . . .) or external (e.g. individual citizens, businesses, research organizations, and state, local, and tribal governments)."[36]

Narratives of technological progress underpinned the notion that the ideal government was one that resembles—in strategy, substance, and ethos—a private firm. Silicon Valley's growing political, economic, and cultural influence had only made old forms of public governance seem less appealing by comparison, hampered by legacy infrastructure and contractors ill-equipped to use modern project management techniques or best-in-class technology.[37] Efforts to modernize government thus explicitly echoed earlier commitments to NPM-style reforms while drawing on often unfavorable comparisons between the public and private sectors.[38]

A common argument revolved around the perception that there was a profound gap between the state's technological capacity and that of private firms, parroting omnipresent talking points that governance and law "lag" behind technological progress.[39] Consider, for example, the comparison offered by Chris Hein, Director of Customer Engineering at Google Cloud:

> Political leaders are facing the pressure from their constituents who are saying, "If I can

34. Rosenbloom & Piotrowski, *supra* note 32, at 5.

35. Exec. Order No. 13571, 76 Fed. Reg. 24339 (Apr. 27, 2011).

36. DIGITAL GOVERNMENT, https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html [https://perma.cc/L7FL-797G] (last visited Apr. 3, 2023).

37. Sheryl Gay Stolberg & Michael D. Shear, *Inside the Race to Rescue a Health Care Site, and Obama*, N.Y. TIMES (Nov. 30, 2013), https://www.nytimes.com/2013/12/01/us/politics/inside-the-race-to-rescue-a-health-site-and-obama.html [https://perma.cc/B69K-X7CP]; Charles Petrie, *The Failure of HealthCare.Gov Exposes Silicon Valley Secrets*, 18 IEEE INTERNET COMPUTING 85 (Nov. 2014); Leonidas Anthopoulos et al., *Why E-Government Projects Fail? An Analysis of the Healthcare.Gov Website*, 33 GOV'T INFO. Q. 161 (Jan. 2016); Ines Mergel, *Agile Innovation Management in Government: A Research Agenda*, 33 GOV'T INFO. Q. 516 (Jul. 2016).

38. Short, *supra* note 28, at 5 (describing "relentless digs" at government).

39. Rebecca Crootof & BJ Ard, *Structuring Techlaw*, 34 HARV. J.L. & TECH. 347, 359 (2020) (identifying "the facile but persistent claim that 'law cannot keep up with new technologies'"); Gary E. Marchant, *The Growing Gap Between Emerging Technologies and the Law*, *in* THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT: THE PACING PROBLEM 19, 19 (Gary E. Marchant, Braden R. Allenby & Joseph R. Herkert eds., 2011).

> get my Amazon packages delivered as quickly as I can, how come I can't get unemployment assistance without filling out 60 pages of forms?" . . . Or how come a consumer can enter Home Depot and use technology to navigate exactly what aisle and bin a screw are in but not be able to locate a form for a fishing license?[40]

Across multiple dimensions, government modernization, digitization, and datafication had its roots in the ideological and pragmatic twinning of government and business. By reimagining citizens as consumers, the state justified its embrace of the same techniques and technologies that it saw as prevalent in business—albeit in impoverished form.[41] Embracing managerialism in this political-cultural climate brought with it the rise of market solutions and outsourcing as integral parts of government modernization. These dynamics then carried over into new modernization efforts oriented around new technologies. As scholars affiliated with the Data & Society Research Institute have described it, "The Datafied State is one remade by the data sources and infrastructures, computational tools and techniques that are being adopted across Government just as they are in the private sector."[42] Indeed, some scholars have contended that public agencies ought to function more like the private sector businesses they regulate by using the same technologies and strategies.[43] The practice of contracting out and outsourcing likewise reflect an ideological commitment to "businesslike government."[44]

On the one hand, political commitments to market-style reforms, privatization, and contracting-out laid the foundation for increased private provision of historically public services. On the other hand, the emergence of new business models and technological capacities also encouraged a further re-envisioning of the state to draw on the best of private innovation. This reimagining of the state encouraged it to try to match the kinds of things possible in a company like Google or Microsoft but not previously in an agency like the Department of the Interior. These twin strands thus proved a remarkably solid footing for the entrée of tech firms into public governance.

However, government actors have neglected a key strand of earlier comparisons between the state and the private sector in at least one crucial way. Advocates of "reinventing government" (in popular parlance) and the NPM (in the jargon of public administration) promoted the notion that the government could, and should, compete with the private sector, abandoning historic

40. *Why Government Leaders are Turning to AI*, NEXTGOV (Aug. 8, 2022), https://www.nextgov.com/sponsors/2022/08/why-government-leaders-are-turning-ai/368708/ [https://perma.cc/N6FL-HWMT].

41. Short, *supra* note 28, at 8 ("[R]egulatory managerialism either degrades or omits key techniques, ideas, and competencies that are essential to management theory and to the successful management of a business in practice.").

42. *The Datafied State*, *supra* note 15.

43. Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 GEO. L.J. 1147, 1153 (2017).

44. *See* MICHAELS, *supra* note 24, at 96–97 ("[Outsourcing] held out the promise of providing the same services for less money and less bureaucracy.").

"monopolies" on public provision.[45] The earlier advocates of privatization and contracting-out saw government dominance of service provision as the "American way."[46] Forcing government actors to compete against the private sector, the thinking went, would make them more entrepreneurial and better equipped to "satisfy people's needs."[47]

If public agencies were made to *compete* with private vendors, then all service providers would "keep their costs down, respond quickly to changing demands, and strive mightily to satisfy their customers."[48] In most of the scenarios in which privatization and contracting-out were envisioned, the "customers" were individual citizens who benefited directly from the service or program at issue: users of the post office, recipients of welfare benefits, and so forth.[49] Indeed, one of the prototypical case studies of how competition between government agencies and private vendors could drive better results was trash collection, where the benefits of better service were visible and tangible.[50]

In reality, however, the competitive rationale for privatization was selectively applied. The state has increasingly opted out of competing with private technology vendors, becoming a customer of dominant software companies rather than a competing producer in its own right. As I describe below, the longstanding presumption that the state ought to procure rather than make commercial products and services is partly responsible for this preference.[51] Guided by budgetary constraints and legal and policy preferences for acquiring commercial products rather than building custom solutions, the federal government spends the majority of its technology budget on contracts.[52] Efforts to promote tech expertise in and around government, such as the Presidential Innovation Fellowship and 18F, a "digital services agency" within the General Services Administration, have had limited effects on the overall preference toward contracting out.[53]

New efforts to bolster tech innovation in government continue to emphasize this approach. For example, the AGILE Procurement Act of 2022 doubles down on this tendency by seeking to advance government innovation not through public development but rather through investment in better procurement

45. Savas, *supra* note 25, at 1736; DAVID OSBORNE & TED GAEBLER, REINVENTING GOVERNMENT: HOW THE ENTREPRENEURIAL SPIRIT IS TRANSFORMING THE PUBLIC SECTOR 82 (1992).

46. OSBORNE & GAEBLER, *supra* note 45, at 79.

47. Savas, *supra* note 25, at 1731.

48. OSBORNE & GAEBLER, *supra* note 45, at 79.

49. E. S. Savas, *It's Time to Privatize*, 19 FORDHAM URB. L.J. 781, 794–95 (1992) (calling on New York City to "give citizens more for their tax dollars").

50. *Id*. at 792–93; Matthew Diller, *Form and Substance in the Privatization of Poverty Programs*, 49 UCLA L. REV. 1739, 1745 (2002); Stevenson, *supra* note 32, at 85.

51. *See infra* text accompanying notes 182–186.

52. AGILE Procurement Act of 2022, S. 4623, 117th Cong. § 2 (2022) ("Contract spending accounts for more than 80 percent of the Federal information technology budget.").

53. Indeed, 18F itself plays a significant role in helping agencies *buy* technologies as much as *build* them. *About*, 18F, https://18f.gsa.gov/about/ [https://perma.cc/D4QY-FCDV] (last visited Apr. 3, 2023).

efforts.[54] At the state and local level, budgetary constraints are yet more palpable and tech expertise is harder to come by, pushing even more toward contracting-out as a mechanism for acquiring innovative governance technologies.[55]

III

FROM PUBLIC TRANSPARENCY TO CORPORATE SECRECY

The withering of publicly funded and developed technology, and the preference for commercial sourcing, allowed the private sector to dominate the provision of tech to state actors. The increasing importance of technology-driven functions that the government lacks the capacity to perform also creates new opportunities for the "corporate reconstruction of the state."[56] By buying data, software, and technological infrastructure from private vendors, governments can take advantage of technological advances. But much of that software is private in two senses: First, the software is privately developed. Second, key aspects of the software are not public; they are held in secret or in confidence. Along with the state's corporate reconstruction comes a displacement of the traditional modes of government accountability by corporate secrecy. The modernization of government infrastructure, in this form, comes at a cost to public values.

At one level, privatization reduces government competence and thus amplifies claims of ineptitude and haplessness. Outsourcing means that government agencies often lack information, understanding, and knowledge about how new infrastructures and governance techniques function.[57] Public records laws don't reach government contractors directly, and public agencies often don't have records reflecting how these tools function.[58] In cases when government agencies do have relevant records, vendors frequently cite trade secrecy interests as justification for nondisclosure.[59] As Julie Cohen has put it, open government laws are "poorly adapted to ensuring transparency where a significant privatization component is involved."[60]

Indeed, privatization stretches the framework of transparency law to its limits. Although public records statutes are the "legal bedrock of the public's right to know about our government," they fall short of fulfilling this role amid

54. S. 4623 §§ 5–6.

55. *Cf.* MICHAELS, *supra* note 24, at 93–94 (explaining how privatization tended to unfold at the state and local level faster than the federal level).

56. Fourcade & Gordon, s*upra* note 5, at 78.

57. Stolberg & Shear, *supra* note 37; *see also* Ryan Calo & Danielle Keats Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 EMORY L.J. 797, 817 (2021) (describing how government reliance on algorithms "jettison[s] expertise and discretion").

58. Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1299 (2020).

59. FMI v. Argus Leader, 139 S. Ct. 2356, 2358 (2019); Christopher Morten, *Publicizing Corporate Secrets*, 171 UNIV. PA. L. REV. (forthcoming 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4041556 [https://perma.cc/CM6E-SV2Z].

60. JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 191 (2019).

broad shifts toward privatization and contracting-out.[61] The federal Freedom of Information Act ("FOIA") and its state equivalents are the "dominant means by which the public obtains information" from government agencies.[62] These statutes are designed as "right-to-know" or "open government" laws, which entitle individuals to request agency records.[63] Open government laws are, by design, focused exclusively on records held by government agencies. They do not reach records outside of an agency's control—including records held by government contractors.[64] The inability to use open government laws to retrieve information from private vendors and contractors makes them a subpar mechanism for achieving meaningful oversight. In a critical account, David Pozen has described how open government statutes have reinforced the state's image as hapless, corrupt, and inefficient compared to a private sector that benefits from relative reputational purity.[65]

Emerging technology-intensive forms of governance heighten concerns that the rights-based, reactive framework of open government laws is insufficient to protect transparency and accountability. One major worry is the rise of trade secrecy to conceal how new technologies of governance operate. Public records laws shelter corporate secrets from disclosure through exemptions for trade secrets and confidential commercial information.[66] As a result, when individuals or organizations petition for access to corporate records held by the government, agencies often defer to industry and argue that those records are exempt.[67]

In governance contexts involving contractors and vendors, exemptions for trade secrets thus weaken what would otherwise be clear-cut transparency obligations. Writing in 2007, David Levine described how Diebold, a manufacturer of voting machines, invoked trade secrecy to avoid disclosing the machines' source code for public inspection.[68] When important elements of public infrastructure are contracted out, Levine argued, trade secrecy threatens to transform infrastructure into "just another product that is bought and sold."[69] In a clash between trade secrecy and public records law, Levine argued, democratic norms meant that the latter should prevail.[70]

Fifteen years later, the phenomenon Levine described has dramatically expanded. The rise of automated decision-making across various domains has

61. Beth Simone Noveck, *Is Open Data the Death of FOIA*, 126 YALE L.J.F. 273, 273 (2016); Robert Brauneis & Ellen P Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 151–52 (2018).

62. Morten, *supra* note 59, at 13.

63. ARCHON FUNG, MARY GRAHAM & DAVID WEIL, FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 24–26 (2007).

64. Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1299 (2020).

65. David E. Pozen, *Transparency's Ideological Drift*, 128 YALE L.J. 100, 157 (2018).

66. Morten, *supra* note 59, at 26.

67. *Id.*

68. David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135, 139 (2007).

69. *Id.* at 165.

70. *Id.*

ushered in a new era of corporate secrecy in public governance. Algorithmic governance in criminal legal enforcement, immigration, the provision of public benefits, child protection, and a variety of other settings has transformed how individual rights are enforced and how benefits are allocated.[71] Trade secrecy has become particularly relevant in the context of software. As Sonia Katyal has written, rules on copyright and patent for software effectively discourage firms from employing those protections for intellectual property and encourage broader use of trade secrecy.[72] As a result, emerging information-intensive modes of governance often involve broad claims of trade secrecy. As individuals who are affected by these mechanisms seek redress, high-profile legal controversies have increasingly pitted due process rights against trade secrecy arguments.[73]

Tech firms use a combination of trade secrecy and contract to designate information related to public governance as confidential and conceal it from public view. In litigation, this puts agencies in the position of arguing for their vendors' commercial interests. For instance, when a journalist sought records concerning an artificial intelligence defense system developed by defense contractor Anduril and adopted by the Marine Corps, Anduril "influenced the decision" by the Marine Corps to withhold the records on the basis that they contained purported trade secrets.[74] Likewise, when civil liberties advocates sought access to information about Palantir, the New York Police Department resisted the request, arguing that Palantir's trade secrecy interests precluded it from releasing information under New York's Freedom of Information Law.[75] Similarly, consider *State v. Pickett*, in which New Jersey prosecutors argued that trade secrecy interests belonging to a vendor of probabilistic DNA software precluded the prosecution from disclosing source code to the defense.[76] All of these cases involve government actors leveraging private firms' ostensible trade secrecy interests to justify keeping public records under wraps.

Trade secrecy is not the only corporate secrecy doctrine, however.[77] The law also insulates corporate decision-making regarding publicity from external

71. VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 3 (2018) ("Automated eligibility systems, ranking algorithms, and predictive risk models control which neighborhoods get policed, which families attain needed resources, who is short-listed for employment, and who is investigated for fraud.").

72. Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 125 (2019).

73. Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1346 (2018); Natalie Ram, *Innovating Criminal Justice*, 112 NW. L. REV. 659, 659 (2018).

74. First Look Inst., Inc. v. U.S. Marine Corps, No. 2:21-cv-05087-MCS-RAO, 2022 WL 2784431, at *1 (C.D. Cal. June 13, 2022).

75. Brennan Ctr. for Just. at N.Y. Univ. Sch. of Law v. N.Y.C Police Dep't, 2017 N.Y. Misc. LEXIS 5138, at *9 (N.Y. Sup. Ct. Dec. 22, 2017).

76. State v. Pickett, 466 N.J. Super. 270, 306 (App. Div. 2021).

77. *See generally* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241 (1998); Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311 (2008) (exploring lingering questions about how trade secrecy law fits with other areas of law that protect corporate information).

control in broader respects. Companies possess "enormous latitude to designate information as confidential" and prevent employees from speaking about corporate matters beyond bona fide trade secrets.[78] Nondisclosure agreements ("NDAs"), corporate information policies, and other agreements are widespread. By some estimates, nearly two-thirds of tech workers are subject to an NDA, and nearly forty percent are bound to silence about "injustices in the workplace."[79] NDAs can create serious social costs even when parties with equal bargaining power freely and voluntarily enter into them.[80] Beyond NDAs, firms also impose broader systems of corporate control over corporate information through contract.[81] For example, Google has terminated whistleblowers for violating company file storage and email policy.[82]

Corporate control of information can extend to government settings as well. Through contract, technology firms sometimes require government agencies to circumvent requirements of open government and due process by signing NDAs. The paradigmatic example is Harris Corp., the manufacturer of StingRay surveillance devices, which required jurisdictions not to disclose the existence of the technology to anyone—even criminal defendants whose due process rights were implicated by the surveillance technique.[83] Hacking Team, the Italian vendor of offensive surveillance capabilities, likewise required police agencies to sign broad NDAs in order to even try the technology.[84] Even outside the context of law enforcement, NDAs remain common: Amazon required cities interested in bidding for its second headquarters ("HQ2") to sign nondisclosure and confidentiality agreements with the company.[85] Those agreements helped to

78. Rachel S. Arnow-Richman et al., *Supporting Market Accountability, Workplace Equity, and Fair Competition by Reining in Non-Disclosure Agreements*, DAY ONE PROJECT 2 (Jan. 2022), https://uploads.dayoneproject.org/2022/04/14172008/Supporting-Market-Accountability-Workplace-Equity-and-Fair-Competition-by-Reining-in-Non-Disclosure-Agreements_final.pdf [https://perma.cc/SEE4-C4FR].

79. Emily Birnbaum, *A Wall of Silence Holding Back Racial Progress in Tech: NDAs*, PROTOCOL (July 1, 2020), https://www.protocol.com/nda-racism-equality-diversity-tech [https://perma.cc/H7NN-T5AS].

80. David A. Hoffman & Erik Lampmann, *Hushing Contracts*, 97 WASH. UNIV. L. REV. 165, 174 (2019); *see also* David A. Hoffman & Cathy Hwang, *The Social Cost of Contract*, 121 COLUM. L. REV. 979, 982 (2021) (discussing how the public interacts with private contracts).

81. *See* Deepa Varadarajan, *The Trade Secret-Contract Interface*, 103 IOWA L. REV. 1543, 1543 (2018) (foregrounding the role of contract in trade secret law).

82. *E.g.*, *Google Fires Margaret Mitchell, Another Top Researcher on Its AI Ethics Team*, THE GUARDIAN (Feb. 20, 2021), https://www.theguardian.com/technology/2021/feb/19/google-fires-margaret-mitchell-ai-ethics-team [https://perma.cc/4YAD-CE2B]; Jay Peters, *Google settles with worker allegedly fired for his workplace activism*, THE VERGE (Sept. 8, 2021), https://www.theverge.com/2021/9/8/22663354/google-laurence-berland-workplace-activism-nlrb [https://perma.cc/2AZ9-KNFF] (discussing Google's settlement with a whistleblower).

83. Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 19, 22 (2017).

84. *Hacking Team Non-Disclosure Agreement*, MUCKROCK, https://www.muckrock.com/foi/california-52/ucsb-police-department-hacking-team-emails-and-acquisition-docs-19961/#file-51963 [https://perma.cc/EZJ9-M723].

85. Martin Austermuhle, *Amazon Insists on Silence from Twenty HQ2 Finalists*, WAMU (Jan. 30, 2018), https://wamu.org/story/18/01/30/amazon-insists-silence-twenty-hq2-finalists/

ensure that the public would not possess detailed information about the kinds of incentives that cities were offering Amazon.[86]

Technology vendors also mount security-based arguments against disclosure that seem more familiar to government actors, reflecting broader alignments between the interests of the state and those of its contractors. As Levine points out, trade secrecy has been "increasingly linked to national security" as a core aspect of economic security.[87] As Frank Pasquale has observed in the context of intelligence-gathering, government interests in security have fostered a "pragmatic, powerful, and largely secret partnership with interests whose concern is not the public good, but private profit or personal advance."[88]

In short, private and government interests in secrecy are converging. At the state and local levels, the alignment of corporate secrecy with government secrecy interests is remarkable, as both Palantir and *Pickett* illustrate. In this same vein, consider *Crawford v. DoITT*, a New York Freedom of Information lawsuit in which Professor Susan Crawford sought access to maps of New York City's broadband conduit network to understand where new entrants might be able to provide internet service.[89] In response to the request, the city asserted that disclosing the records could leave the infrastructure vulnerable to terrorist attacks and reveal the trade secrets of broadband service providers, such as AT&T and Time Warner Cable, that leased conduit space from the city.[90] Meanwhile, broadband service providers intervened in the litigation, arguing that disclosing the location of the conduits would jeopardize both security and commercial interests.[91] As their overlapping arguments demonstrate, the commercial secrecy interests of firms like AT&T and Time Warner Cable were overtly aligned with the city's professed interest in security.

Finally, broader structural dynamics buttress claims of corporate secrecy and undermine transparency. When governments contract out to private technology firms, the firms themselves often retain critical information about how the technology works.[92] As Deirdre Mulligan and Kenneth Bamberger have put it,

---

[https://perma.cc/T32K-FPGU].

86. Julie Creswell, *Cities' Offers for Amazon Base Are Secrets Even to Many City Leaders*, N.Y. TIMES (Aug. 5, 2018), https://www.nytimes.com/2018/08/05/technology/amazon-headquarters-hq2.html [https://perma.cc/XNU5-BJHM]; Greg Bluestein, *Inside Georgia's Secret Bid for Amazon's Second Headquarters*, ATLANTA J.-CONST. (Nov. 14, 2018).

87. Levine, *supra* note 68, at 162.

88. FRANK PASQUALE, BLACK BOX SOCIETY 43 (2015).

89. Brief for Petitioner, Crawford v. N.Y.C. Dep't of Info. Tech. & Telecomms., No. 157002/2015 (N.Y Sup. Ct. July 10, 2015).

90. Memorandum of Law in Support of Respondent's Verified Answer at 5–6, Crawford v. N.Y.C. Dep't of Info. Tech. & Telecomms., No. 157002/2015 (N.Y Sup. Ct. Feb. 3, 2017).

91. *See, e.g.*, Memorandum of Law in Support of Time Warner Cable Inc.'s Motion for Leave to Intervene as Respondent and in Opposition to Petitioner's Application for a Judgment under CPLR Article 78 at 8–9, Crawford v. N.Y.C. Dep't of Info. Tech. & Telecomms., No. 157002/2015 (N.Y Sup. Ct. Nov. 12, 2015); Memorandum of Law in Support of AT&T Corp.'s Motion for Leave to Intervene at 4–5, Crawford v. N.Y.C. Dep't of Info. Tech. & Telecomms., No. 157002/2015 (N.Y Sup. Ct. Nov. 19, 2015) (arguing that both security and trade secrecy concerns mitigated against disclosure).

92. Robert Brauneis & Ellen P Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE

artificial intelligence and machine learning systems "frequently displace discretion" formerly held by government officials with "an opaque logic."[93] Proprietary records also displace public records. After filing dozens of open records requests, Ellen Goodman and Robert Brauneis found that in many cases, government agencies "simply did not have many records concerning the creation and implementation of algorithms, either because those records were never generated or because they were generated by contractors and never provided to the governmental clients."[94]

In this way, public-private partnerships can both undermine government expertise and provide a powerful justification for public actors to disclaim responsibility and even awareness of significant problems. Consider, for example, what happened when the Houston Independent School District ("HISD") contracted with the technology firm SAS to evaluate teacher effectiveness. SAS developed an algorithm to distinguish between effective and ineffective teachers. But because it treated the algorithm as a trade secret, HISD neither had meaningful access nor knew how it worked.[95] HISD used the algorithm-generated scores to assess teachers' value and whether they were deserving of continued employment.[96] Teachers argued that relying on scores calculated using SAS's opaque methodology violated their due process rights regarding their employment because they could not "meaningfully challenge terminations."[97] These kinds of agreements allow both vendors and public agencies to point fingers and shirk responsibility. Indeed, Houston said that it could not reproduce teachers' scores to ensure they were error-free in part because it would cost too much for them to do so.[98]

The tech industry's secrecy baseline, coupled with firms' increasing role in public governance, has increased pressure on whistleblowers and leaks to provide key information about public-private partnerships. For example, whistleblowers who work at private technology firms have played an important role in drawing public attention to contracts with immigration and national security agencies.[99] Other whistleblowers, such as Frances Haugen at Facebook, Christopher Wylie at Cambridge Analytica, and Peiter "Mudge" Zatko at Twitter have come forward with information that is deeply relevant to public governance, even if it

J.L. & TECH. 103, 152 (2018).

93. Deirdre K. Mulligan & Kenneth A. Bamberger, *Procurement as Policy: Administrative Process for Machine Learning*, 34 BERKELEY TECH. L.J. 773, 778 (2019).

94. Brauneis & Goodman, *supra* note 92, at 152.

95. Hous. Fed'n of Teachers, Local 2415 v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1176–77 (S.D. Tex. 2017).

96. *Id.*

97. *Id.* at 1173.

98. *Id.* at 1177.

99. Jay Peters, *Google Settles with Worker Allegedly Fired for His Workplace Activism*, VERGE (Sept. 8, 2021), https://www.theverge.com/2021/9/8/22663354/google-laurence-berland-workplace-activism-nlrb [https://perma.cc/PQ27-8WGD]; Colin Lecher, *GitHub Will Keep Selling Software to ICE, Leaked Email Says*, VERGE (Oct. 9, 2019), https://www.theverge.com/2019/10/9/20906213/github-ice-microsoft-software-email-contract-immigration-nonprofit-donation [https://perma.cc/3MHU-4PDM].

does not relate directly to regulation.

In contexts of overwhelming secrecy, leaks provide a crucial safety valve to ensure that critical information finds an audience.[100] But workers who disclose company information do so at their own peril. Across disparate domains, legal baseline rules favor firms' decision-making about how to control and share information. These baselines leave workers beholden to corporate decision-making about information sharing and unable to disclose even newsworthy information without significant legal risk. [101] Labor law, for example, has long adopted what Gali Racabi calls the "employer prerogative," which creates "a rebuttable presumption against contractual, statutory, and constitutional intrusions into management decision-making."[102] The employer prerogative "cuts against claims of protected speech at the workplace" and operates as a default rule that subordinates workers' speech interests to those of their employers.[103]

These four informational dynamics—trade secrecy, corporate control, the alignment of corporate and security interests, and the divestment of knowledge from the public to the private sector—collectively constrain the potential avenues for the public to understand a broad range of emerging governance issues. Alongside the broadening adoption of automated tools in public governance, simultaneous shifts are taking place from public-oriented frameworks for transparency and accountability toward much more limited frameworks for private transparency.

IV

PUBLIC CONTROL OF THE DATAFIED STATE

The introduction of technology-mediated techniques in public governance thus brings with it a shift in power from the public to the private sector. It replicates and extends previous tendencies toward privatization and outsourcing, but it also gives credence to commercial claims of confidentiality and secrecy that further immunize private authority from accountability. This new paradigm for governance requires us both to rethink the necessary preconditions of democratic accountability and public transparency as well as imagine frameworks and approaches that might be better suited to safeguarding these values in an increasingly privatized state.

A. Bar Trade Secrecy in Public Contracting

To start, we might rethink the presumption that government contractors can

100. RAHUL SAGAR, SECRETS AND LEAKS 43 (2013).

101. Gali Racabi, *Abolish the Employer Prerogative, Unleash Work Law*, 43 BERKELEY J. EMP. & LAB. L. 79, 95 (2022).

102. *Id.* at 85.

103. *Id*.

assert trade secrecy to conceal vital aspects of their services and products.[104] A trade secret, broadly speaking, is information that is kept secret and that is valuable at least in part *because* it is secret.[105] Protections for trade secrecy are rooted in part in economic efficiency: trade secrets are said to encourage creators to innovate by minimizing the risk that others will freeride on their initial investment.[106] Trade secret laws are also said to reduce transaction costs and economic investment in practical secrecy measures; "deterring wasteful investments in an economic espionage arms race."[107] Finally, there are also moral and ethical justifications for punishing the misappropriation of trade secrets.[108] On the other hand, the significant social costs of secrecy create tensions with other intellectual property values, including valuable disclosure that facilitates both speech and innovation activities.[109]

Baked into protections for corporate secrecy for government contractors is an underlying assumption that private firms will not contract with government entities unless they retain robust protections for their intellectual property and trade secrets. The theory is that private firms compete for lucrative government contracts; yielding any degree of intellectual property protection makes them less competitive. Further, the lower cost to taxpayers of privatization through contract justifies the tradeoff with transparency.

On closer inspection, however, it is far from self-evident that protecting trade secrets in the context of government contracts is essential to compensate innovators and ensure that government has access to cutting-edge technology. As Yafit Lev-Aretz and Katherine Strandburg have argued, intellectual property protections compensate innovators in situations where competitors would otherwise free-ride on the innovator's investment in research and development.[110] But where government agencies face high legal and logistical switching costs, vendors have significant first-mover advantages that may more than compensate for their otherwise free-rideable investments.[111] Beyond face value, certain government contracts also have other appealing features that might offset diminished protection for corporate secrecy. The value of government contracts for certain artificial intelligence or machine learning applications is at

104. Under Executive Order 12600, federal agencies are required to notify entities that submit trade secrets and confidential commercial information when someone submits a FOIA request for those records. Exec. Order No. 12600, 52 Fed. Reg. 23781 (June 23, 1987).

105. Michael Risch, *Why Do We Have Trade Secrets*, 11 MARQ. INTELL. PROP. L. REV. 1, 7–8 (2007) (setting forth UTSA and Restatement definitions of trade secrets).

106. Bone, *supra* note 77, at 263; Lemley, *supra* note 77, at 326. *But see* Risch, *supra* note 105, at 27 ("[T]he marginal incentive to innovate protected by trade secret law is small because companies would still protect secret information by—obviously enough—keeping such information secret.").

107. Eli Siems, Katherine Strandburg & Nicholas Vincent, *Trade Secrecy and Innovation in Forensic Technology*, 73 HASTINGS L.J. 773, 778 (2022); Bone, *supra* note 77, at 272.

108. Risch, *supra* note 105, at 36.

109. Siems, Strandburg & Vincent, *supra* note 107, at 798–99.

110. Yafit Lev-Aretz & Katherine J. Strandburg, *Regulation and Innovation: Approaching Market Failure from Both Sides*, 38 JREG BULL. 1, 12–13 (2020).

111. *Id.* at 14–15.

least partially that tech firms can ingest data provided by the state to train machine learning models.[112] If I am correct that the data itself is of significant value, then perhaps trade secrecy for other key information about how the models work is less important. But the prospect that vendors might profit by using sensitive data collected by the state in undisclosed, unpredictable ways raises important concerns about privacy.[113] It is unpalatable, to say the least, that sensitive individual data might compensate innovators for their research and development costs, particularly where individuals have no voice in the matter.

Policymakers might reasonably decide that the significant social costs of secrecy outweigh the need to incentivize innovation through trade secrecy. In criminal law enforcement, for example, trade secrecy is running headlong into due process protections, as police agencies use proprietary software to investigate and surveil without disclosing critical information to defendants.[114] In response, policymakers have begun to constrain secrecy and mandate additional disclosure, particularly where due process is at stake. For instance, in 2019, Idaho passed a law that bars trade secrecy defenses for pretrial risk assessments.[115] The politics of this are complicated: bail bondsmen have opposed pretrial risk assessments because they depart from the traditional mechanism of money bail to ensure pretrial release.[116] Similarly, the Justice in Forensic Algorithms Act, sintroduced in 2019, would require defendants to be given access to source code and other critical information about forensic algorithms.[117]

However, most initiatives to bring transparency to algorithmic governance to date adopt a managerial approach. Consider SB 5116, a bill introduced in Washington that would require state agencies to affirmatively generate certain records about algorithmic governance (while leaving corporate secrecy largely untouched). Under SB 5116, agencies are only permitted to develop, procure, and use automated decision systems after the agency completes and approves an

112. *See* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 361–62 (2022) (providing a clear explanation of how this works in practice).

113. In particular, the Privacy Act of 1974 limits the circumstances under which government actors might share individual records. 5 U.S.C. § 552(a). *See* Solow-Niederman, *supra* note 112 (arguing that even if information is shared for a "routine use," which is permitted under the statute, vendors might derive significant benefits from processing that data and drawing inferences from it).

114. Natalie Ram, Christi J. Guerrini & Amy L. McGuire, *Genealogy Databases and the Future of Criminal Investigation*, 360 SCIENCE 1078 (June 2018); Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. 192 (2019); Deborah Won, *The Missing Algorithm: Safeguarding Brady against the Rise of Trade Secrecy in Policing*, 120 MICH. L. REV. 157 (2021).

115. H.B. 118, 65th Leg., 1st Sess. (Idaho 2019).

116. *Idaho Officials Proclaim the Success of the Idaho Pretrial Risk Assessment Tool the Day Before a Landmark Study Came out that Proves It Doesn't Work*, AM. BAIL COAL. (Nov. 26, 2019), https://ambailcoalition.org/idaho-officials-proclaim-the-success-of-the-idaho-pretrial-risk-assessment-tool-the-day-before-a-landmark-study-came-out-that-proves-it-doesnt-work/.

117. *Rep. Takano Introduces the Justice in Forensic Algorithms Act to Protect Defendants' Due Process Rights in the Criminal Justice System*, TAKANO (Sept. 17, 2019), https://takano.house.gov/newsroom/press-releases/rep-takano-introduces-the-justice-in-forensic-algorithms-act-to-protect-defendants-due-process-rights-in-the-criminal-justice-system [https://perma.cc/CEG4-3YHV].

algorithmic accountability report.[118] SB 5116 also requires vendors to make automated decision systems available for independent audits.[119] SB 5116 is a step toward reducing algorithm secrecy, but aside from an auditing mandate, it does not impose any additional obligations or requirements on the vendors themselves. Indeed, the auditing mandate it adopts might rightly be scrutinized itself as symptomatic of the privatization of regulation.[120] Rather, SB 5116 foists additional disclosure requirements on state agencies without implicating corporate secrecy at all.

More substantial departures from the managerial approach are necessary to address corporate secrecy. One set of reforms should tackle the problem of agency deference to corporate secrecy claims. As Christopher Morten and Amy Kapczynski have argued in the context of the Food and Drug Administration, federal agencies can and should rescind regulations that promise not to publicly disclose trade secrets or confidential commercial information.[121] In a separate work, Morten has argued that, far from requiring agencies to guard trade secrets closely, "the federal regulatory state can and should undertake a comprehensive, intentional program of information publicity."[122] As Morten and Kapczynski show, at least as a matter of federal law, agencies are far more capable of disclosing trade secrets than is commonly appreciated.[123]

At a minimum, legal change could require vendors to defend their own trade secrecy interests in litigation instead of expecting government agencies to litigate trade secrecy defenses on behalf of their vendors. Imagine, for instance, that a journalist, defendant, or advocacy group files a lawsuit to compel an agency to release information about a new piece of software that the agency is using. The software developer claims that the records being sought contain trade secrets. The current framework allows the agency to advance that trade secrecy claim on behalf of the vendor.[124] The agency, not the vendor, bears the burden of establishing that the records are exempt from disclosure.[125]

It need not be this way. Because FOIA exemptions are permissive, not mandatory, agencies could adopt regulations that authorize them to make discretionary releases of trade secrets.[126] Agencies should also simply refuse to litigate trade secrecy cases on behalf of private entities.[127] Instead, entities who

118. S.B. 5116, 67th Leg., Reg. Sess. (Wash. 2021).

119. *Id.*

120. ARI EZRA WALDMAN, INDUSTRY UNBOUND 241 (2021) (discussing the rise of privacy audits).

121. Christopher J. Morten & Amy Kapczynski, *The Big Data Regulator, Rebooted: Why and How the FDA Can and Should Disclose Confidential Data on Prescription Drugs and Vaccines*, 109 CAL. L. REV. 493, 540–41 (2021).

122. Morten, *supra* note 59, at 30.

123. *See* First Look v. Marine Corps, No. 221CV05087MCSRAO, 2022 WL 2784431 (C.D. Cal. June 13, 2022) (showing that just because an agency *can* disclose trade secrets doesn't mean that it will).

124. *See supra* discussion accompanying notes 84–109.

125. 5 U.S.C. § 552(a)(4)(A).

126. Morten, *supra* note 59, at 63.

127. 5 U.S.C. § 552(b)(4) (FOIA's disclosure requirements do "not apply" to trade secrets or confidential commercial information"). As Chris Morten points out, the federal Trade Secrets Act

seek to suppress disclosure should be permitted to intervene as interested parties to make the trade secrecy claims themselves. This would require vendors, not taxpayers, to foot the bill if they want to prevent disclosure. Precedent exists for this kind of burden-shifting. Vendors often file what are known as "reverse FOIA" lawsuits to *enjoin* the disclosure of records containing purported trade secrets in response to public records requests.[128] In all likelihood, requiring the owners of trade secrets to justify their nondisclosure would be efficiency-enhancing because those owners are the best positioned to describe the competitive impact of disclosure and the measures they have taken to protect the alleged secrets.

Other reforms might require more robust transparency requirements. Through legislation or through executive order, the government can require that vendors create certain kinds of information and submit it to agency customers on the understanding that the documentation may be subject to open government laws. In spirit and in substance, this reform follows the model of what Fung, Graham, and Weil call the "second generation of legislated transparency, *targeted transparency policies* . . . [which] mandate access to precisely defined and structured factual information from private or public sources with the aim of furthering particular policy objectives."[129] Targeted transparency is particularly essential with respect to technologically mediated forms of governance that might be opaque or inscrutable even if data is made public.[130]

Targeted transparency does not abandon managerialism, but it could lend more rigor. Drawing from the proposal that standardized documentation procedures be employed to explain how artificial intelligence and machine learning models function, the government could require vendors of technology to affirmatively generate and disclose certain kinds of information in standardized formats and for specific audiences.[131] For example, tools used to make decisions about public benefits or criminal punishment should be required to regularly undergo independent, third-party validation tests. Regular, repeated, independent validation that is conducted out in the open minimizes, though does not eliminate, the risk that oversight might be reduced to a compliance exercise of "procedural box-checking."[132] With respect to automated decision systems, vendors could be required to produce documentation of any model in use, including an executive summary, a list of variables that the model considers and

prohibits federal employees from disclosing trade secrets "unless authorized by law." Morten, *supra* note 59, at 60. But numerous agencies *are* authorized to disclose trade secrets under their authorizing regulations. *Id.* at 63–67.

128. Christopher S. Yoo & Kellen McCoy, *Privacy vs. Transparency: Handling Protected Materials in Agency Rulemaking*, 96 IND. L.J. 1259, 1277 (2021) (describing how businesses can use reverse FOIA suits to prevent the disclosure of bona fide trade secrets).

129. FUNG, GRAHAM & WEIL, supra note 63, at 25.

130. *See* Jenna Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, 3 3 BIG DATA & SOC'Y., no. 1, at 1, 1–2 (Jun. 2016) (explaining algorithmic opacity).

131. Margaret Mitchell et al., *Model Cards for Model Reporting*, PROC. CONF. ON FAIRNESS ACCOUNTABILITY & TRANSPARENCY, 220 (2019).

132. WALDMAN, *supra* note 120, at 136.

their relative weights, an explanation of the techniques employed by the model, documentation explaining how the model was trained, and the results of any validation tests that have been conducted.

Importantly, at least some of these policy goals might be achieved through executive action, even if Congress or state legislatures balk. Under the Federal Property and Administrative Services Act of 1949, the President has the power to "prescribe policies and directives that the President considers necessary to carry out"[133] the statutory goals of promoting an "economical and efficient system" for contracting.[134] This sweeping statutory language confers broad discretion for the President to exercise control over federal contracting. Using this authority, the federal government can use its power as a customer to encourage contractors to use trade secrecy more sparingly. The government can leverage its appeal as a customer in order to secure substantive change on the part of its contractors. For example, an executive order initially adopted under the Johnson Administration bars federal contractors from discriminating on the basis of race, gender, gender identity, religion, protected veteran status, and other characteristics and requires federal contractors to adopt affirmative action programs to promote equal opportunity.[135] In a more depressing turn, the Trump Administration infamously wielded its control over federal contractors to attempt to bar workplace diversity trainings that involved "stereotyping or scapegoating."[136] Until December 2022, when the Fifth Circuit invalidated the Biden Administration's vaccine mandate for federal contractors, a court had never struck down an executive order under the Procurement Act.[137]

The Procurement Act requires the President to demonstrate a sufficiently close nexus between the statute's goals of efficiency and economy, and the requirements set forth in an executive order.[138] This standard is not demanding. It is entirely plausible that, through executive order, the federal government can shift the procedural and substantive rules governing trade secrecy in federal contracts. For example, an executive order could require federal contracts for automated decision systems to include a clause that waives trade secrecy protections in noncommercial data, software, and documentation. Because trade secrecy protections can dampen competition, the Procurement Act's interests in economy and efficiency could straightforwardly justify such a waiver requirement. Similarly, an executive order could also require federal contractors to abide by targeted transparency requirements and to collect, create, and share information when they might otherwise choose not to.[139] Indeed, the affirmative

133. 40 U.S.C. § 121.

134. 40 U.S.C. § 101.

135. Exec. Order No. 11246, 30 Fed. Reg. 12319 (Sept. 28, 1965).

136. Exec. Order No. 13950, 86 Fed. Reg. 7009 (Sept. 21, 2020).

137. Louisiana v. Biden, 55 F.4th 1017, 1039 (5th Cir. 2022) (Graves, J., dissenting).

138. *See* Am. Fed'n of Lab. & Cong. of Indus. Orgs. v. Kahn, 618 F.2d 784, 792 (D.C. Cir. 1979) ("Because there is a sufficiently close nexus between those criteria and the procurement compliance program established by Executive Order 12092, we find that program to be authorized by the FPASA.").

139. Even though the Procurement Act confers broad discretion on the president, such a requirement

action obligations for federal contractors encompass some similar targeted transparency requirements and disclosure obligations in order to permit regulators to evaluate compliance.[140]

Presidential action could have significant knock-on effects in other contexts. Most prominently, if the federal government were to take significant steps to limit trade secrecy assertions in government contracting, it could reduce the obstacles that corporate secrecy poses at the state level, too. If certain data or information were required to be made public at the federal level, vendors would no longer be able to claim that that information is a bona fide trade secret at the state level.[141]

B. Empower Whistleblowers

A second mechanism for reducing excessive secrecy is to empower tech workers to blow the whistle and disclose information of public concern. Whistleblowers are a necessary part of an overall enforcement regime intended to make new forms of governance more transparent and more accountable.[142] As Orly Lobel has observed, whistleblower protections for employees are particularly critical because of the unique vantage point that workers have as organizational insiders.[143] In technology-intensive contexts, whistleblowers are even more important because regulators and lawmakers lack access to crucial data necessary to assess legal compliance and policy issues.[144] And in the context of governance regimes that are increasingly reliant on public-private partnerships, whistleblowing is yet more significant as a potential source of accountability.[145]

---

might nonetheless confront constitutional concerns. *See, e.g.*, Complaint for Declaratory and Injunctive Relief, Nat'l Urban League v. Trump, No. 1:20-cv-03121 (D.D.C. Oct. 29, 2020) (challenging the constitutionality of the "Executive Order on Combating Race and Sex Stereotyping" on First Amendment grounds). Essentially, the argument would be that requiring firms to collect and disseminate this kind of information would compel speech in violation of the First Amendment. *See generally* Amy Kapczynski, *The Public History of Trade Secrets*, 55 UC DAVIS L. REV. 1367 (2022) (discussing the constitutionalization of trade secrecy).

140. For example, Google was selected for a "compliance review" of its pay practices after it was awarded a federal contract in 2014. The Office of Federal Contract Compliance Programs required Google to disclose additional granular data about its practices in order to evaluate potential gender-based pay disparities. *U.S. Labor Department Sues Google for Compensation Data*, REUTERS (Jan. 4, 2017), https://www.reuters.com/article/us-alphabet-lawsuit-idUSKBN14O2D9 [https://perma.cc/Z9RA-UF5A].

141. *See* Deepa Varadarajan, *The Trade Secret-Contract Interface*, 103 IOWA L. REV. 1543, 1551 (2018) ("The plaintiff must have subjected the information to reasonable secrecy precautions . . . preventing its disclosure.").

142. *See* Orly Lobel, *Citizenship, Organizational Citizenship, and the Laws of Overlapping Obligations*, 97 CALIF. L. REV. 433, 441–43 (2009) (explaining whistleblower protections and providing examples of successful whistleblowers); *cf.* Terry Morehead Dworkin, *Sox and Whistleblowing*, 105 MICH. L. REV. 1757 (2007) (arguing that the Sarbanes–Oxley Act has not been effective in facilitating whistleblowing).

143. Lobel, *supra* note 142, at 459.

144. Morten, *supra* note 59, at 53 (describing "huge information asymmetries" confronting regulators); *see also* Morten & Kapczynski, *supra* note 121, at 500–01 (describing how information-intensive economic activity gives rise to broader claims of trade secrecy).

145. Lobel, *supra* note 142, at 473; Katyal, *supra* note 72, at 128–29.

It is no surprise that tech whistleblowing has expanded. Widespread secrecy of the kind embraced by the technology industry, as Part II described, reflects a powerful default rule of corporate control of information. But the norm of secrecy in Silicon Valley has also prompted workers to come forward with information of concern to the public, lawmakers, and regulators.[146]

Current whistleblower laws largely, albeit unevenly, protect workers who disclose waste, fraud, abuse, and legal violations. Some whistleblower protections already extend to private employees working on government contracts or grants. Under federal law, contractors, subcontractors, and grantees are prohibited from retaliating against workers who disclose evidence of any of the following:

> [G]ross mismanagement of a Federal contract or grant, a gross waste of Federal funds, an abuse of authority relating to a Federal contract or grant, a substantial and specific danger to public health or safety, or a violation of law, rule, or regulation related to a Federal contract . . . or grant.[147]

But state whistleblower protections are not uniform.[148]

However, whistleblowing protections often do not extend to ethical harms or legal violations that are perceived to be less serious.[149] For example, a whistleblower is protected for disclosing information they reasonably believe shows a violation of law, even if that information is a protected trade secret.[150] But many of the problems emerging from the new algorithmic governance—for example, fundamental issues of bias, fairness, or accuracy—are not yet regulated by statute. The current absence of law on algorithmic governance leaves a corresponding void for whistleblowers, who are typically not protected when they, for example, alert lawmakers about unethical or unfair technological practices.

Expanding the subject matters entitled to whistleblower protections could enable better governance. Imagine, for example, that a Google engineer

---

146. *See, e.g.*, Ryan Gallagher, *Google Plans to Launch Censored Search Engine in China, Leaked Documents Reveal*, INTERCEPT (Aug. 1, 2018), https://theintercept.com/2018/08/01/google-china-search-engine-censorship/ [https://perma.cc/E9HY-C4M8] (noting that a Google employee came forward with information about a secret project at Google to bring a censored version of the search engine to China); Georgia Wells, Deepa Seetharaman & Jeff Horwitz, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, WALL ST. J. (Sept. 14, 2021), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739 [https://perma.cc/2GGG-B5UL] (discussing knowledge at Facebook and Instagram of the negative effects of the apps on young users, leaked to reporters by an employee); Harry Davies et al., *Uber Broke Laws, Duped Police and Secretly Lobbied Governments, Leak Reveals*, GUARDIAN (July 11, 2022), https://www.theguardian.com/news/2022/jul/10/uber-files-leak-reveals-global-lobbying-campaign [https://perma.cc/B58R-BJZU] (reporting on findings from files leaked from Uber).

147. 41 U.S.C. § 4712(a)(1).

148. *See* JULIA TAYLOR & MELISSA S. SCHEEREN, CONG. RSCH. SERV., MEMORANDUM ON SELECTED STATE STATUTES ON WHISTLEBLOWER PROTECTIONS AND FALSE CLAIMS (2021), https://whistleblower.house.gov/sites/whistleblower.house.gov/files/CRS_Selected_State_Statutes_on_Whistleblower_Protections.pdf [https://perma.cc/Q7WS-SFCA] (surveying whistleblower protections in various states).

149. Katyal, *supra* note 72, at 129.

150. Peter S. Menell, *The Defend Trade Secrets Act Whistleblower Immunity Provision: A Legislative History*, 1 BUS. ENTREPRENEURSHIP & TAX L. REV. 398, 400 (2017).

discovers that the company's Wisconsin unemployment fraud detection algorithm has a flaw: it penalizes individuals who are unable to work full-time because of disability. The result is that claims submitted by disabled individuals are disproportionately denied and flagged as fraudulent. Surely reasonable people would agree that this is a problem. But is it a violation of law? Those who are affected might argue that it is because the denials violate their due process rights.[151] Google, however, might argue that as a private actor, it cannot violate constitutional rights.[152] At least from the perspective of the engineer, the law might appear ambiguous.

A concerned engineer might still be tempted to sound the alarm, but Wisconsin law offers no protections.[153] The engineer might speak out nonetheless, choosing to defy a non-disclosure agreement or corporate policy that prohibits them from disclosing confidential corporate information. By doing so, they run the significant risk that Google might retaliate against them. The prospect of losing their job is likely to cause even the most socially-conscious worker to refrain from blowing the whistle.[154] And by retaliating, Google sends a message to its other workers that deters them from coming forward. Importantly, this chilling effect exists regardless of whether the engineer is ultimately in the right.

Broader whistleblower protections are necessary to keep up with the realities of modern privatized governance and more effectively respond to the ecology of secrecy that shapes the tech sector. In light of growing interest in issues involving bias, inaccuracy, and opacity in artificial intelligence, broader whistleblower protections could help encourage important disclosures on these topics of public concern.[155] Whistleblowers should also be empowered and encouraged to alert authorities about the kinds of data privacy and security harms that are often invisible to outsiders.[156]

Whistleblower protections can take different shapes, ranging from antiretaliation measures for those who choose to report to mandatory reporting obligations to "incentive-based systems" that create bounties.[157] These design questions have important implications for the effectiveness of any whistleblower

151. *See*, *e.g.*, Cahoo v. SAS Analytics Inc., 912 F.3d 887, 899 (6th Cir. 2019) (presenting plaintiffs' due process argument).

152. *See*, *e.g.*, Cahoo v. SAS Inst. Inc., 322 F. Supp. 3d 772, 792 (E.D. Mich. 2018) (discussing the state actor issue).

153. WIS. STAT. § 230.83 (prohibiting retaliation by government employers against public employees).

154. *See* Cynthia L. Estlund, *Free Speech and Due Process in the Workplace*, 71 IND. L.J. 101, 103 (1995) (arguing that free speech protections are not enough to encourage whistleblowing for at-will employees).

155. *See, e.g.*, FED. TRADE COMM'N, COMBATTING ONLINE HARMS THROUGH INNOVATION 56 (June 2022), https://www.ftc.gov/reports/combatting-online-harms-through-innovation [https://perma.cc/97DE-PKVR] (discussing the risks of artificial intelligence and the need for whistleblower protections).

156. Bloch-Wehba, *The Promise and Perils of Tech Whistleblowing*, *supra* note 10, at 50.

157. Yuval Feldman & Orly Lobel, *The Incentives Matrix: The Comparative Effectiveness of Rewards, Liabilities, Duties, and Protections for Reporting Illegality*, 88 TEX. L. REV. 1151, 1153 (2010).

mechanism at incentivizing valuable disclosures and protecting individuals who disclose.[158] Securities laws offer some models: under the Commodity Exchange Act, for example, individuals who report "original information" about violations of the Act to the Commodity Futures Trading Commission Whistleblower Office are guaranteed confidentiality and protected from retaliation.[159] Similarly, individuals who provide information to the Securities and Exchange Commission about violations of the securities laws are also protected.[160] Indeed, in both cases, whistleblowers whose disclosures lead to successful enforcement actions are handsomely rewarded with financial bounties.[161] Here, however, whistleblowers are less likely to come forward with evidence that leads to successful enforcement precisely because the law is so underdeveloped, making enforcement an elusive goal.[162] That makes bounties a less attractive mechanism for whistleblower protection, even if the prospect of financial remuneration would incentivize valuable disclosures.

Firms would undoubtedly be concerned about empowering workers to speak more freely about corporate practices. One potential response is to create fairly narrow channels through which whistleblowers can report unethical practices either internally or to designated authorities.[163] Through statute, Congress could require companies to adopt additional mechanisms for internal whistleblowing, as it did in the Sarbanes Oxley Act ("SOX"). Under SOX, individuals who blow the whistle internally about fraud are protected from retaliation.[164] In addition, SOX requires firms to establish independent audit committees that have formal channels for receiving complaints about, among other things, "questionable" accounting matters.[165]

Internal mechanisms for reporting, however, are also likely to be of limited effectiveness.[166] Most notably, the tech sector's culture of secrecy makes the social costs of blowing the whistle significant, even if anti-retaliation provisions exist.[167]

158. *Id.*; Anthony J. Casey & Anthony Niblett, *Noise Reduction: The Screening Value of Qui Tam*, 91 WASH. U. L. REV. 1169, 1173 (2014); David Freeman Engstrom, *Private Enforcement's Pathways: Lessons from Qui Tam Litigation*, 114 COLUM. L. REV. 1913, 1918 (2014); Geoffrey Christopher Rapp, *Mutiny by the Bounties? The Attempt to Reform Wall Street by the New Whistleblower Provisions of the Dodd-Frank Act*, 2012 BYU L. REV. 73, 75–76 (2012).

159. 7 U.S.C. § 26(h)(1)–(2).

160. 15 U.S.C. § 78u-6(h).

161. U.S. Securities and Exchange Comm'n, *SEC Awards More Than $20 Million to Whistleblower* (Dec. 12, 2022), https://www.sec.gov/news/press-release/2022-218 [https://perma.cc/J7KW-JAWP].

162. Bloch-Wehba, *The Promise and Perils of Tech Whistleblowing*, *supra* note 10.

163. *Cf.* Lobel, *supra* note 142, at 445 (distinguishing between internal and external channels).

164. 18 U.S.C. § 1514A(a)(1)(C) (protecting individuals who blow the whistle to people with "supervisory authority").

165. 15 U.S.C. § 78j-1(m)(4)(B).

166. Dworkin, *supra* note 142, at 1771–72; Miriam A. Cherry, *Whistling in the Dark? Corporate Fraud, Whistleblowers, and the Implications of the Sarbanes-Oxley Act for Employment Law*, 79 WASH. L. REV. 1029, 1070 (2004) (identifying reasons that SOX whistleblower protections have been less effective than might have been anticipated); ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 240–41 (2021) (comparing SOX whistleblower channels).

167. *See* Erin Woo, *A Tech Whistle-Blower Helps Others Speak Out*, N.Y. TIMES (Nov. 24, 2021),

It is easy to imagine that individuals who blow the whistle internally will be penalized by their managers and their peers. Particularly given the likelihood that whistleblowers will be ostracized, a whistleblower provision must include protections for anonymity to ensure that those who risk disclosing information do not face economic and social ruin.[168]

The most difficult question about whistleblower protections, then, is identifying an appropriate external institution to receive whistleblower reports. One option is for each agency to broaden the scope of the Office of Inspector General to include receiving whistleblower complaints about ethical questions that arise within their contractors. For example, if an Amazon employee working on a contract for the Federal Bureau of Investigation has an ethical concern about, say, bias in the company's facial recognition system, they could report it to the independent inspector general within the Department of Justice. Because inspectors general already receive whistleblower reports regarding waste, fraud, abuse, and legal violations, they are not a wholly inappropriate entity to receive additional complaints.[169] At the state level, state attorneys general—who play a critical role in enforcing state privacy and unfair competition laws—could also establish offices to receive these complaints.

Another option is to develop an entity that is specifically tasked with receiving tech ethics complaints. The National Institute of Standards and Technology ("NIST"), the Federal Trade Commission ("FTC"), or another expert agency could play an important role here as a trusted intermediary. As the FTC has become the leading regulator of artificial intelligence, privacy, and security, it may be better suited as a recipient of whistleblower complaints than NIST.[170] Indeed, as legislators seek to embolden the FTC to more directly regulate the tech industry, the need for the FTC to address pervasive information asymmetries impeding regulation is crucial.[171] To date, however, lawmakers have largely focused on the kinds of information that firms should be required to maintain, collect, and disclose. Whistleblower complaints are distinct: unlike the disclosure-focused paradigm, whistleblowers tell regulators what firms would

https://www.nytimes.com/2021/11/24/technology/pinterest-whistle-blower-ifeoma-ozoma.html [https://perma.cc/3CYV-78JW] (discussing efforts taken to encourage whistleblowing despite the prevalence of non-disclosure agreements in the tech industry).

168. Janet P. Near & Marcia P. Miceli, *Effective Whistle-Blowing*, 20 ACAD. MGMT. REV. 679, 692 (1995).

169. *See*, *e.g.*, 41 U.S.C. § 4712(a)(2)(B) (protecting workers who disclose wrongdoing to inspectors general from retaliation).

170. *See, e.g.*, Andrew Selbst & Solon Barocas, *Unfair Artificial Intelligence: How TC Intervention Can Overcome The Limitations of Discrimination Law*, 171 U. PA. L. REV., (forthcoming 2023) (manuscript at 3–5) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4185227 [https://perma.cc/F63Q-AUGC]).

171. *See, e.g.*, Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. § 3(b) (2022) (requiring the FTC to promulgate regulations requiring private entities to conduct algorithmic impact assessments and produce summary reports about the assessment of automated decision systems); Platform Accountability and Consumer Transparency Act, S. 797, 117th Cong. § 5(g) (2021) (providing that violations of the Act's transparency provisions "shall be treated as" violations of the FTC Act's prohibition on unfair and deceptive trade practices).

prefer that regulators *not* hear.

At bottom, whistleblower protections are not a complete answer to the problem of pervasive corporate secrecy—no single solution is. But unauthorized disclosures of information by corporate insiders are a critical source of information about what could be going wrong. As in many other regulatory contexts that involve profound information asymmetry—fraud, insider trading, taxation, and health and safety, to name a few—inside information is particularly important for law enforcement and policymaking in the technology space. Rather than focusing exclusively on how firms should be encouraged to share additional information, we should also incentivize and protect disclosure by individuals who offer competing information that might undermine corporate narratives.

C. Develop a Public Option

The two previous proposals offer reformist approaches to significantly publicize the provision of services, products, and infrastructure by private technology firms. This proposal considers a different path: direct provision by the state itself. It contemplates the government creation of a public option to compete with private vendors.

An underlying theory supporting privatization is that government works better when it is made competitive; where the government's competitors more efficiently or cheaply provide the' public services, the state should buy those services rather than providing them itself.[172] In some respects, the federal government is best positioned to compete with the private sector, especially where private vendors are leveraging government data to help government actors render decisions about government benefits. But it routinely contracts out to private vendors instead of insourcing at the cost of public values.

There are at least two basic related reasons to consider insourcing the informational infrastructure, automated decision systems, and artificial intelligence models that are increasingly transforming governance. First, outsourcing the government's technological infrastructure threatens to undermine core values of public-ness. Second, continued outsourcing erodes the government's technological competence and reinforces persistent narratives of private sector dominance.

Federal procurement law forbids the government from contracting out its performance of "inherently governmental functions."[173] Under the Federal Activities Inventory Reform Act of 1998, an activity is inherently governmental if it is "so intimately related to the public interest as to require performance by Federal Government employees."[174] In 2011, the Office of Management & Budget ("OMB") clarified the definition of "inherently governmental" in a

172. *See* Short, *supra* note 28, at 12 (explaining the "make-or-buy" decision).

173. Off. of Mgmt. & Budget, Circular No. A-76, Performance of Commercial Activities § 5(b) (Aug. 4, 1983, revised 1999).

174. Federal Activities Inventory Reform Act of 1998, Pub. L. 105-270, § 5(2), 112 Stat. 2382, 2384–85.

policy letter.[175] Under the policy letter, "inherently governmental" was defined to include activities requiring "the exercise of discretion in applying Federal Government authority or the making of value judgments in making decisions."[176] "Inherently governmental" also includes the "interpretation and execution" of laws that "significantly affect the life, liberty, or property of private persons."[177]

Outsourcing even non-inherently governmental functions, however, might have broader implications for government effectiveness, competency, and oversight capacity.[178] The policy letter also identified a second group of "critical functions," which are "necessary to the agency being able to effectively perform and maintain control of its mission and operations."[179] OMB warned that agencies must sufficiently staff their "critical functions" to ensure that Federal employees, not contract workers, can "provide for the accomplishment of, and maintain control over, their mission and operations."[180] In addition, OMB reminded agencies that some activities were so "closely associated with inherently governmental functions" that contracting out might "impinge on Federal officials' performance" of their work.[181]

At the same time, a basic tenet of federal procurement policy is the preference to acquire commercial products and services where available.[182] This principle is longstanding, going back to 1955 when a Bureau of the Budget bulletin established the government's position that it ought not compete with the private sector's provision of commercial products or services.[183] Today, the preference for commercial products and services is set forth in OMB Circular A-76.[184] Circular A-76 also sets out a process by which public agencies must compete with the private sector to ensure cost savings.[185] Circular A-76 thus incorporates two potentially competing policy goals: a preference for the private sector on the one hand and a preference for competition between government and the private sector on the other.[186]

Federal law tries to draw a bright line between "inherently governmental

175. *See generally* Publication of the Office of Federal Procurement Policy (OFPP) Policy Letter No. 11-01, Performance of Inherently Governmental and Critical Functions, 76 Fed. Reg. 56227, 56236 (Sept. 12, 2011) (explaining activities falling under inherently governmental functions).

176. *Id.*

177. *Id.*

178. Dan Guttman, *Governance by Contract: Constitutional Visions; Time for Reflection and Choice*, 33 PUB. CONT. L.J. 321, 340 (2004).

179. Policy Letter No. 11-01, 76 Fed. Reg. at 56236.

180. *Id.* at 56237.

181. *Id.*

182. 48 CFR § 1.102(b)(i) (2021) (setting forth a plan to "maximiz[e] the use of commercial products and commercial services").

183. Exec. Off. of Pres., Bulletin No. 55-4, Commercial Industrial Activities of the Government Providing Products or Services for Governmental Use (Jan. 15, 1955).

184. OFF. OF MGMT. & BUDGET, Circular No. A-76, § 5(b) (Aug. 4, 1983, revised 1999).

185. *Id.* § 4(c) (Aug. 4, 1983, revised 2003).

186. Steven L. Schooner, *Competitive Sourcing Policy: More Sail Than Rudder?*, 33 PUB. CONT. L.J. 263, 271 (2004)

functions," which must be performed by government workers and cannot be contracted out, and "commercial products and services," which must be competitively sourced. Novel technologies of governance, however, make application of the "inherently governmental function" test exceedingly difficult. For example, OMB's policy letter identifies the following as paradigmatic "inherently governmental functions": "the direct conduct of criminal investigation," "security that entails augmenting or reinforcing others . . . in combat," and "the direction and control of Federal employees."[187]

New technologies of governance blur the kinds of boundaries that procurement law relies upon. Even where new technologies of governance are not used to perform "inherently governmental functions," they might be so closely related to those functions that contracting out might undermine Federal employees' control over their operations. For example, one might ask whether Anduril's artificial intelligence defense system, Lattice, runs afoul of this definition. As Anduril markets Lattice, it is an operating system that "autonomously parses data from thousands of sensors and data sources."[188] Lattice utilizes learning models to present decision support.[189] Does it therefore provide security to augment those in combat? Do its recommended decisions direct Federal employees? Similar questions also apply to many other investigative technologies that focus on data analysis as well as those that drive and inform criminal law enforcement.[190] As Deirdre Mulligan and Kenneth Bamberger have put it, the cost-oriented approach of procurement law is a poor fit when the "design, adoption, and use" of a technical system "make substantive policy."[191] To date, however, the provision of the state's informational infrastructure has not been understood as closely associated with an inherently governmental function.

The more that informationally-intensive governance regimes rely on privately provided infrastructure, the harder it becomes to distinguish a "commercial product" from the "governmental function" it supports. The advent of artificial intelligence, big data, and related decision-making methodologies should prompt us to reconsider whether the distinctions that procurement law draws between "commercial" and "governmental" can be sustained.

At a minimum, the use of technology in service of state decision-making about life, liberty, and property should be considered an inherently governmental

187. Publication of the Office of Federal Procurement Policy (OFPP) Policy Letter No. 11-01, Performance of Inherently Governmental and Critical Functions, 76 Fed. Reg. 56227, 56240 (Sept. 12, 2011).

188. ANDURIL, LATTICE OS, https://www.anduril.com/lattice/ [https://perma.cc/HDY5-ER8G] (last visited Apr. 3, 2023).

189. *See generally id.* (providing information through an operating system to assist in decision making).

190. *See, e.g.*, Complaint at ¶¶ 14–15, Elec. Privacy Info. Ctr. v. U.S. Immigr. & Customs Enf't, No. 1:17-cv-02684 (D.D.C. Dec. 15, 2017) (discussing how Palantir's data analytics software raises profound questions about compliance with statutory privacy protections).

191. Mulligan & Bamberger, *supra* note 93, at 780.

function. Under this definition, the use of an algorithm to allocate public benefits, computer vision to identify potential targets for military force, or facial recognition for criminal law enforcement purposes should be considered an inherently governmental function. Critics will charge that broadening the definition of "inherently governmental" will create monumental strain and that, by requiring insourcing of all these technologies, this proposal will create high costs for taxpayers and bureaucrats alike. At the same time, requiring insourcing can create meaningful incentives to rebuild the technical competence of a hollowed-out state. To date, models like the Presidential Innovation Fellowship and 18F, discussed above, have served as important engines of innovation within the federal government. A decision to emphasize and invest in insourcing would empower those offices and require them to staff up significantly. And federal investment in insourced data analytics, decision-making, and artificial intelligence tools could benefit states, too, that might adopt these tools even in the absence of a mandate to do so.

By the same token, however, regulation of an information-intensive economy is likely to require strategic partnerships between the public and private sectors, calling into question whether the existing distinctions between "commercial" and "governmental" continue to hold water. Instead, emerging public-private partnerships embrace "commercial" technologies for governance without the accountability and transparency requirements that apply to "governmental functions." Consider the following example: During the coronavirus crisis that overwhelmed the United States in the spring of 2020, Americans attempted to file for unemployment benefits in unprecedented numbers, resulting in a backlog of millions and massive delays.[192] In Wisconsin, over ninety percent of the millions of calls to the state agency overseeing unemployment benefits went unanswered.[193] In October 2020, the state of Wisconsin turned to Google, paying the company $1 million to use its Cloud analytics platform to process jobless claims that human workers had struggled to keep up with.[194] Without Google's intervention, the thinking went, Wisconsin would never have been able to dig out of the backlog it had fallen into.

The evident need to harness private innovation for public governance shows the limitations of the existing procurement-focused strategy. The existing framework encourages the state to procure "commercial" tools for governance

192. Tony Romm & Heather Long, *Out of Work — and Cash — Millions of Americans Are Still Waiting for Their First Unemployment Check*, WASH. POST (Apr. 23, 2020), https://www.washingtonpost.com/business/2020/04/23/unemployment-benefits-backlog-coronavirus/ [https://perma.cc/B5GR-U5K6].

193. Molly Beck, *Less than 1% of Calls to State Unemployment Call Centers Were Answered, Audit Shows*, MILWAUKEE J. SENTINEL (Sep. 25, 2020), https://www.jsonline.com/story/news/politics/2020/09/25/less-than-1-calls-unemployment-call-centers-were-answered/3529690001/ [https://perma.cc/XNF7-4MRQ].

194. Laura Schulte, *Wisconsin Unemployment Department Says Adjudication of Claims Will Be Sped up Thanks to New Partnership with Google Cloud*, MILWAUKEE J. SENTINEL (Oct. 19, 2020), https://www.jsonline.com/story/news/2020/10/19/wisconsin-unemployment-adjudication-getting-help-google-cloud/5981380002/ [https://perma.cc/QZV3-XKPX].

where possible, without regard for other public values that might be traded off. But acknowledging that these tools play a crucial role in public governance suggests that a different approach is necessary to secure the benefits of privately developed technology without compromising the integrity of democratic institutions.

That crisis might create needs and opportunities for public-private partnership is not a new idea. Indeed, the contemporary relationship between government and the technology industry has its origins in the 1940s, when wartime needs created a "sea-change in the relationship between science and government in the United States."[195] The Office of Scientific Research and Development ("OSRD") leveraged relationships between industry, academia, and government for wartime research in both defense and medical research.[196] But critics also charged that the partnership between government and science was a "grab by which a small company of scientists and engineers . . . got hold of the authority and money for the program of developing new weapons."[197]

No coordinated policy of the kind exemplified by OSRD governs today's partnerships between the technology sector and the state. Indeed, the wartime patriotism that pressed industry and academia into service is largely gone, replaced by the goal of maximizing shareholder value.[198] However, similar concerns about anti-competitiveness in government contracting remain. New regulatory instrumentalities to meet the needs of a changing technological and economic landscape require this level of coordination.[199]

A new OSRD—let's call it OSRD v.2.0—could facilitate this kind of cooperation. A coordinated office for the federal government's development of new technology could help incentivize the nation's tech companies and universities to enter into contracts to build prototypes and custom software for the federal government.[200] A coordinated office would need to have sufficient technical expertise to be able to oversee both the acquisition process and the development process. Crucially, it would also need to abandon the preference for "commercial" products and off-the-shelf software in favor of custom solutions developed for government ends.[201]

A centralized strategy for the development of government technology could

195. Larry Owens, *The Counterproductive Management of Science in the Second World War: Vannevar Bush and the Office of Scientific Research and Development*, 68 BUS. HIST. REV. 515, 516 (1994).

196. DON KRASHER PRICE, GOVERNMENT AND SCIENCE: THEIR DYNAMIC RELATION IN AMERICAN DEMOCRACY 44–47 (1954); STEPHEN KLEPPER, EXPERIMENTAL CAPITALISM: THE NANOECONOMICS OF AMERICAN HIGH-TECH INDUSTRIES 154–55 (2016).

197. Owens, *supra* note 195 at 523.

198. Price, *supra* note 196 at 46. *See generally* RACHEL WEBER, SWORDS INTO DOW SHARES: GOVERNING THE DECLINE OF THE MILITARY-INDUSTRIAL COMPLEX (2001) (analyzing the conflicts between shareholder capitalism and the public interest in the context of the defense industry).

199. Cohen, *supra* note 60, at 200.

200. Under the federal laws governing defense procurement, a specific set of rules applies to prototype contracts. I'm not suggesting that those rules ought to apply here.

201. 48 CFR § 1.102(b) (2021).

better optimize for transparency and accountability values. By funding the development of new technology at government expense, the government would retain rights to the technology (known in the defense contracting space as "technical data rights") that would facilitate both disclosure and reuse by other entities.[202] The retention of rights could help to alleviate the pervasive secrecy claims that have characterized the use of new technologies of governance to date, as discussed above. A coordinated strategy for developing government technology can also create efficiencies for validation, audit, risk assessment, and other crucial oversight mechanisms.

Coordination is necessary to enlist the nation's firms in creating new technologies of governance oriented around public, not private, values. In short, these are *public* options—alternatives to the dominance of privately developed, privately funded technologies that lack democratic oversight and safeguards. A public option is a "government provided social good that exists alongside a similar, privately provided good."[203] Public options famously exist in healthcare and housing finance.[204] They should also exist in government technology. Creating them would have radical ripple effects not only within the federal government but also within state and local jurisdictions that lack the technical capacity and competence to develop their own purpose-built technological tools.

In some settings, the infrastructure for developing a public option may already exist. Most obviously, the federal government already possesses massive troves of data, and as Bridget Fahey notes, intergovernmental data exchange is already prolific and extensive. In the context of unemployment specifically, she notes that the National Directory of New Hires ("NDNH") "contains information on almost all American employees" and is "used to verify eligibility for a suite of public benefits programs whose benefits are conditioned on employment."[205] Presumably, then, the NDNH may also contain extensive information relevant to benefits conditioned on *unemployment.*

One can easily imagine that the federal government might fruitfully leverage existing troves of data to build a public "hub."[206] Doing so might, similarly, facilitate the development of an automated decision tool to assist in assessing eligibility, built on this public data and engineered for maximal transparency. For

202. 48 CFR § 252.227-7013 (2021).

203. Anne Alstott & Ganesh Sitaraman, *Introduction*, *in* POLITICS, POLICY, AND PUBLIC OPTIONS 1 (Anne Alstott & Ganesh Sitaraman eds., 2021).

204. *See* Jacob S. Hacker, *Between the Waves: Building Power for a Public Option*, 46 J. HEALTH POL. POL'Y & L. 535, 536 (Aug. 2021) (explaining public options for healthcare); *see* Adam J. Levitin & Susan M. Wachter, *The Public Option in Housing Finance*, 46 U.C. DAVIS L. REV. 1111, 1115 (2013) (explaining public options for housing finance).

205. Bridget A. Fahey, *Data Federalism*, 135 HARV. L. REV. 1007, 1021–22 (2022).

206. An example of this kind of cooperation is the Centers for Medicare & Medicaid Services Data Services Hub, which was created pursuant to the Affordable Care Act to bring together data from across disparate domains in order to allow states to assess eligibility for enrollment in health care coverage. Rather than outsourcing the eligibility assessments to private actors, CMS and IRS built the hub themselves (though certain maintenance tasks for the hub have been outsourced). I am grateful to Jason Schultz for this example.

example, a federal agency might consult with states to understand how they assess eligibility and then build an automated decision tool that is capable of considering all the relevant criteria identified by states. Each state might thus implement a version of the public tool with the criteria that it chooses to use. That tool can then be independently validated on each relevant population for predictive accuracy and assessed for disparate impact and other distributive harms.[1] It can be routinely and repeatedly audited by state officials. A public option can thus compete with private options on cost, and therefore on accessibility, but it might also compete on transparency, accountability, and democratic values.

Still, there are obstacles. Concerns about privacy and surveillance may, and in some cases should, discourage government information-sharing between and within agencies.[207] Growing hostility to the administrative state and efforts to hollow it out may further deter agencies from pursuing in-house development. And even public algorithmic governance can suffer from serious accountability and transparency flaws. Consider MiDAS, the Michigan unemployment system, which was publicly operated, albeit developed by a private firm, and falsely accused thousands of people of unemployment fraud, with devastating effects.[208]

Ultimately, however, there are significant benefits of retaining these functions within government that may outweigh the potential drawbacks. Private alternatives are also ultimately subject to the same concerns about privacy and surveillance, even though they are subject to fewer public accountability constraints. Algorithmic governance operated by public agencies is a better fit with current transparency and accountability frameworks, even if it is not perfect.

V

CONCLUSION

For almost four decades, the United States has been reinventing government to operate more like a business. Amid broad shifts toward a digital economy, it is no surprise that the drive to reinvent government today draws on the desire to make it look more like a *tech* business. But in the effort to modernize, the state is relying on private partners to the detriment of public values. In no small part, our frameworks for acquiring new technologies of governance reinforce this predicament by ensuring that the government prefers commercial vendors to publicly developed solutions.

Existing frameworks for incentivizing, encouraging, and constraining the provision of services to government actors have largely failed to keep pace with technological change. Technology vendors reap financial benefits from their close relationships with state actors while shirking democratic obligations like transparency and accountability. Yet divesting from partnerships with the private sector is not sufficient, let alone realistic, as an answer to these problems.

207. Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 72 VAND. L. REV. 1563, 1572 (2019).

208. Crawford & Schultz, *supra* note 1.

Instead, the very real need to empower the regulatory state to govern an informationally-intensive economy requires new ways of enlisting private enterprise for social good. As Ben Green put it in his study of smart cities, "governments eager to take advantage of new technologies must act as responsible gatekeepers and public stewards in structuring their technology to protect equity and fundamental rights."[209] Doing so requires reassessing the functions that technology is performing in governance and those that we *want* it to perform. Most of all, it requires a disciplined, coordinated, and concerted effort to use public dollars for public good rather than private gain.

209. BEN GREEN, THE SMART ENOUGH CITY 92 (2019).