Preliminary Concept Paper

Legitimacy and Accountability in the Information-Era Administrative State

REDESIGNING THE GOVERNANCE STACK
GEORGETOWN LAW

Preliminary Concept Paper

Legitimacy and Accountability in the Information-Era Administrative State

MAY 5, 2026

Julie E. Cohen
Nina-Simone Edwards
Meg Leta Jones
Paul Ohm

Co-Signers:[1]
Kiel Brennan-Marquez
Andrew Selbst
Jennifer Selin
Bijal Shah
Jodi Short
Salome Viljoen
Daniel Walters

---

1 The ideas in this concept paper were developed in part through workshops held with academics and regulators. Some of the attendees have decided, as well, to co-sign the paper. Although not every one of the co-signers agrees with every idea set forth below, each supports the proposals overall. In addition to the co-signers, we would like to thank Hilary Allen, Elettra Bietti, Bill Buzbee, Chris Havasy, Matthew Lawrence, Laura Moy, Deirdre Mulligan, Blake Reid, Noah Rosenblum, Alan Rozenshtein, Alicia Solow-Niederman, and Michael Veale for their participation in the academic workshop and their constructive and generous feedback. This work was developed with the support of the Tech & Public Policy program at the McCourt School of Public Policy at Georgetown University, the Ford Foundation, and the Economic Security Project.

Executive Summary

This report is part of a broader project to redefine the administrative state's role in effective governance. It considers mechanisms and arrangements for constraining and overseeing administrative action.

We begin by canvassing a number of significant threats to administrative legitimacy and accountability. In brief, the current assault on administrative institutions and the rapid influx of automated "solutions" have exacerbated the problems of a system that was already buckling under the strains of functional opacity, technical opacity, unequal access and influence, process proliferation and paralysis, and inaction.

An overarching reason for the legitimacy and accountability challenges confronting the administrative state is a paradigm for administrative legitimacy and accountability that is court-centered and no longer fit for purpose. We describe two core requirements of legitimacy and accountability–which, as we will explain, are interdependent concepts–and then articulate three component requirements–transparency and demystification, care and respect, and oversight–that are designed to give those concepts more concrete and specific meaning.

Next, we present recommendations for operationalizing the criteria of legitimacy and accountability and the component requirements of transparency and demystification, care and respect, and oversight across the domains of policy-making, enforcement, citizen-focused decision-making, and government technology and data.

Finally, to help implement those recommendations, we recommend creating two new offices with cross-cutting authority: a government information commission to ensure better and more consistent accountability and an Office of Government Integrity to oversee uses–and detect and disclose misuses and abuses–of government technical systems and data. In addition, we recommend revised and streamlined processes for hiring into agency civil service positions.

Introduction

This report is part of a broader project to redefine the administrative state's role in effective governance. It builds on earlier reports that have focused on regulatory monitoring of information-economy activities, provisioning digital tools and systems for government use, designing nimble and dynamic policymaking mechanisms, fostering meaningful public participation in administrative governance, and leveraging new tools to enhance administrative enforcement capabilities. As we detailed in those documents, the administrative state–an industrial-era artifact whose foundational texts and institutional structures are nearly a century old–is struggling with the complex and emergent challenges posed by the information economy. Fundamental reconceptualization and redesign–reaching all the way down to those century-old foundations–is urgently needed. The report, like the others listed above, is undertaken in that spirit.

Here, we turn our attention to mechanisms and arrangements for constraining and overseeing administrative action. Legitimacy and accountability standards for the administrative state have been hotly debated for decades, and we return to the question of definitions below. At minimum, for the administrative state to be legitimate and accountable, it must: Make its own operations sufficiently transparent; afford all citizens fair treatment and equal access to administrative policymakers and processes; act in ways consistent with its prescribed public mandates; and use public resources effectively in ways that produce results and avoid process paralysis.

As we summarize in Part 1, administrative processes often have fallen short of these aspirations for a variety of reasons. Although networked digital technologies have exacerbated the legitimacy and accountability deficits, many problems predate the emergence of the networked information economy. The opacity of administrative processes and discourses has presented challenges for many decades. Additionally, traditional administrative frameworks often leave agencies both too constrained and under-equipped: too procedurally rigid to respond to fast-moving digital challenges and too vulnerable to influence by powerful economic and political actors.

As Part 2 explains, one reason for the legitimacy and accountability challenges confronting the administrative state is a paradigm for administrative legitimacy and accountability that is court-centered and no longer fit for purpose. Governing at scale in a sophisticated, information-driven economy requires an administrative state with powerful, information-driven capabilities of its own; this, in turn, requires a legitimacy and accountability framework developed with the needs and failure modes of administrative institutions in mind. Part 2 describes core elements of that framework.

Part 3 presents recommendations for operationalizing the legitimacy and accountability framework described in Part 2 across the domains of policymaking, enforcement, citizen-focused decision-making, and government technology and data. Part 4 recommends three sets of cross-cutting institutional changes designed to help implement and oversee operation of the new mechanisms: a government information commission, revised and streamlined processes for hiring into agency civil service positions, and an Office of Government Integrity to oversee uses–and detect and disclose misuses and abuses–of government technical systems and data.

As we have done in previous reports, we wish to emphasize a few preliminary points. Overall, our goal is to equip government agencies with the frameworks and capabilities necessary to govern the information economy in a manner that supports appropriately scoped delegations of power while enabling meaningful democratic control. At this stage, we are less concerned with how that might affect operational costs or how these proposals might be challenged under current law. To the contrary, to the extent that provisions of current law are inconsistent with the proposals we advance here, we think it is current law that needs to change. Second, we focus here on sketching a legitimacy and accountability framework for the domains of economic and social welfare regulation. As we have previously observed, very different oversight, due process, and rule-of-law considerations attach to law enforcement and border control activities, and we do not intend any recommendations about those activities.

Part 1: Threats to Legitimacy and Accountability

In an age in which "deep state" conspiracy theories flourish alongside overheated rhetoric about bureaucratic overreach and dire warnings about the inevitably dystopian implications of government automation, it is important to underscore that many of the most significant threats to administrative legitimacy and accountability have older and far more basic causes, which we summarize below. In brief, the assault on administrative institutions and the rapid influx of automated "solutions" have exacerbated the problems of a system that was already buckling under the strains of functional opacity, technical opacity, unequal access and influence, process proliferation and paralysis, and inaction.

Functional Opacity

Networked digital technologies have been a mixed blessing for government openness and accountability. On one hand, federal agencies can and do maintain extensive, public-facing websites to provide information to the public. A wide range of interactions with those agencies, from requesting benefits to filing taxes to submitting Freedom of Information Act (FOIA) requests, can be conducted online. On the other hand, the profusion of online information available at federal agency websites can be bewildering. Both specific pieces of information and more comprehensive data about government operations can be hard to find. Although some administrations in recent years have worked to release certain kinds of government datasets to the public, not all have done so.

Open release of designated government datasets, however, is not the same thing as open government.[2] Statutorily required Federal Register disclosures about administrative operations–such as those accompanying a proposed rulemaking or notifying citizens about a proposed collection or use of their personal information as required by the Privacy Act–can be simultaneously hyper-technical and blandly formulaic. Many other kinds of information about the workings of policymaking and enforcement processes are much harder to obtain. The FOIA was intended to function as guarantor of government transparency to the public, but it no longer serves that purpose effectively.[3] And the idea that individual requesters of information can and should serve as the primary engines of government transparency to the public has enabled policymakers to avoid systematic thinking about other, more proactive ways for federal agencies to disclose meaningful information about their operations.

More generally, ordinary citizens often struggle to understand how the administrative state performs its various functions.[4] It is worth noting that the classic "Schoolhouse Rock" video about how bills "become law" omits the administrative state altogether–arguably encouraging magical thinking about what must be done to ensure that priorities set by Congress "become law" in any effective sense–and that K-12 civics curriculum materials on the executive branch focus mainly on the President's constitutional powers and provide very little detail on administrative policymaking and enforcement.

2 Harlan Yu & David G. Robinson, *The New Ambiguity of Open Government*, 59 UCLA L. Rev. Discourse 178 (2011).

3 Margaret Kwoka, Saving the Freedom of Information Act (2021).

4 Gabriel Scheffler & Daniel E. Walters, *The Submerged Administrative State*, 2024 Wisc. L. Rev. 789 (2024).

Technical Opacity

Other kinds of opacity surrounding administrative processes and operations are technical.

Two of these long pre-date the advent of data driven automated technologies and systems. One is the inherently technical nature of many expert discourses on which regulators need to rely. As discussed in our report on "Mechanisms for Including Publics in Administrative Governance," such discourses are relatively inaccessible to many of those with important interests at stake, and exclusive reliance on technical expertise also crowds out the other kinds of knowledge that affected publics possess.

A second longstanding source of technical opacity in administration is deliberate secrecy. In theory, at least, the Administrative Procedure Act's notice requirements together with open-government statutes such as FOIA and the Government in the Sunshine Act make administrative concealment difficult. Yet, as we discuss in our report on "Regulatory Monitoring in the Information Economy," regulated entities work hard to keep many aspects of their own operations secret, and FOIA's trade secrecy exception continues to shelter such information even after it has been provided to regulators. That exception also shelters technical information about digital tools and services that agencies procure from private vendors.

As automated decisionmaking technologies proliferate within the administrative state–a process that is already underway–their adoption and use threatens to magnify both preexisting kinds of technical opacity while adding a third.[5] As discussed at some length in our report on "Provisioning Digital Tools and Systems for Government Use," data driven machine learning processes operate in inherently opaque ways, producing results that can be difficult or even impossible to explain in cause-and-effect terms. This problem can be expected to worsen, at least in the short run, to the extent that agencies begin to incorporate apps developed using mass-marketed large language model capabilities into their workflows.

Unequal Access and Influence

Although administrative processes are formally insulated from some kinds of secretive private influence, patterns of access and influence in the modern administrative state remain starkly unequal.[6] To begin with, powerful economic actors find information overload less overwhelming and technical opacity less intimidating. They can and do hire lawyers, technical subject matter experts, and public relations teams; therefore, they are relatively unhindered by the problems we discuss in the two sections above.

Powerful economic actors also enjoy other special kinds of influence over the results of policymaking and enforcement processes. So, for example, as we discuss in our reports on policy-making and inclusion, during public-facing processes such as rulemakings or requests for information, such actors now routinely mount astroturf campaigns, flooding the zone with comments supportive of their preferred position. They also donate to nonprofit advocacy groups as a way of generating other favorable, seemingly independent interventions.[7] They are relatively well-equipped to weigh in during the more informal processes through which agencies formulate guidances

5 On administrative uptake of automated digital systems, see Cary Coglianese, A Framework for Governmental Use of Machine Learning, Report for the Administrative Conference of the United States (Dec. 2020);David Freeman Engstrom, Daniel E. Ho, Catherine M. Sharkey & Mariano-Florentino Cuéllar, Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies, Report for the Administrative Conference of the United States (Feb. 2020). On the three kinds of opacity in automated systems, see Jenna Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, 3 Big Data & Soc'y 1 (2016).

6 Existing laws intended to prevent or limit secretive private influence include the Government in the Sunshine Act, 5 U.S.C. § 552b (2006), and the Lobbying Disclosure Act of 1995, 2 U.S.C. § 1601 *et seq.*

7 Marianne Bertrand et al., *Hall of Mirrors*, 136 Q. J. Econ. 2413, 2417-2419 (2021).

and other communications and to participate in the working groups that some agencies use to consult stakeholders on best practices and standards.[8] Their ability to hire experts, convene panels and conferences, and curate other public presentations of their views can enable them to effect intellectual capture of the discussions both around particular regulatory questions and on questions of administrative authority more generally. And, as we discuss in our report on "Rebooting Administrative Enforcement for the Information Economy," they have become expert at negotiating consent decrees that do not require them to admit wrongdoing or impose other meaningful sanctions.

Last but not least, additionally, in an era when government is increasingly dependent upon information-based tools and resources provisioned by private actors, those actors may gain new kinds of pervasive access to government officials and processes.[9] As digital tools and services are developed, configured, reconfigured, and updated, their providers also may gain a partial measure of control over what government agencies see, pervasively shaping the ways they approach the matters they have been charged to handle.[10]

Process Proliferation and Paralysis

Although adequate and fair process is an essential component of legitimacy and accountability, process proliferation and paralysis can cause the administrative state to lose legitimacy and hinder it from fulfilling its public mandates. Most obviously, process proliferation raises the costs of agency action and creates delays; it also discourages agencies from taking the risks that may be necessary to act effectively.[11]

For our purposes here, two kinds of process proliferation are especially worrisome. In policymaking contexts, layering in process requirements–even when such requirements are intended to broaden opportunities for public participation or public access to information–can have the effect of conferring additional advantages on already well-resourced actors.[12] When additional process stages are paired with additional opportunities to seek judicial review, already lengthy proceedings may drag on for years without resolution, and policymakers may spend too much time looking for ways to harden the record against appeals.[13] In contexts involving decisions about access to government services and benefits, process proliferation can prevent individual citizens from obtaining timely access to needed assistance, creating frustration and hardship that colors citizens' interactions with and opinions about government more generally.

Inaction in the Face of Persistent Harms and Threats

Last but not least, failure to act can be a powerful delegitimizing force. Administrative actors lose legitimacy when they fail to respond to experienced harms–for example, discriminatory algorithmic decisionmaking that harms consumers, employees, or prospective tenants and predatory design and pricing practices designed to

8 Wendy Wagner et al., *Deliberative Rulemaking: An Empirical Study of Participation in Three Agency Programs*, 73 Admin. L. Rev. 609, 626-35 (2021).

9 Wendy E. Wagner, *Administrative Law, Filter Failure, and Information Capture*, 59 Duke L.J. 1321 (2010).

10 Deirdre K. Mulligan & Kenneth A. Bamberger, *Procurement as Policy: Administrative Process for Machine Learning*, 34 Berkeley Tech. L. J. 773 (2019).

11 Nicholas Bagley, *The Procedure Fetish*, 118 Mich. L. Rev. 345 (2019).

12 Karen E.C. Levy & David Merritt Johns, *When Open Data is a Trojan Horse: The Weaponization of Transparency in Science and Governance*, 3 Big Data & Soc'y 1 (2016).

13 *See* Wagner et al., *supra* note 8, at 635-50; Nicholas Bagley, *The Puzzling Presumption of Reviewability*, 127 Harv. L. Rev. 1285 (2015).

take advantage of predictable vulnerabilities–or when they engage in cumbersome, opaque, and unwieldy processes that span years but ultimately fail to produce meaningful change in the problems they were attempting to address.

Many factors contribute to agency inaction and ineffectiveness. Most obviously, both can result from the patterns of unequal access and influence described above and/or from efforts by powerful actors to impede new regulation, as described above. Other factors are more deeply embedded in contemporary regulatory practice. In particular, as described in our reports on "Designing Policymaking Mechanisms for Regulatory Dynamism" and "Mechanisms for Including Publics in Administrative Governance," over-reliance on cost-benefit analysis prevents policymakers from acting to address certain kinds of harms, and the inability of most agencies to engage in precautionary policymaking dooms them to playing catch-up, unable to act until harms have become large and often irreversible.

Part 2: (Re)Defining Core Concepts and Values

The ideas of legitimacy and accountability that have played such important roles in the literatures on administrative processes connect to a larger ideal of the rule of law, so we begin our discussion there. The classic statements of the rule-of-law ideal revolve around judicial reasoning, judicial process, and their relationships to legislative enactments.[14] Those statements powerfully shaped the legal process model of the administrative state that emerged in the mid-twentieth century, and they continue to inform both judicial and scholarly thinking about administrative legitimacy today. To be clear, we agree with the many scholars who have argued that a strong administrative state is an essential precondition for a functioning democracy.[15] From our perspective, part of the problem is a legitimacy and accountability paradigm that is no longer fit for purpose. Two mismatches between the contemporary administrative state and traditional rule-of-law thinking are particularly significant.

First, classic statements of the rule-of-law ideal emphasize a particular type of reasoned decisionmaking in which already-agreed general rules are applied to specific cases in a way that is consistent, transparent, and explained. But the various kinds of specialized technical expertise on which administrative institutions need to rely often operate via modalities that resist both abstraction and case-specific explication–that involve and require consideration of factors such as probabilities, margins of error, and emergent ecosystem effects. Automated data driven algorithmic systems exacerbate this mismatch in two important ways. Because such systems operate predictively and opaquely based on population data, producing results that will vary as the underlying population data changes, the results they generate cannot and will not conform to the classic rule-of-law requirements summarized above.[16] And because automated data driven algorithmic systems tend to work around broad, general rules intended to constrain their operation, attempts to regulate their development and operation using broad, general rules will fail.[17] For all of these reasons, legitimacy constraints on decisionmaking appropriate to and effective for the era of networked digital technologies will need to be formulated differently.

Second, classic statements of the rule-of-law ideal situate the traditional, highly individualized model of judicial process (including both adversarial hearings and opportunities for appeal) as the principal engine of accountability and error correction.[18] As noted in Part 1 above, process requirements can be weaponized to prevent agencies from acting in furtherance of their public mandates. But a more fundamental problem is that, particularly when modalities of specialized technical decisionmaking and data driven automated decisionmaking are taken into account, the traditional process model

14 Lon Fuller, The Morality of Law (1969); Joseph Raz, The Authority of Law: Essays on Law and Morality (1979); Joseph Raz, The Authority of Law: Essays on Law and Morality (1979); Hans Kelsen, Pure Theory of Law (1934).

15 *See, e.g.*, Blake Emerson, L*iberty and Democracy Through the Administrative State: A Critique of the Roberts Court's Political Theory,* 73 Hastings L.J. 371 (2022); K. Sabeel Rahman, *Anti-Domination and Administration*, 100 N.Y.U. L. Rev. 1984 (2025); Edward L. Rubin, Lecture, *Responsive Democracy and the Administrative State,* 75 Case W. Rsrv. L. Rev. 929 (2025).

16 Danielle K. Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249, 1253–54 (2008); *see also* Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 Geo. L.J. 1147 (2017).

17 Lorin Brennan, *AI Ethical Compliance is Undecidable*, 14 Hastings Sci. & Tech. L.J. 311 (2023); Wendy Currie et al., *Rethinking Technology Regulation in the Age of AI Risks*, 40 J. Info. Tech. 236 (2025).

18 Additionally, some of the leading work on lay ideas of legal legitimacy focuses heavily on the family law and criminal justice systems. *See* Tom Tyler, *Psychology and Institutional Design*, 4 Rev. L. & Econ. 801 (2008); Tom Tyler, *Citizen Discontent with Legal Procedures: A Social Science Perspective on Civil Procedure Reform*, 45 Am. J. Comp. L. 871 (1997).

can be counterproductive. In particular, certain kinds of decisions about precautionary regulation need to be made prospectively, on an evidentiary record that will necessarily be incomplete and subject to margins of error, and such decisions also need to consider catastrophic risks even when models trained on past events might rate the probability of such events as low.[19] Automated decisionmaking is the result of complex ongoing sets of activities that begin with the construction of models and the assembly of datasets, extend into model training and revision, and evolve continually as predictive systems are applied to new cases and fact patterns. At least some of these activities may be more usefully assessed using different kinds of processes that operate at different points in time.[20]

For some, the lesson to be drawn from these mismatches is that expert administrative processes are illegitimate modes of governance in a democratic society or, perhaps, necessary evils to be tolerated so long as efforts are made to constrain them within the classic rule-of-law framework. Those arguments have lent strength to other arguments about administrative illegitimacy that sound in separation of powers but stem from philosophical commitments to minimal governance. More recent rule-of-law critiques of the impacts of automated, data-driven, algorithmic technologies have simply added fuel to an already roaring blaze.[21]

We think that, rather than attempting to shoehorn administrative processes into a paradigm that cannot accommodate them, a different rule-of-law framework for administrative institutions is necessary.[22] Governing at scale in a sophisticated, information-driven economy requires an administrative state, and if that administrative state is to have any hope of discharging its public mandates effectively, it must have powerful, information-driven capabilities of its own. Fully developing such a rule-of-law framework and situating it in the academic debates on the topic are tasks beyond the scope of this report. Here, we confine ourselves to describing the core requirements of legitimacy and accountability–which, as we will explain, are interdependent concepts–and then articulating three component requirements–transparency and demystification, care and respect, and oversight–that are designed to give those concepts more concrete and specific meaning.

Legitimacy

One basic rule-of-law requirement for administrative institutions is legitimacy. Legitimacy cannot derive simply from the fact that a particular administrative entity is established by legislative enactment and conducts its processes in the way the law prescribes. Laws and regulations can prescribe–or permit or excuse–arbitrariness or abuse of power. Systems of administrative governance can work to entrench special interest capture or cronyism and self-dealing. A system of administrative governance that is cruel, indifferent, or unfair will lose legitimacy in the eyes of the public. Put differently, legitimacy also has descriptive and normative aspects.[23] Each aspect introduces a complex set of considerations.

Descriptive legitimacy refers to whether affected publics–including both individual citizens and the particular communities in which they are members–perceive administrative institutions and their various activities as legitimate. This might seem to be a predominantly empirical question, calling for expert measurement and interpretation. That is not the meaning we intend, for two reasons. First, public perception can be unstable

19 *See generally* Elizabeth Fisher & Sidney A. Shapiro, Administrative Competence: Reimagining Administrative Law 35-65 (2020) (discussing the contours and necessity of administrative expertise); Nassim Nicholas Taleb, The Black Swan: The Impact of the Highly Improbable (2007).

20 *See* David Freeman Engstrom & Daniel E. Ho, *Algorithmic Accountability in the Administrative State*, 37 Yale J. on Reg. 800 (2020); Mulligan & Bamberger, *supra* note 10.

21 *See* Noah Rosenblum, *What We Talk about When We Talk about the Rule of Law in the Administrative State*, 16 N.Y.U J. L. & Liberty 467 (2023).

22 *See* Edward L. Rubin, Lecture, *Responsive Democracy and the Administrative State*, 75 Case W. Rsrv. L. Rev. 929 (2025).

23 *See, e.g.*, Chris Havasy, *Relational Fairness in the Administrative State*, 109 Va. L. Rev. 749, 760-67 (2023).

and vulnerable to manipulation. The current historical moment is instructive. As many studies have documented, the regulatory state has been the target of systemic delegitimation for decades.[24] Second, as we discuss below, public perception is in part a function of the way the administrative state engages with the publics whose interests it is supposed to serve. Put differently, descriptive legitimacy depends in part on whether and how the administrative state is accountable to affected publics. Empirical measures of public perception have an important role to play in assessing whether systems of administrative governance are on the right track–and, if not, why the public thinks they are on the wrong track. But we are wary of appearing to enshrine any specific group of subject matter experts as the principal arbiters of administrative legitimacy.

To maintain–and deserve–descriptive legitimacy, a regime of administrative governance also needs normative legitimacy, which refers to whether administrative institutions conform their behavior to the justifications for creating them and investing them with power. In an era when invocations of expertise are often weaponized, older conceptions of normative legitimacy premised on neutral expertise have been difficult to sustain. Newer conceptions have emerged to fill the void. One prominent contender has been presidential control of administration, based on the premise that the President's broad-based electoral accountability legitimates administrative action. As recent events have illustrated, however, the presidential control theory lacks internal safeguards against deployment of administrative power in the service of naked acts of political aggression. Other contenders hold that normative legitimacy in administration depends on agencies' pursuit of some explicitly articulated substantive moral basis for their authority.[25] Within such theories, both the particular goals an administrative agency should pursue and the ways it should pursue them are the subject of considerable debate and disagreement. As Jodi Short explains, moreover, to the extent that theories of "moral administration" devolve into "state sponsored morality projects," they contain significant internal tensions.[26]

We think that it is possible to identify and defend a minimum set of requirements for normative legitimacy in administrative governance that hedge to some extent against the risks of unchecked political and/or moral overreach. We describe these requirements, which relate in part to considerations of accountability and in part to a set of component requirements that also incorporate process considerations, below.

Accountability

A second basic rule-of-law requirement for administrative institutions is accountability. Like "legitimacy," the term "accountability" can have many meanings.[27] We think it cannot mean simply that administrative institutions must give some account of themselves but that any account, however perfunctory or self-justifying, will do. As we note above, systems of administrative governance can be cruel or unfair and can work to entrench special interest capture and self-dealing. In such cases–and even in others where regulators are well-intentioned but regard the task of account-giving as burdensome or secondary–disclosures intended to provide regulatory accountability can be largely performative or designed

24 Gillian E. Metzger, *1930s Redux: The Administrative State Under Siege*, 131 Harv. L. Rev. 1 (2017); Thomas O. McGarity, Freedom to Harm: The Lasting Legacy of the Laissez Faire Revival (2013).

25 Jodi Short, *The Moral Turn in Administrative Law*, Ind. L. J. (forthcoming 2026), https://ssrn.com/abstract=4909394.

26 *Id.*, Part IV.

27 *See, e.g.*, Jerry L. Mashaw, *Accountability and Institutional Design: Some Thoughts on the Grammar of Governance, in* Public Accountability: Designs, Dilemmas and Experiences 115, 118–26 (Michael W. Dowdle ed., 2006); Gillian E. Metzger & Kevin M. Stack, *Internal Administrative Law*, 115 Mich. L. Rev. 1239 (2017).

for expert or political audiences.[28] Put differently, the kind of accountability that reinforces legitimacy also has descriptive and normative aspects, which relate to the content and the direction of account-giving.

To be accountable as a descriptive matter, administrative institutions must give accounts of their activities and operations that are adequate to enable the recipients to assess whether and how such institutions are discharging their public mandates. The accounts must explain what such institutions are doing (or choosing not to do), the kinds of information on which they are relying (or choosing not to rely), and the methods by which they are choosing to proceed.

For a system of administrative accountability to be normatively sufficient, accountability must run to the public. Without question, accountability in administration also needs to run in other directions. Some kinds of accounts need to flow internally within the executive branch, and other kinds of accounts already flow to Congress as required by the various statutes creating and conferring authority on the various agencies. In our view, however, a system of administration that does not have accountability to the public at its core cannot be normatively legitimate and is unlikely to be descriptively legitimate.

There is some question whether the most reliable institutional route to public accountability may run through Congress. Congressional committees with jurisdiction over the various executive branch agencies have some accumulated knowledge, yet those committees are also underresourced, and many of their staff members are generalists. A properly designed information commission located in the legislative branch might effectively discharge multiple kinds of accountability functions. We discuss creating such an office as an administrative institution in Part 4 below, but we are agnostic on its location.

Minimum Requirements for Legitimacy and Accountability

Here, we identify and defend a set of minimum component requirements for legitimacy and accountability in administrative governance. As described below, the requirements blend substantive and process commitments, and that is so by design. A rule-of-law paradigm for administrative institutions cannot rest exclusively on notions of fair process, but it also cannot ignore procedural fairness.

Transparency and Demystification

The first essential component of legitimacy and accountability in administration is attentiveness to the particular ways in which account-giving is undertaken. We will refer to this requirement as a requirement of transparency and demystification.

Turning first to substance, adequate account-giving will not simply be a matter of producing whatever information currently exists. As noted in Part 1 above, there are many possible sources of knowledge capture within government, and information overload also can obfuscate or otherwise impair the efficacy of even well-intentioned disclosures. We have discussed strategies for ensuring adequate information production from private economic actors in multiple previous reports, and many of the same strategies can be used within government. In particular, as discussed in our report on "Regulatory Monitoring in the Information Economy" and "Designing Policymaking Mechanisms for Regulatory Dynamism," it may be necessary to introduce new governance seams–discontinuities or other deliberately created intervention points through which systems that appear to be seamless can be rendered more legible and more amenable to governance–to enable the kinds of information production that will allow legislators and the public to assess the efficacy of administrative processes and actions.

28 Daniel E. Walters, *Communicative Administration: The Administrative State Beyond Legal Administration*, 78 Stan. L. Rev. (forthcoming 2026), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5376707.

Additionally, as described in our report on "Mechanisms for Including Publics in Administrative Governance," in crafting disclosures, administrative institutions need to consider the perspectives and capabilities of affected publics. Although administrative institutions often must rely on expert information to discharge their public mandates, they must devote care and effort to demystifying expert discourses so that affected publics can be at the table. Demystification has a similar role to play in administrative account-giving.

Satisfying the requirement of transparency and demystification also requires attention to process considerations. As discussed in Part 1, the current regime of accountability to the public relies too heavily on the public to decipher highly technical Federal Register notices and then, as needed, to make FOIA requests for other types of information. A framework for administrative legitimacy must be built on regular, consistent production of trustworthy information about both regulated entities, regulatory beneficiaries, and regulators themselves. We discuss possible mechanisms and institutional forms for achieving this sort of accountability below.

Care and Respect

A second essential component of legitimacy and accountability in administration is attentiveness to the public mandates with which administrative institutions are charged and to the full range of human and societal interests that those mandates implicate. We will refer to this requirement as a requirement of care and respect.

The requirement of care and respect implicates two other, more common ways of evaluating institutional performance–accuracy and efficiency–but does not simply reduce to them. Consider first accuracy, which concerns whether the system has produced the "right" results. Any decision making system will make mistakes. An automated decision system that makes too many mistakes, that refuses to acknowledge and correct its mistakes, and/or that exhibits persistent bias will be illegitimate–but, conversely, a system that avoids those problems will be allowed some leeway for error. A system of expert policymaking that persistently overweights industry interests, fails to consider emergent threats, and/or fails to acknowledge and correct its own misjudgments is illegitimate–but, conversely, a system that avoids those problems will be allowed some leeway, as well. Now consider efficiency. A system for policymaking or enforcement that wastes resources or that succumbs to paralysis and fails to produce results will be illegitimate–but a system that fails to permit adequate contestation will also be illegitimate.

For these reasons, we think that neither accuracy nor efficiency standing alone can serve as a benchmark of legitimacy and that care and respect are more useful concepts for encompassing not only accuracy and efficiency but also (and more importantly) the orientation that a system of administrative governance should bring to pursuing those goals.

Like the criterion of transparency and demystification, that of care and respect has intertwined substantive and process dimensions. To manifest care and respect, administrative agencies must attend to the full range of human and societal interests that their public mandates implicate and work to produce results that honor those mandates.[29] They must superintend processes that preserve room for valid critique while averting capture or delegitimation by the powerful. Care and respect are also relational concepts. A legitimate system of administrative governance must operate in ways that manifest empathy for and acknowledge the dignity of all of its constituents.[30] This means, at minimum, that it must initiate and sustain meaningful dialogues with all of the publics whose interests it is supposed to serve and must acknowledge and work to correct its own inevitable failures.

29 Blake Emerson, *Public Care in Public Law: Structure, Procedure, and Purpose*, 16 Harv. L. & Pol'y Rev. 35 (2021).

30 Cristie Ford, *Regulation as Respect,* 86 L. & Contemp. Probs. 133 (2023); Chris Havasy, *Relational Fairness in the Administrative State*, 109 Va. L. Rev. 749 (2023); Sofia Ranchordas, *Empathy in the Automated Administrative State*, 71 Duke L. J. 1341 (2022).

As used in this report, care and respect will refer to institutions that attempt to fulfill their public mandates accurately and effectively–producing results that honor those mandates, getting it "right" enough of the time, and avoiding persistent bias for or against particular groups; that manifest respect for all of their constituents; and that work openly and honestly to correct departures from these ideals. The mechanisms and institutional arrangements we discuss below are intended to empower and constrain the regulatory state to operate within these parameters.

Oversight

A final essential component of legitimacy and accountability in administration relates to oversight. Here again, the term "oversight" can mean different things to different people. Some hold that systems for ensuring transparency to the public and/or to Congress–i.e., systems designed to require government entities and institutions to produce information about themselves and their activities, as we have described above–both enable and inevitably engender oversight. The theory is that, after being provided with adequate information about the inner workings of administrative agencies, Congress will make–or the public will demand–changes in the underlying processes and practices. We think that understanding of oversight is too narrow. Standing on its own, disclosure may not be enough to ensure needed corrections or changes.

For others, "oversight" may mean the ability to compel production of additional information beyond what has already been disclosed in the ordinary course. We think investigative authority is an important component of effective oversight. However, investigation-centered theories of oversight retain the ultimate focus on disclosure as the primary engine of change, and again, we are skeptical.

A third way of understanding "oversight," and the meaning we intend in this report, moves beyond disclosure and investigative authority to include specified consequences to be imposed when agencies or agency officials deviate significantly from their public mandates or engage in other abuses of power. We discuss possible mechanisms for institutionalizing effective oversight below.

Part 3: Mechanisms for Achieving Legitimacy and Accountability

In this Part, we present recommendations for operationalizing the criteria of legitimacy and accountability and the component requirements of transparency and demystification, care and respect, and oversight across the domains of policymaking, enforcement, citizen-focused decision-making, and government technology and data.

Empowering and Channeling Precautionary Policymaking

One important dimension of administrative legitimacy and accountability concerns the ways that agencies engage in policymaking. Policymaking inevitably implicates competing interests and requires regulators to make tradeoffs. As our report on "Designing Policymaking Mechanisms for Regulatory Dynamism" describes, however, regulators today labor under other burdens that are not inevitable. Legacy policymaking processes designed nearly a century ago force policymaking into a reactive stance, effectively disabling regulatory responses to some of today's most pressing problems. That report develops a series of proposals designed to allow regulators to act more nimbly and proactively but brackets questions about the precise contours of legislative authorization and judicial review. Here, we consider those questions and connect them to the overarching themes of legitimacy and accountability more generally.

Both in our earlier report and here, we are especially focused on empowering regulators to identify and mitigate or prevent harms that are emergent and probabilistic in character. We note, as well, that policymaking becomes even more difficult when regulators must consider entities whose activities implicate multiple public regulatory regimes and multiple agencies. In particular, the largest technology platform companies and the largest financial services companies regularly engage in such activities. It may be desirable to reconsider aspects of the structure and jurisdiction of federal agencies to align them more effectively with the ways that information-economy actors and activities are structured. That task, however, is outside the scope of this report.

Pending more comprehensive reorganization, we think the best approach lies in adapting a model that already exists in certain specialized sectors as a template for precautionary policymaking directed toward specific types of emergent threats. So, for example, the Federal Reserve monitors a wide range of economic indicators, meets periodically to consider what those indicators suggest about the likely path of the economy, and can adjust parameters such as interest rates if the data suggest need for a correction.[31] The Financial Stability Oversight Council was created in hopes of establishing a central vantage point for mitigating systemic financial risk by recommending adjustments to capital requirements, leverage limits, and stress testing protocols, although its limited authority and unwieldy structure have

31 *2024 Annual Report: Overview*, Bd. Governors Fed. Rsrv. Sys., https://www.federalreserve.gov/publications/2024-ar-overview.htm; 12 U.S.C. § 5365.

compromised its efficacy.[32] To detect and mount effective responses to emergent public health threats–ranging from recommendations about the availability of antiviral drugs to instructions on the composition of seasonal vaccines to emergency measures such as social distancing, masking, and quarantines–public health officials rely on "sentinel surveillance indicators" that operate both retrospectively and predictively.[33]

The framework we envision would be built around legislation clearly authorizing a designated agency or group of agencies to monitor and regulate on one or more questions relating to the systemic effects of particular economic activities on an identified threat or threats to the public welfare–for example, the relationship(s) between social media usage, mental health, and trust in social institutions; the effects of hyperscale data centers on energy use, water consumption, and carbon production; and so on. The legislation should clearly articulate the values to be promoted and should instruct the agency or agencies to: identify relevant indicators of harms or threats, monitor the indicators, and act on reasonable projections of future (or already emerging) harm or systemic instability. It should explicitly disfavor a narrow cost-benefit approach to questions of harm and threat and instead direct the agency or agencies to proceed in a manner consistent with best practices in a range of expert disciplines, considering not only "consensus" but also emerging concerns that command the attention of a significant minority of those working in the field. And, importantly, it should instruct the agency or agencies to place a precautionary thumb on the scale with regard to emergent systemic effects and "black swan" effects.

More specifically, when the agency or agencies observe relevant indicators–including new indicators identified in connection with emerging concerns–reaching thresholds that support reasonable projections of future (or already emerging) harm or systemic instability, they should identify an "impact zone" consisting of the entities, activities, or technologies that the indicators have implicated; notify those included in the impact zone; and prescribe information production requirements. From there, the agency or agencies would have authority to compel specific changes in design or business practices, to require pre-market review of contemplated changes or business practices, and/or to establish cross-cutting rules governing design features, functions, and or business practices.

To ensure appropriate accountability to all interested parties, agencies should be required to "show their work" on these questions. However, the legislative authorization should clearly acknowledge both the inherently uncertain and probabilistic nature of forward-looking, precautionary policy-making and the potential harms flowing from regulatory inaction. It should instruct reviewing courts to defer to reasonable agency interpretations of the available evidence provided that the agency or

32 *Financial Stability Oversight Council: Council Work*, U.S. Dep't. Treasury, https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/financial-stability-oversight-council/council-work; Hilary J. Allen, *Putting the Financial Stability in Financial Stability Oversight Council*, 76 Ohio St. L. J. 1087 (2015).

33 Sandra W. Roush, *Chapter 18: Surveillance Indicators*, Ctrs. Disease Control & Prevention (June 3, 2025), https://www.cdc.gov/surv-manual/php/table-of-contents/chapter-18-surveillance-indicators.html; *End-to-End Integration of SARS-CoV-2 and Influence Sentinel Surveillance: Revised Interim Guidance*, World Health Org. (Jan. 31, 2022), https://www.who.int/publications/i/item/WHO-2019-nCoV-Integrated_sentinel_surveillance-2022.1.

agencies also have considered the severity of the potential harm or threat and crafted a proportionate response.[34] The agency or agencies should be instructed to conduct iterative reassessment of their decisions and actions, as many pieces of legislation now require, but the effects of systemic interventions on matters such as mental health or natural resources consumption takes time to manifest. The legislative authorization should clearly acknowledge as much and should prescribe a timeframe for iterative assessment that is long enough to make questions about efficacy meaningful.

To be most effective, a framework for precautionary regulation also must incorporate safeguards against paralysis, weaponization, and delegitimation. Regulated industries may argue that regulators have failed to consider contrary evidence or have strayed from their legislatively defined mandates, and they should be entitled to raise such arguments. To ensure that precautionary policymaking can proceed quickly enough to be effective in safeguarding the public interest, however, windows for appeal should be limited to designated intervention points. In particular, determinations about the relevant indicators, the covered impact zone, and the content of ongoing information production obligations directed to covered entities would not be subject to immediate appeal; instead, issues relating to those determinations would be preserved for consideration along with appeals relating to subsequent regulatory actions. At the same time, the agency or agencies need to ensure that affected publics understand the purpose of the precautionary delegation and are involved in the process from beginning to end. In the particular context of precautionary policymaking, it will be necessary to explain why the desired result–no catastrophic harm, and if all goes very well, maybe not much to see at all–represents a successful investment of public resources.[35]

Empowering and Incentivizing Effective Enforcement

A second important dimension of administrative legitimacy concerns the ways in which agencies pursue–or, sometimes, choose not to pursue–enforcement of public mandates. Our report on "Rebooting Administrative Enforcement for the Information Economy" offers detailed recommendations for redesign of enforcement mechanisms. Here, we briefly discuss two intersections between those recommendations and legitimacy interests; the reader seeking more detail on either issue should consult the other document.

With growing frequency in recent years, some federal agencies–and especially those that have attempted to grapple with diffuse, emergent harms precipitated by new business models and product offerings in the technology and financial services industries–have confronted a steady drumbeat of charges that they have exceeded their enforcement authority as that authority is currently defined. Weighing in on the merits of those charges is outside our scope, but we think the fix is straightforward. To the extent that enforcement authority has been conceptualized as a legitimacy problem relating to legislative authorization, the issues can be addressed by enabling legislation covering, among other things, the authority to: impose disgorgement penalties, mandate changes in the design of networked digital services and platforms; issue product-and-service-recalls, mandate changes in organizational structure, and charge individual officers, directors, and employees for corporate wrongdoing.

34 *See Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984); *see also* Rory Van Loo, *Stress Testing Governance,* 75 Vand. L. Rev. 553 (2023). For a technical overview of threat modeling, see Adam Shostack, Threat Modeling: Designing for Security (2014). For discussions of how to adapt this method in policy contexts, see Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. Colo. L. Rev. 1117, 1149 (2013); Paul Ohm, *Sensitive Information*, 88 S. Cal. L. Rev. 1125, 1131 (2015).

35 *See* Hilary J. Allen, *Regulatory Managerialism and Inaction: A Case Study of Bank Regulation and Climate Change*, 86 L. & Contemp. Probs. 71 (2023); Frank Pasquale, *Power and Knowledge in Policy Evaluation: From Managing Budgets to Analyzing Scenarios*, 86 L. & Contemp. Probs. 39 (2023).

Other critics charge that agencies underenforce public mandates, thereby failing to discharge their obligations to the public and to Congress. Our enforcement report lays out a set of reforms designed to increase the incentives for enforcers to exercise their proper authority and to help reveal when they do not.

Restructuring Automated Decision-Making for Systemic Legitimacy

A third important dimension of administrative legitimacy and accountability concerns the ways that government agencies make determinations about benefits due to and/or obligations owed by individual citizens. This issue often has been framed in terms of contestability, which, in turn, is traditionally understood as mandated by constitutional guarantees of due process. Within the due process literature, it is well recognized that some types of safeguards may be infeasible in programs that must be administered at scale, and others may be undesirable in view of the drain they would create on finite administrative time and resources.[36] Long ago, the Supreme Court instructed courts reviewing due process challenges brought by individual claimants to weigh: (1) the private interest affected by the action; (2) the risk of an erroneous deprivation of that interest and the potential value of additional procedural safeguards; and (3) the government's interest, including the administrative and fiscal burdens of any additional safeguards.[37] This interest-balancing inquiry does not translate well into the age of automated decision-making, in which safeguards inhere (or fail to inhere) at least partly in the ways digital tools are designed and trained. When an agency makes automated decisions affecting the provision or denial of benefits to individual claimants, one might argue that due process interests attach at multiple levels/points, including: an interest in understanding how the automated decision reached the result it did in a particular case and what facts might have produced a different result; an interest in human review; an interest in contesting elements of the automated system, such as parameters and/or the training data, that produce systemic effects; and an interest in contesting the system's procurement and/or pre-deployment testing and configuration.[38]

Based on this insight, Congress could prescribe multiple sets of new opportunities for individuals to challenge automated systems that make, or ultimately will make, decisions affecting them. This, however, would threaten a level of process paralysis that would place acute stress on agency resources–and, ultimately, undermine the public legitimacy of the programs that agencies must administer and on which many members of the public rely for important kinds of support. Instead, we think the shift to automated digital tools presents an opportunity to rethink legitimacy and accountability structures. The goal should not be to eliminate automation but rather to ensure performance of two complementary types of legitimacy and accountability functions that work together to keep automation in its lane. One involves genuinely humanizing the process for individual citizens; the other, subjecting automated data driven tools and systems to the multiple necessary kinds of systematic scrutiny and correction.

To serve the first goal–humanizing the process for individual citizens–agencies should be obliged to provide clear information about how the automated systems work, and human support must be built into the process at accessible points. In an ideal world, applicants should be able to speak with a trained agency representative who can explain and guide them through the applicable processes. These representatives would not have authority to alter decisions but instead would provide informational and navigational support. They would, however, have

36 For the canonical treatment of these issues, see Jerry L. Mashaw, Bureaucratic Justice (1983).

37 *Mathews v. Eldridge*, 424 U.S. 319 (1976).

38 *See* Danielle K. Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014); Deirdre K. Mulligan & Kenneth A. Bamberger, *Procurement as Policy: Administrative Process for Machine Learning*, 34. Berkeley Tech. L. J. 773 (2019).

both sufficient training and sufficient authority to flag troubling cases for the agency teams charged with the second goal, discussed below.[39] In some cases, designated organizations might train representatives to perform some or all of these functions.[40] To help prevent the creation of Kafkaesque systems that look reasonable on paper but prove impenetrable in practice, agency leadership and system designers should be required to undergo the agency's automated processes themselves.

The second goal–systematically scrutinizing and correcting automated processes–will be served most effectively if policymakers ignore much of the conventional wisdom about the salutary effects of a "human in the loop" and about the individualized appeal as the sine qua non of legitimacy. Instead, they should create rules to drive automatic, iterative assessment and correction in ways that shift the burden from individual citizens (who now must discover problems and file appeals) to agencies (which should have continuing duties to interrogate the procurement, development, retraining, and operation of automated systems from beginning to end and correct errors proactively).

To begin, automated systems used in agency decision-making should be configured to engage in active pattern detection, continuously monitoring whether results differ systematically in ways that suggest illegitimate algorithmic bias, other forms of systematic error, or persistent failures of compassion and care rather than relevant variation in individual circumstances.[41] Monthly reporting should track approval rates (for benefits), audit rates (for income taxes and other obligations), and/or other relevant rates, broken down by a range of demographic and other categories. Appeals would have a role to play–and, indeed, we think that some role for appeals is constitutionally necessary–but rather than treating every case as an isolated black box and inserting a human reviewer who may end up simply deferring to the automated system's recommendations, appeals should be handled differently and human reviewers should play a different kind of role. As has already been noted, automated systems' outputs resist individualized explanation, but such outputs may become more legible along a number of axes when they are viewed in aggregate. To the extent feasible, then, most appeals should be pooled for evaluation. Additionally, human reviewers with appropriate expertise should audit a percentage of the outputs without access to the AI system or its recommendations, with a particular emphasis on the kinds of cases for which accumulated learning on algorithmic fairness suggests higher rates of error. So, for example, human experts might review a designated percent of benefits decisions for people with cognitive disabilities or income tax audit decisions affecting members of designated racial/ethnic minority groups.[42] To guard against the risk that an agency might choose to ignore or bury adverse information about system performance, aggregate perfor-

39 To the extent that automated agents are envisioned (now or in the near future) as performing various support functions, we think that a firm distinction should be drawn between those functions and the kind of humanization work that we are recommending here. Additionally, automated support agents provided by government agencies should have been trained to represent citizens' interests and developed in a manner that conforms to the recommendations in our report on "Provisioning Digital Tools and Systems for Government Use."

40 *See, e.g., VA Accredited Representative FAQs,* U.S. Dep't. Veteran Affairs, https://www.va.gov/resources/va-accredited-representative-faqs/.

41 *See* Engstrom & Ho, *supra* note 20; Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. Cal. L. Rev. 1529, 1557–58 (2019).

42 *See* Julian Christensen et al., *Human Capital and Administrative Burden: The Role of Cognitive Resources in Citizen-State Interactions.* 80 Pub. Admin. Rev. 127-136 (2020); Hadi Elzayn, et al., *Measuring and Mitigating Racial Disparities in Tax Audits*, 140 Q. J. Econ. 113 (2025).

mance data should be made publicly available, as should information about any studies or reports conducted or commissioned by the agency, and non-governmental researchers should be given conditional access to more granular data (perhaps using a system similar to that for gaining access to census data).

Next and importantly, processes of pattern detection–whether ex ante or originating in pooled appeals–should drive corrections that are automatic, retroactive, and system-wide. For instance, if an audit reveals systematic underweighing of certain evidence affecting eligibility for particular benefits, all affected cases should be reprocessed with correct weights, and wrongful denials should be reversed automatically. When flawed training data is discovered, the agency should notify the public and begin a process to replace the system, following the recommendations detailed in our report on "Provisioning Digital Tools and Systems for Government Use." When a new issue emerges regarding programming or calibration of the system more generally, all prior decisions within a prescribed period of time should automatically be revisited. In each of these situations, individuals mistakenly denied benefits or subjected to intrusive audits should receive apologies along with meaningful information about what factors led to the mistakes and what has been done to correct the problem(s). To guard against the risk that agencies will design their systems to under-award or over-audit at the front end, knowing that corrections will be made later, this tendency should be trained out of the system by instructing it–repeatedly, as necessary–to place a precautionary thumb on the scale in favor of the individual applicant/taxpayer.

Monitoring Uses of Government Technology and Data

A final dimension of administrative legitimacy and accountability concerns the extent to which agencies and/or their officials and employees are accountable and subject to oversight for uses, misuses, and abuses of government technology and data. Existing government accountability statutes do not fully address current needs. Many commentators have observed that the Privacy Act, which covers records of personally identified data maintained by executive branch agencies, is woefully outdated. It is riddled with exceptions, incomplete in its coverage, focused on the kinds of siloed systems of records that existed decades ago, and overly wedded to lengthy, turgid Federal Register notices as a principal engine of compliance with the statutory requirements.[43] The Paperwork Reduction Act pre-dates the digital era; many of its provisions are poorly adapted to the kinds of communications that agencies need to make now and/or easily weaponized by those seeking to restrict the kinds of information-gathering processes that agencies can conduct.[44] The Government in the Sunshine Act requires disclosures about agency meetings but not about the behind-the-scenes configuration of digital tools and services used for conducting agency business.[45] As our report on "Provisioning Digital Tools and Services for Government Use" discusses, many of the digital tools and services now used by federal agencies are procured from private vendors. In those cases, agencies themselves face challenges in understanding either how the tools and services on which they now rely have been configured or how they are operating in real time. And, as noted in Part 1, the FOIA's trade secrecy exception shields many features of privately-provided digital tools and services from disclosure to members of the public.

43 Robert Gellman, From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974 (2021); Sarah Lamdan, *Revisiting the Privacy Act of 1974 for Big Data Policing,* 6 Geo. L. Tech. Rev. 386 (2022); Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection,* 2006 U. Ill. L. Rev. 357 (2006); *State of Federal Privacy and Data Security Law: Lagging Behind the Times?: Hearing Before the S. Subcomm. on Oversight of Gov't Mgmt., the Fed. Workforce, & the D.C. of the S. Comm. on Homeland Security & Governmental Affairs*, 112th Cong. (2011-2012) (statement of Peter Swire, former Center for American Progress Senior Fellow).

44 Stuart Shapiro, *The Paperwork Reduction Act: Benefits, Costs and Directions for Reform,* 30 Gov't Info. Q. 204 (2013).

45 5 U.S.C. § 552b.

The kinds of information needed for accountability and oversight are relatively easy to describe. Our report on "Regulatory Monitoring in the Information Economy" describes the changes that are needed to equip the administrative state to monitor information-economy activities effectively. Similar capabilities are needed to create accountability for both government agencies and the vendors that supply them with digital tools and services. In brief, those include information production requirements, on-site inspections, audits and supervision requirements, and the authority to devise and run experiments to test the capabilities and performance of digital architectures, platforms, and services. Our report on "Provisioning Digital Tools and Systems for Government Use" describes the changes that are needed to help federal agencies understand tools and systems procured from private sector vendors, as well as other changes that are needed to help them take charge of the processes of planning and provisioning more generally. In brief, those include eliminating the statutory preference for private sector providers, empowering agencies to take a lifecycle approach to managing their govtech needs, and empowering agencies to impose interoperability requirements on private vendors to avoid lock-in.

The more difficult challenges concern where and how to institutionalize these mechanisms to harden them against capture and cooptation. We turn to that question in Part 4 below.

Part 4: New Institutional Structures

To help implement the recommendations in Parts 2 and 3, we recommend creating two new offices with cross-cutting authority: a government information commission to ensure better and more consistent accountability and an Office of Government Integrity to oversee uses–and detect and disclose misuses and abuses–of government technical systems and data. In addition, we recommend revised and streamlined processes for hiring into agency civil service positions.

Accountability Beyond the Federal Register and FOIA

We begin by returning to the core value of accountability and the component requirement of transparency and demystification discussed in Part 2. Federal agencies, and the federal government more generally, should be institutionally equipped to give ongoing accounts of themselves and their activities, and those accounts should be adequate to enable the public to understand the ways that agencies are discharging (or, perhaps, not discharging) their public mandates. Much of this information should be produced automatically. Members of the public should not be expected to infer it by reading between the lines of Federal Register disclosures crafted to the specifications of decades-old statutes or to extract it piece by piece using FOIA requests. We therefore endorse Margaret Kwoka's call for the creation of an information commission charged with collecting and releasing information about how the federal government works and what it is doing.[46] Here, we build on that proposal with a few additional suggestions.

Information production that sheds light on the administrative state and its activities has been a core concern in all of our previous reports. Although our report on "Regulatory Monitoring in the Information Economy" focuses primarily on ensuring access by researchers and the public to information about the activities of digital platform firms and other important information economy actors, it also highlights the need to develop and share information about standards and best practices for auditing information economy activities. Our reports on "Designing Policymaking Mechanisms for Regulatory Dynamism" and "Rebooting Administrative Enforcement for the Information Economy" address the need for government agencies to be more forthcoming about their own policymaking and enforcement choices. Those recommendations, moreover, must be read in conjunction with our report on "Mechanisms for Including Publics in Administrative Governance," which underscores the need for effective information production as part of a two-way dialogue with affected publics. Last but not least, as discussed in our report on "Provisioning Digital Tools and Systems for Government Use," affected publics need to understand the provenance and capabilities of digital tools and services used by government agencies, and this requires additional specific forms of disclosure and transparency.

An information commission can help to develop best practices for all of these kinds of disclosure. Additionally and more generally, it can help to standardize and demystify the kinds of information made available on agencies' own websites and the processes for navigating agency websites and databases. It can serve as a central repository for more basic information, such as agency organization charts and framework statutes. It can also produce public education materials to inform citizens

46 Margaret B. Kwoka, *The Anti-Managerial Information Commission*, 86 L. & Contemp. Probs. 197 (2023).

about how the administrative state works and what federal civil service employees (discussed at greater length below) do.

An information commission would not obviate the need for a statute requiring government agencies to respond to citizen requests for information, but it would necessitate some rethinking of the statutes and processes that currently exist. For example, the new regime should override and effectively narrow some of FOIA's more troublesome exemptions, including the trade secrecy exemption that we have discussed in our earlier reports and above. It also will need to implement comprehensive privacy protections for personal data contained in government records. This need presents an opportunity to consider the many well-founded criticisms of the existing Privacy Act noted in Part 3 and also to create new, streamlined processes for individuals to gain access to their own records held by administrative agencies.[47]

Other issues will require more study. For example, we envision that some types of FOIA requests may become unnecessary under the new regime and that, instead, the information commission's own Inspector General together with the new government integrity regime described below will work to make sure that appropriate information is produced in a timely manner. In some circumstances, however, the need for an additional disclosure mechanism will be important. An act of Congress mandating the creation of an information commission should require the new commission to conduct a time-limited study of the ongoing uses of FOIA and prepare recommendations for an amended FOIA.

An Independent and Functional Civil Service

Next, returning to the core value of legitimacy and the component requirement of care and respect discussed in Part 2, we think that any path toward an administrative state that manifests care and respect for citizens must involve both an independent and well-functioning civil service system.[48] None of the mechanisms for ensuring legitimacy and accountability in the federal civil service and political appointments systems is currently working as originally intended, and at least some of the dysfunctions predate the current administration.

First, a baseline level of democratic accountability should flow from rules providing for the hiring and retention of an apolitical corps of civil service employees.[49] Those rules have now been substantially weakened by the second Trump administration's issuance of "Schedule Policy/Career," which (together with a proposed Office of Personnel Management (OPM) rule regarding implementation) removes the protections against adverse employment actions that career federal employees in policy-relevant positions formerly enjoyed.[50] Congress should legislatively rescind Schedule Policy/Career and restore the previous system of protections for civil service employees, with a few additions. For example, it should prohibit requiring employees to take oaths of loyalty to the president.

But policymakers should not stop there. Critics have argued that the hiring process (stewarded mostly by OPM) is too slow for all employees and, in particular, makes it harder to hire into specialized/technical

47 For sensible proposed reforms relating to individual access, see Margaret Kwoka, Saving the Freedom of Information Act (2021).

48 *See* Noah Rosenblum, *Toward a Realist Defense of the Civil Service*, 13 Reg. Rev. In Depth 7 (2024). It also requires a functioning system for making political appointments, a task that will entail comprehensive revision and reconciliation of a number of existing statutes and that we do not address here. *See* Anne Joseph O'Connell, Acting Agency Officials and Delegations of Authority, Report to the Administrative Conference of the United States (Dec. 2019).

49 *See, e.g.*, Catherine Fisk, *Democracy and a Nonpartisan Civil Service*, 67 Ariz. L. Rev. 629 (2025).

50 *See* Exec. Order No. 14,171, 90 Fed. Reg. 8625 (Jan. 20, 2025); Improving Performance, Accountability and Responsiveness in the Civil Service, 91 Fed. Reg. 5580 (Feb. 6, 2026) (to be codified at 5 C.F.R. pts. 210, 212, 213, 302, 432, 451, 537, 575, and 752).

positions with qualifications less familiar to OPM.[51] Some participants in our convening process invoked the children's game "Chutes and Ladders" to describe the current federal hiring process: it's easy to leave federal employment, but getting hired requires a laborious climb. A workaround that allows circumvention of many hiring formalities via short-term "loans" of employees without pay from private sector employers creates glaring conflict of interest problems. The chutes and ladders polarity should be reversed by streamlining and simplifying the background checking process. Additionally, federal agencies and Congress should revisit and rethink a host of other rules and policies that affect employee satisfaction and retention, ranging from rules about telework to rules about investment conflicts of interest. As we noted in our report on "Provisioning Digital Tools and Systems for Government Use," the rules about investment conflicts of interest are not uniform across agencies, making it more difficult to hire and retain technologists and other staff who do cross-agency work; that problem should be corrected. Last, building on the recommendations in our govtech provisioning report and our report on "Regulatory Monitoring in the Information Economy," Congress should create a comprehensive new program to recruit talented and motivated individuals into public service.

A final very important issue affecting the integrity of federal employees at all levels involves the "revolving door" phenomenon, in which departing employees secure lucrative private employment with the same industries they formerly regulated (or with lawyers representing those industries), and in which the prospect of such employment constrains the behavior of those still in government employ. The Biden Administration instituted a rule prohibiting former federal agency employees, including political appointees, from lobbying or otherwise materially assisting any company regulated by the agency during the 2-year period following their departure from government employment, but that rule has since been rescinded, although a narrower, statutory conflict of interest provision remains in place.[52]

Among those who support restricting the revolving door phenomenon, time limits are controversial.[53] Some argue that a flat time limit may discourage certain types of employees from working for the government. However, there is now a robust pipeline into public interest technology work. Additionally, if the previous system of civil service protections is restored as we recommend above, the government can offer other valuable inducements, including job security. We also think that a strict revolving door ban is especially important for those in political appointments and senior and midlevel civil service positions, because such positions can position someone for highly consequential post-government employment. We therefore recommend reinstituting the rule for all political appointees and all senior and midlevel civil service employees. For senior and midlevel technologists formerly employed by the federal government, an analogous rule should prohibit working for any tech company that currently serves or potentially may serve as a vendor to any federal agency for which the individual worked (either directly or indirectly by working on a govtech project intended for use within multiple agencies). We would also end the rule allowing a brief "loan" of an employee from a private employer to a federal agency without pay. Instead, such employees must resign from private employment and (assuming they fulfill senior or mid-level government roles) then become subject to the 2-year ban upon leaving government service.

---

51 U.S. Gov't Accountability Off., GAO-19-696T, Human Capital: Improving Federal Recruiting and Hiring Efforts (2019); Laura Moy et al., *Illusory Conflicts: Post-Employment Clearance Procedures and the FTC's Technological Expertise*, 35 Berkeley Tech. L. J. 793, 795 (2020).

52 18 U.S.C. § 207; *see* Exec. Order No. 13,989, 86 Fed. Reg. 7029 (Jan. 1, 2022); Exec. Order No. 14,148, 90 Fed. Reg. 8237 (Jan. 20, 2025).

53 *See* James D. Cox & Randall S. Thomas, *Revolving Elites*, 107 Geo. L. Rev. 845, 847-48 (2019).

Networked Oversight with Hard-Coded Limits

Finally, return to the component requirement of oversight discussed in Part 2. Here too, the relevant rules have been substantially weakened (if not entirely eviscerated) by the current administration's dismissal of most in-agency inspectors general (IGs). And here too, the preexisting system had some notable defects. We first describe three significant defects in existing oversight arrangements and then propose reconfiguring oversight authority to address needs of a networked and digital administrative state.

First, it is important to acknowledge that vesting too much power in oversight systems can be counterproductive. Such power can be used to obstruct needed government functions rather than to protect the public's interests, and it can also produce other unintended obstructive effects. As examples of the former, lack of clarity about what constitutes "waste" of government resources may support an overly narrow, cost-benefit approach to oversight of agency activities, and lack of clarity about accountability structures for IGs themselves may create incentives for IGs to align their activities with the policy preferences of the incumbent administration rather than serving as independent watchdogs. As an example of the latter, well-intentioned reporting and documentation rules can, in aggregate, impose significant demands on agency employees.

As recent events involving the Department of Government Efficiency (DOGE) have demonstrated, moreover, the prospect of post hoc investigations by inspectors general may not deter important categories of violations that involve subversion of government systems and/or unauthorized transfers of government data. To detect and, hopefully, guard against such violations in something more closely approximating real time, it's necessary to monitor the activities of those who maintain (and, sometimes, destroy or undermine the reliability of) government systems and data. (IGs have some ex ante monitoring authority with respect to the administration of programs now, but the extent to which such authority encompasses uses and abuses of government technology and data more specifically is unclear.[54])

Additionally, oversight authority for IG operations is vested in the Council of Inspectors General on Integrity and Efficiency (CIGIE), which has been chaired by the deputy director for management of OMB. Although IGs work with considerable independence, this structure vests some policy authority in the executive. More generally, although this dotted line arrangement (which also exists for agency CIOs and agency CPOs) was initially intended to open lines of communication to OMB for employees charged with important operational functions, we think it has come to produce a level of operational centralization in OMB that is unwise. As we noted in our report on "Provisioning Digital Tools and Systems for Government Use," we see a benefit to delineating a clearer separation of other such operational functions away from OMB and the policy priorities of the incumbent administration. One possibility is to situate oversight authority in Congress, perhaps by supplementing the powers now enjoyed by the General Accounting Office or creating a separate body that operates in parallel with the GAO. We think, however, that Congress may be an insufficiently forceful check on executive overreach, and that an independent agency exercising countervailing networked management authority to that asserted by OMB may prove relatively more effective.[55]

To address these problems, we recommend reconfiguring the existing IG system around a new independent agency–a "hub" designed to: move oversight out of OMB; extend the capabilities of the existing IG system

54 *See* 5 U.S.C. § 406.

55 On the relative inefficacy of Congress as a check, see Jason Marisam, *DOGE's Matrix Structure and Presidential Power,* 64 U. Louisville L. Rev. 77 (2025).

to encompass uses and misuses of technical systems and data; and develop and support best practices for accountability reporting that work to detach accountability from cost-benefit ideology and (insofar as possible) to minimize cumulative demands on employee time and attention. Under the system we envision, agency IGs would remain in place, but the CIGIE would be moved out of OMB, relocated within the new agency, and chaired by a senior employee of the new agency who is not a political appointee. For ease of reference, we'll refer to the new agency as the Office of Government Integrity (OGI).

We have twice before recommended other hubs: (1) A Digital Architectures, Systems, and Platforms Oversight Board (DASPOB) charged with developing standards for regulatory monitoring of information-economy activities, including especially those performed by digital platforms, and releasing data to the public, and (2) a Department of Technology charged with supporting the development and, where necessary, the procurement of digital tools and systems for government use. As with those two recommendations, we aim to strike a balance. On one hand, it is important to build on carefully developed specialization and expertise. On the other, it is equally important to understand that many of the problems we are currently confronting require new thinking about building and implementing cross-agency capabilities.

The Office of Government Integrity proposed here will complement the other two hubs and the existing system of IGs in two specific ways. The first relates to mandate. As under the current IG system, the OGI will be empowered to ferret out waste, fraud, and abuse of government technical resources. Beyond that, it will be expressly directed to ferret out configurations of government networks, systems, or data that might be used (or are being used) to: shelter unlawful government conduct; frustrate oversight of government activities; invade civil rights and civil liberties; concentrate undue power in any single part of the executive branch; or facilitate unsanctioned third party access to government networks, systems, or data. The second relates to capabilities. The OGI will extend the technical monitoring and auditing capabilities of the DASPOB from the private to the public sector. It will also complement the provisioning-related capabilities of the Department of Technology by providing a different type of ongoing oversight.

To some extent, the OGI should have powers analogous to those that IGs currently enjoy to inspect and monitor the activities of executive branch agencies and independent agencies. For example, it will need the authority to compel the production of documents and testimony from agency leadership and staff.[56]

In other cases, however, the OGI's powers must be tailored–and in some cases expressly restricted–to guard against some accountability threats that the new agency might otherwise create by its own actions. Necessarily, the OGI will require certain kinds of direct access to the computer networks, systems, and data of executive branch and independent agencies. It will require a new suite of authorities and related capabilities directed toward detecting and flagging misuse of government systems and data. It should be authorized to employ a red-team methodology, meaning it will be charged with using its powerful toolkit to propose and test hypotheses, probe weaknesses, and stress test the technical and data-related operations of other agencies against both external and internal threats to their operational integrity.

At the same time, to address the potential for abuse, four kinds of limits are necessary and should be viewed as non-negotiable. First, although OGI investigators and other OGI officials should be able to understand who accessed and used the personal data of citizens, and for what purposes, they themselves should have no direct access to the personal data of citizens. Here we borrow from the computer security principle of least privilege

56 *See, e.g.*, 5 U.S.C. § 406(a) (empowering IGs to, *inter alia*, access documents, subpoena records, take sworn statements, and interview agency officials and employees).

(the idea that users should be given the minimum amount of access they need to accomplish a task and no more)–and more generally from the fair information practice principles of data minimization, purpose specification, and use limitation found in the current Privacy Act. Second, and again borrowing from the principle of least privilege, the OGI's access to all other systems should be read-only. Third, data exfiltration by OGI investigators or other OGI officials should be expressly prohibited, and intentional violations should be subject to criminal sanctions. Fourth, all actions by the OGI must be tracked in immutable audit logs and reported regularly to a standing legislative committee.

Finally, like IGs under the current system, the OGI will have great power to scrutinize the inner workings and nascent plans of other agencies but no authority to command or obstruct the work of those agencies. Its main power will be to bring worrisome activities, strategies, or impacts to Congress's and the public's attention. It will have no authority to block or reshape the activities it finds objectionable–and the access limits described in the previous paragraph are intended to constrain its ability to take more direct forms of action. It will be charged with identifying the risks raised by objectionable or illegal practices, assessing their imminence, tailoring its alerts according to such assessments, and report regularly to the White House and Congress. For the most egregious or the most irreversible misconduct (for example, if it detects that another agency is exfiltrating government data to share with a private company or foreign adversary), it will be obligated to report immediately to the White House, Congress, and the public.

Conclusion

A fundamental premise of the Redesigning the Governance Stack Project has been that administrative institutions must undergo redesign if they are to keep pace with changes in political economy more generally. Like our other reports, this report has focused on the design of mechanisms and institutional arrangements–in this case, for ensuring legitimacy and accountability in administrative governance. We have argued, however, that basic narratives about what makes administrative institutions legitimate and accountable modes of governance also require some rethinking if the overall project of institutional redesign is to succeed.

Bibliography

Legitimacy, Accountability, and Administrative Governance

Nicholas Bagley, *The Procedure Fetish*, 118 Mich. L. Rev. 345 (2019).

Nicholas Bagley, *The Puzzling Presumption of Reviewability*, 127 Harv. L. Rev. 1285 (2015).

Blake Emerson, *Liberty and Democracy Through the Administrative State: A Critique of the Roberts Court's Political Theory*, 73 Hastings L.J. 371 (2022).

Karen E.C. Levy & David Merritt Johns, *When Open Data is a Trojan Horse: The Weaponization of Transparency in Science and Governance*, 3 Big Data & Soc'y 1 (2016).

K. Sabeel Rahman, *Anti-Domination and Administration*, 100 N.Y.U. L. Rev. 1984 (2025).

Noah Rosenblum, *What We Talk About When We Talk About the Rule of Law in the Administrative State*, 16 N.Y.U J. L. & Liberty 467 (2023).

Edward L. Rubin, Lecture, *Responsive Democracy and the Administrative State*, 75 Case W. Rsrv. L. Rev. 929 (2025).

Gabriel Scheffler & Daniel E. Walters, *The Submerged Administrative State*, 2024 Wisc. L. Rev. 789 (2024).

Automated Decisionmaking and Administrative Governance

Lorin Brennan, *AI Ethical Compliance is Undecidable*, 14 Hastings Sci. & Tech. L.J. 311 (2023).

Jenna Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, 3 Big Data & Soc'y 1 (2016).

Danielle K. Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249 (2008).

Cary Coglianese, A Framework for Governmental Use of Machine Learning, Report for the Administrative Conference of the United States (2020).

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

Wendy Currie et al., *Rethinking Technology Regulation in the Age of AI Risks*, 40 J. Info. Tech. 236 (2025).

David Freeman Engstrom & Daniel E. Ho, *Algorithmic Accountability in the Administrative State*, 37 Yale J. on Reg. 800 (2020).

Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability,* 92 S. Cal. L. Rev. 1529 (2019).

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

Recentering Moral Values in Administrative Governance

Blake Emerson, *Public Care in Public Law: Structure, Procedure, and Purpose*, 16 Harv. L. & Pol'y Rev. 35 (2021).

Cristie Ford, *Regulation as Respect*, 86 L. & Contemp. Probs. 133 (2023).

Chris Havasy, *Relational Fairness in the Administrative State,* 109 Va. L. Rev. 749 (2023).

Sofia Ranchordas, *Empathy in the Automated Administrative State,* 71 Duke L. J. 1341 (2022).

Jodi Short, *The Moral Turn in Administrative Law*, Ind. L. J. (forthcoming 2026), https://ssrn.com/abstract=4909394.

The Many Dimensions of Institutional Capacity

Hilary J. Allen, *Putting the Financial Stability in Financial Stability Oversight Council*, 76 Ohio St. L. J. 1087 (2015).

Hilary J. Allen, *Regulatory Managerialism and Inaction: A Case Study of Bank Regulation and Climate Change*, 86 L. & Contemp. Probs. 71 (2023).

Elizabeth Fisher & Sidney A. Shapiro, Administrative Competence: Reimagining Administrative Law 35-65 (2020).

Catherine L. Fisk, *Democracy and a Nonpartisan Civil Service*, 67 Ariz. L. Rev. 629 (2025).

Margaret B. Kwoka, *The Anti-Managerial Information Commission,* 86 L. & Contemp. Probs. 197 (2023).

Jason Marisam, *DOGE's Matrix Structure and Presidential Power*, 64 U. Louisville L. Rev. 77 (2025).

Jerry L. Mashaw, Bureaucratic Justice (1983).

Jerry L. Mashaw, *Accountability and Institutional Design: Some Thoughts on the Grammar of Governance,* in Public Accountability: Designs, Dilemmas and Experiences 115 (Michael W. Dowdle ed., 2006).

Gillian E. Metzger & Kevin M. Stack, *Internal Administrative Law*, 115 Mich. L. Rev. 1239 (2017).

Frank Pasquale, *Power and Knowledge in Policy Evaluation: From Managing Budgets to Analyzing Scenarios*, 86 L. & Contemp. Probs. 39 (2023).

Noah Rosenblum, *Toward a Realist Defense of the Civil Service*, 13 Reg. Rev. Depth 7 (2024).

Rory Van Loo, *Stress Testing Governance,* 75 Vand. L. Rev. 553 (2023).

Daniel E. Walters, *Communicative Administration: The Administrative State Beyond Legal Administration*, 78 Stan L. Rev. (forthcoming 2026), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5376707.

Harlan Yu & David G. Robinson, *The New Ambiguity of Open Government*, 59 UCLA L. Rev. Discourse 178 (2011).

ITT REDESIGNING THE GOVERNANCE STACK

GEORGETOWN LAW