DATA FEDERALISM

Bridget A. Fahey

CONTENTS

DATA FEDERALISM

Bridget A. Fahey[*]

Private markets for individual data have received significant and sustained attention in recent years. But data markets are not for the private sector alone. In the public sector, the federal government, states, and cities gather data no less intimate and on a scale no less profound. And our governments have realized what corporations have: It is often easier to obtain data about their constituents from one another than to collect it directly. As in the private sector, these exchanges have multiplied the data available to every level of government for a wide range of purposes, complicated data governance, and created a new source of power, leverage, and currency between governments.

This Article provides an account of this vast and rapidly expanding intergovernmental marketplace in individual data. In areas ranging from policing and national security to immigration and public benefits to election management and public health, our governments exchange data both by engaging in individual transactions and by establishing "data pools" to aggregate the information they each have and diffuse access across governments. Understanding the breadth of this distinctly modern practice of data federalism has descriptive, doctrinal, and normative implications.

In contrast to conventional cooperative federalism programs, Congress has largely declined to structure and regulate intergovernmental data exchange. And in Congress's absence, our governments have developed unorthodox cross-governmental administrative institutions to manage data flows and oversee data pools, and these sprawling, unwieldy institutions are as important as the usual cooperative initiatives to which federalism scholarship typically attends.

Data exchanges can also go wrong, and courts are not prepared to navigate the ways that data is both at risk of being commandeered and ripe for use as coercive leverage. I argue that these constitutional doctrines can and should be adapted to police the exchange of data. I finally place data federalism in normative frame and argue that data is a form of governmental power so unlike the paradigmatic ones our federalism is believed to distribute that it has the potential to unsettle federalism in both function and theory.

INTRODUCTION

The last two decades have witnessed an explosive growth in private markets for individual data. Firms gather more and more data directly from individuals, but they have also developed refined systems to buy and sell data from one other, accelerating aggregation and facilitating the power that comes uniquely from large aggregations of data. But data markets are not for the private sector alone.

[*] Assistant Professor of Law, University of Chicago Law School. I am grateful for exceptional research assistance from Kenny Chiaghana, Charlotte Mostertz, Jasper Primack, Mikaila Smith, and Amber Stewart, and for the care and insight of the editors at the *Harvard Law Review*. Thank you also to Emily Buss, Barry Friedman, Aziz Huq, Alison LaCroix, Genevieve Lakier, Ela Leshem, Jonathan Masur, Richard McAdams, Robert Mikos, David Pozen, David Schleicher, Christopher Slobogin, Lior Strahilevitz, and David Strauss for spirited conversations and thoughtful feedback, and to workshop participants at the University of Chicago, Vanderbilt, and the University of Wisconsin's Public Law in the States Conference. My deepest thanks are, as always, to Alex Hemmer.

In the public sector, the federal government, states, and cities gather data no less intimate and on a scale no less profound, both directly from individuals and, like private firms, indirectly from other levels of government. Our governments, in short, have realized what corporations have: It is often easier to obtain data about their constituents in compilations ready made than it is to collect it piecemeal from those people themselves. As in the private sector, these exchanges have multiplied the data available to every level of government for a wide range of purposes, created a new source of leverage and tension between levels of government, and deeply complicated data use and governance.

This Article exposes this substantial and rapidly expanding intergovernmental marketplace in individual data.[1] In sectors ranging from policing, immigration, and national security to employment and social services to public health, our levels of government have dramatically expanded their capacity to acquire and use personal data collected (frequently for different purposes) by their sister governments. They buy or trade for discrete datasets in one-off transactions; they exchange data on a recurrent or annual basis in repeat transactions; and they erect programs to continuously pool data and make it available to officials at all levels of government at any time. Data increasingly sits at the heart of the most significant collaborations — and most significant disputes — between the federal government, states, and cities.

These cross-governmental data exchanges — and their diffusion of information about the wages we earn, the illnesses we contract, and our interactions small and large with government officials — hold far-reaching significance for both privacy and federalism. The basic importance of these transfers for privacy is apparent: The easy movement of data between governments propels its aggregation and expands the knowledge each government has about our lives. Intergovernmental data markets, however, introduce unique privacy risks that reach beyond mere aggregation. In this system, data collected by one government is often used by another and, contrary to widely accepted fair information principles, without notice to the data subject and for uses that diverge from those that justified its initial collection.[2] When data moves

---

[1] My focus here is *personal identifying information*, which can include a person's name, address, phone number, and physical description; employment information, Social Security number, wages, and licenses; and biometric data like fingerprints, photographs, and DNA. *See generally* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011). I use the terms *data*, *information*, and *personal data* as shorthand for this kind of personal information.

[2] For influential articulations of these principles, see, for example, ORG. FOR ECON. CO-OPERATION & DEV., THE OECD PRIVACY FRAMEWORK 14 (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [https://perma.cc/27NH-F5NY], describing the "collection limitation" and "purpose specification" principles, and U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS xx–xxi (1973) (similar).

across governmental boundaries, moreover, access proliferates and multiplies opportunities for insecurity and misuse. One government's conscientious data collection policy, meanwhile, can easily be compromised by data exchanges that, as is commonly the case, impose inadequate restrictions on the recipient government — as when data collected by a friendly city about its immigrant members to administer public benefits is ultimately used by federal officials to enforce immigration laws. Likewise, one government's flawed data collection can be easily amplified by data exchanges — as when a city that disproportionately polices a minority population infuses its biased data into a cross-governmental database. These transactions, in short, add a federalism inflection to government data collection, use, and management that has been largely overlooked in the privacy literature.

But the widespread growth of intergovernmental data exchange is no less consequential for federalism. As this Article will argue, we have incompletely understood a significant number of contemporary federalism projects and disputes because we have missed a common thread: that they are, at their core, about *data*. Because our paradigms for understanding federalism are intimately tied to the types of power we assume our federalist system to be distributing and balancing between levels of government — and because data functions differently than the forms of power conventionally believed to be so disbursed — recognizing the centrality of data power to current federalism interactions has significant descriptive, doctrinal, and normative implications.[3] Data programs are also, for reasons I develop, frequently shielded not just from public view, but also from scholarly critique.

---

[3] This Article thus intervenes in several ongoing conversations. It builds on a growing federalism literature that considers how intergovernmental interactions have evolved in practice in order to reevaluate the values that federalism advances in theory. *See* sources cited *infra* note 26. Just as data has transformed private markets, I argue, it has intimately shaped interactions between governments, often in unexpected ways, and our understanding of federalism is incomplete without it. Professor Robert Mikos is one of the few scholars to have observed a connection between data and federalism, identifying efforts by the federal government to mandate state data sharing. *See generally* Robert A. Mikos, *Can the States Keep Secrets from the Federal Government?*, 161 U. PA. L. REV. 103 (2012). I widen the lens to show that those mandates exist against a vast backdrop of *voluntary* data sharing and data pooling, which reveals a more institutionally, legally, and theoretically complex drive to aggregate data across governments and contextualizes the comparatively unusual efforts to obtain data by mandate. Finally, there are also specialized literatures about some of the policy programs that have resulted from the data exchanges I discuss here, most prominently about the national security and privacy consequences of "fusion centers." *See generally* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721 (2014); Matthew C. Waxman, *National Security Federalism in the Age of Terror*, 64 STAN. L. REV. 289 (2012). My goal is not to evaluate the merits of any individual data sharing policy program, but instead to develop an understanding of the institutional structures that govern data programs across sectors and provide needed perspective on the unseen terrain in which decisions to pursue data policies are made and influenced.

The story, though, begins with data's unnoticed presence at the heart of a staggering number of federal-state interactions, as a quick review of front-page federalism news reveals. From President Trump's effort to aggregate state voting data to "investigat[e] voter fraud";[4] to the development of facial recognition technology using hundreds of millions of state DMV photographs;[5] to the Census Bureau's attempt to circumvent the Supreme Court's decision prohibiting it from asking about immigration status on the census questionnaire by seeking the same information from states and cities;[6] to the tit-for-tat skirmish between the Trump Administration and then–Governor of New York Andrew Cuomo over the state's participation in the Global Entry Program;[7] to the states withholding vaccination information because of skepticism about how the federal government will handle it,[8] data is the common thread — and it is both a spur to collaboration and a source of considerable tension.

In perhaps no area is this more true than in the immigration context, where the federal government has for decades made the acquisition of data about noncitizens from state and local law enforcement a centerpiece of its immigration enforcement strategy. A cornerstone of President Obama's immigration policy, the controversial Secure Communities program, sought biometric data on immigrant arrestees from cities and states in exchange for federal policy commitments. When the federal government reneged on the deal, opting to simply requisition state data without recompense, cities and states accused the Administration of unlawful commandeering.[9] And the recently concluded "sanctuary city" litigation that pit immigrant-friendly localities against federal immigration officials was centrally about a federal law

---

[4] *See* Michael Tackett & Michael Wines, *Trump Shutters His Commission on Voter Fraud*, N.Y. TIMES, Jan. 4, 2018, at A1.

[5] *See* Drew Harwell, *FBI, ICE Tap into License Photos*, WASH. POST, July 8, 2019, at A1.

[6] *See* Trevor Hughes, *Trump, Census Bureau Collect Driver's License Data to Check Citizenship Status of Americans*, USA TODAY (July 16, 2020, 2:07 PM), https://www.usatoday.com/story/news/nation/2020/07/16/trump-seeks-drivers-license-data-iowa-sc-check-citizenship/5445492002 [https://perma.cc/PW2X-PQGA]; Kim Norvell, *Iowa to Share Driver's License Data to Help Feds Determine Citizenship*, DES MOINES REG. (July 16, 2020, 2:05 PM), https://www.desmoinesregister.com/story/news/2020/07/15/iowa-shares-drivers-license-data-census-bureau-find-citizenship-status/5445010002 [https://perma.cc/F3T5-HYQJ].

[7] *See* Jesse McKinley, Zolan Kanno-Youngs & Annie Correal, *New York Law on Immigrants Spurs Reprisal*, N.Y. TIMES, Feb. 7, 2020, at A1.

[8] *See* Akilah Johnson, *Race Data Lacking Amid Rollout*, WASH. POST, Feb. 2, 2021, at A1, A5; Sheryl Gay Stolberg, *States Balk at Vaccine Rule on Personal Data*, N.Y. TIMES, Dec. 9, 2020, at A10.

[9] *See infra* p. 1027. In its first three years, the reach of Secure Communities was vast: State and local governments shared over 11 million fingerprints with federal officials, which led to the removal of over 142,000 people. U.S. IMMIGR. & CUSTOMS ENF'T, SECURE COMMUNITIES: IDENT/IAFIS INTEROPERABILITY 2 (2011), https://www.ice.gov/doclib/foia/sc-stats/nationwide_interoperability_stats-fy2011-to-date.pdf [https://perma.cc/P2BF-R7S3].

that forces cities and states to surrender the data they gather about their residents to federal officials.[10]

But as in private-sector markets, this Article argues, most data exchange between governments never makes front-page news or sees the inside of a courthouse. Most of the data our governments trade is uncontroversial — *too* uncontroversial. Our governments have developed complex systems, often outside public view, for transferring their data to one another and aggregating it for their joint use. Because we have not noticed that data moves so easily between governments, we have likewise not seen the parallels in efforts across policy areas to form what I call "data pools." Although federalism traditionally divides power between governments, these data pools aggregate power and diffuse access.

Data pooling occurs in many policy areas. Against a chorus of calls in the summer of 2020 to reduce funding to the police, the public paid far less attention to another intergovernmental source of police power: their data. The National Crime Information Center (NCIC) and its network of linked databases is a massive effort to aggregate federal, state, and local data on arrests, fingerprints, and criminal history.[11] Nor are most Americans aware that their wage history, employment status, and biographical data are shared by states with the federal government and pooled in the National Directory of New Hires.[12] Or that "fusion centers" — institutions that gain legal authority from an amalgamation of federal and state sources — were erected throughout the country after 9/11 to improve terrorism-related information sharing, but now have remits that extend far beyond national security.[13] Of particular interest in the wake of the COVID-19 pandemic, data pooling is essential to the disease surveillance system run by the CDC — a system that operates with minimal statutory oversight and gathers a mishmash of diagnoses from thousands of local health departments.[14] Using previously uncompiled legal documents from a range of governmental institutions, Part I provides an account of the types and forms of these data programs.[15]

---

[10] *See* sources cited *infra* notes 84–85, 255 and accompanying text.

[11] *See infra* pp. 1022–23.

[12] *See infra* pp. 1021–22.

[13] *See infra* pp. 1024–25.

[14] *See infra* note 53 and accompanying text.

[15] There are no broadscale disclosure rules that require federal or state agencies to make public the information necessary to understand the scale of data sharing or how data sharing functions. Most of the sources on which I rely are not readily made public by their authoring governments, and those that are frequently speak only incidentally to data sharing. For instance, although disclosures related to data sharing are not formally required, federal agencies often reveal clues about data sharing programs incidentally in the "systems of records notices" and Privacy Impact Assessments mandated for other purposes by the Privacy Act of 1974. *See infra* notes 125–126 and accompanying text. Some documents, especially those related to data sharing programs that vary

The scale of intergovernmental data exchange alone makes its practices worth excavating. But appreciating how our governments come to possess their data is also, I argue, key to understanding how that data is regulated and even what institutions make those regulatory decisions. Part II turns to the unorthodox law and policymaking processes that facilitate data exchange and, in turn, establish the rules that govern our data.

Programs that are jointly administered by federal and state governments can have significant institutional complexity, but we can at least begin to understand their contours by consulting the often sweeping federal statutes that initiate them. Because the federal government substantially funds many joint initiatives and can preempt conflicting state policy, Congress assumes a role as federalism's first among equals, sketching the outlines of joint programs in the first instance and deciding the terms on which states can enlist. So central is Congress's role in structuring conventional federal-state projects that Professor Abbe Gluck has urged us to see state power in our system of government coming not by constitutional right, but "by grace of Congress."[16]

But the reasons for Congress's central role in so many other federal-state initiatives are diminished in the data context. Data — and the power that derives from it — does not originate in Congress. It is gathered diffusely, by institutions across every level of government. The states and federal government thus engage on more level terrain when initiating and designing joint data programs. Nor do we have a tradition of conceptualizing intergovernmental data sharing as the surrender of a vital governmental asset, which would subject it to the kind of strict alienation controls that require legislative involvement — like those on public funds, which must be legislatively appropriated, and public lands, which can be surrendered only by specific authorization.[17]

Data sharing, I show, happens in a field of striking legislative minimalism. Data exchanges are rarely detailed in congressional legislation; indeed, some appear to occur without any statutory authorization at all. Even the federal government's comprehensive privacy statutes, which could in principle restrain the dispersion or use of data, either directly

---

from state to state, like fusion centers, are disclosed in ways that could charitably be described as haphazard. In developing this narrative, I have thus relied on documents that range from ordinary statutes and regulations; to documents that are voluntarily disclosed but in nonstandardized ways; to documents disclosed only under order of civil discovery in lawsuits brought by private litigants; to documents provided in response to FOIA requests submitted by me and by other researchers.

[16] Abbe R. Gluck, *Intrastatutory Federalism and Statutory Interpretation: State Implementation of Federal Law in Health Reform and Beyond*, 121 YALE L.J. 534, 542 (2011).

[17] *See* U.S. CONST. art. I, § 9, cl. 7 ("No Money shall be drawn from the Treasury, but in Consequence of Appropriations made by Law . . . ."); *id.* § 8, cl. 17 (describing Congress's power "To exercise exclusive Legislation . . . over all Places purchased by the Consent of the Legislature of the State in which the Same shall be, for the Erection of Forts, Magazines, Arsenals, dock-Yards, and other needful Buildings"); *id.* art. IV, § 3, cl. 2 ("The Congress shall have Power to dispose of and make all needful Rules and Regulations respecting the Territory or other Property belonging to the United States . . . .").

or by operation exempt intergovernmental data exchange from their portfolio of constraints.

In Congress's absence — and without the coordinating effect of major federal legislation — the decisions our governments make to share data, the use and privacy restrictions they place on it, and the institutions they erect to govern data pools have arisen organically (though not necessarily thoughtfully, equitably, or democratically) through negotiation between governments, instead of through delegation from the top. Federal-state data collaborations are largely a form of federalism that, contrary to the usual trend, occurs *outside Congress*.

That does not mean they exist without law. I show that the rules governing data exchanges are set out in conceptually challenging legal devices that I have elsewhere called "intergovernmental agreements" — a kind of domestic treaty between the federal government and states or cities.[18] But intergovernmental agreements are only the beginning. Where data exchange becomes regularized into routine flows or permanent data pools, our governments have collaborated to craft bespoke administrative structures to oversee them — structures I call "cross-governmental bureaucracies." These range from the formally chartered to the highly informal, are neither wholly federal nor wholly state in legal character, and are not fully domesticated by either federal or state law. They exist instead in a kind of interstitial space between and across governments that bends our conventional federalism paradigms.[19] Only by beginning to untangle the legal and institutional dynamics in these interstitial spaces can we know how decisions about our data are made and how to affect them.[20]

But data exchanges and data pooling can also go wrong, just like any other effort at intergovernmental engagement. Part III explores how federalism doctrine should apply to data transactions. When the federal government and the states form joint initiatives, three doctrines comprise their basic "rules of engagement": the anti-commandeering rule

---

[18] Bridget A. Fahey, *Federalism by Contract*, 129 YALE L.J. 2326, 2329 (2020).

[19] Writing about federalism tends to assume that the states and federal government either govern separately or participate in joint projects as institutionally distinct parties. "Cooperative federalism," in this frame, describes projects in which the federal government and state governments direct their separate governing apparatuses toward common goals. The cross-governmental bureaucracies that manage data, however, merge together state and federal legal authority, law- and policymaking processes, and even administrative structures into institutions distinct from both federal and state apparatuses. These interstitial institutions raise a new kind of federalism problem: one that arises when our governments do not just direct their existing institutions toward common ends, but craft new institutions that confound the federal-state distinctions that are our system's bedrock.

[20] In the future, then, we can elevate data programs like the NCIC — the biggest coordinated federalism program that federalism scholars never discuss — to their rightful place alongside other complex federal-state governing initiatives and include the analysis of interstitial spaces alongside analyses of other forms of federal-state coordination.

prohibits the federal government from mandating state participation; the anti-coercion rule prohibits it from coercing their participation; and the *Pennhurst*[21] clear statement rule requires that conditions of federal grant funds be clearly stated.

These doctrines, however, arose in contexts in which our governments were joining together, trading, and leveraging governmental powers more conventional than data. The anti-commandeering rule, for instance, turned back the federal government's effort to force states to "enact or administer a federal regulatory program" — to effectively requisition their *administrative* and *regulatory* power by mandating its application to federal ends.[22] The anti-coercion rule most famously prevented the federal government from inducing states to participate in a new grant program by threatening to withdraw far larger funds from an existing program — from flexing its *monetary* power to coerce state involvement.[23] And the *Pennhurst* clear statement rule has, likewise, only ever been invoked to police the conditions placed on federal grant monies.

But the federal government has sought to commandeer state data, as the "sanctuary city" litigation highlights; it has leveraged data to coerce state participation in ostensibly voluntary programs, in ways that mirror its use of money to the same ends; and it has hidden implied terms in the documents that memorialize federal-state data initiatives in just the way that *Pennhurst* prohibits for federal-state grant programs. Courts have yet to recognize, as a general matter, that the forms of power our governments seek and trade in joint initiatives are evolving, but the constitutional principles these rules enact are, I argue, conceptually adaptable to that evolution, at least as it applies to data. Data federalism, however, also provides impetus to reflect on the limits of existing constitutional doctrine to confront the full set of structural problems cross-governmental coordination can raise.

Finally, as I discuss in Part IV, intergovernmental data exchange has important implications for how we theorize today's federalism — as it relates to data and beyond. Federalism is a system of governance that divides power, but most doctrine and some academic commentary still assume that power allocation to be fixed by the Constitution. And even the scholars who have emphasized that the power distribution in our system is negotiated rather than fixed have focused on intergovernmental transfers of a small set of conventional governmental powers — money, regulatory authority, and administrative capacity.[24] The widespread exchange of another form of power, data, shows that power in a federalist system is doubly dynamic: both its *distribution* and its *forms*

---

[21] Pennhurst State Sch. & Hosp. v. Halderman, 451 U.S. 1, 17 (1981).

[22] Printz v. United States, 521 U.S. 898, 926 (1997) (quoting New York v. United States, 505 U.S. 144, 188 (1992)).

[23] *See* NFIB v. Sebelius, 567 U.S. 519, 580 (2012).

[24] *See infra* note 292.

change over time. Each form of power, in turn, will have its own interplay with the federal-state dynamic.

Data, for instance, has unique properties that invert some of the core assumptions about how federalism affects the distribution of power. In contrast to money — perhaps the most frequently transacted form of governmental power in our system — data is nonrival and can be accessed by any number of users without being diminished. When governments share data, they also retain access. Transactions in data thus do not relocate power from one government to another, but instead *duplicate* the power of one government in another — making federalism, in this context, a power multiplier rather than a power divider. I canvass how this and other unique features of data complicate our assumptions about how federalism works.

But data exchange has other implications for contemporary federalism theory. The fact that, as the Article shows, data exchange, pooling, use, and governance largely happen outside Congress and in federalism's interstitial spaces does not just challenge the dominant understanding of how intergovernmental collaborations come to life; it also complicates how those collaborations gain legitimacy, are subjected to legal constraint, and advance democratic norms. And although data federalism strikes a contrast to the usual cooperative federalism programs structured by detailed federal statutes, the issues that arise in data's governance are present in some form even *in* those conventional areas. Congress can address only so many contingencies; our governments collaboratively fill in the rest. Unpacking the stakes of governance in this interstitial space therefore begins to make the institutional control over data more legible and offers a searchlight with which we may notice similar practices elsewhere.

I. THE INTERGOVERNMENTAL DATA MARKET

This Part elaborates the circumstances under which our domestic governments exchange data. The goal is not to offer an exhaustive account, but to provide a picture of the variety, frequency, and significance of intergovernmental data exchange.[25] A small but important federalism literature has framed ordinary "cooperative federalism" programs,

[25] This Part, like the Article generally, focuses on intergovernmental data exchange, not on the government's acquisition of data in the first instance. In particular, the Article does not address the growing practice of governmental acquisition of data from private firms, often without the knowledge of the individuals whose information is conveyed. *See, e.g.*, Laura Hecht-Felella, *Federal Agencies Are Secretly Buying Consumer Data*, BRENNAN CTR. FOR JUST. (Apr. 16, 2021), https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data [https://perma.cc/F9DJ-FQA2]. Although these practices raise profound privacy concerns, my main focus is the institutional and constitutional questions that arise when governmental entities exchange data about their constituents. It is worth noting, however, that the

in which the federal government and states join together their separate resources to achieve common ends, as, in important respects, intergovernmental transactions.[26] Governmental resources are not just combined in the context of these programs; they are also traded. Most commonly, the federal government trades money, typically in the form of grants, for state administrative capacity, which states offer by committing to implement a policy program within federal parameters.[27]

Data transactions can resemble those more conventional, if still understudied, exchanges of governmental goods. Our governments trade data for grant funds, data for policy commitments, and data for administrative capacity. But they also trade data for other data, forming a data pool. In these transactions, which look unlike any other coordinated federalism program, data contributions are the price each government pays for access to a broader multigovernmental data pool.

Regardless of the structure of the intergovernmental transaction, data has distinctive properties as a form of governmental power and resource for intergovernmental trade, which help explain why the trade in governmental data has become so robust, so rapidly. First, data is nonrival.[28] Whereas resources like money and administrative capacity are depleted by use, data can be used and shared without being depleted. Access to data can be multiplied at minimal cost, reducing the barriers to data exchange. Data is also a complementary good — it becomes more valuable as it is aggregated with other specific pieces of data.[29] This helps explain the advent of data pooling programs. Placing data into a common pool, where it can be matched with data gathered by other levels of government about the same person, maximizes the value

---

practices of governmental data exchange can only magnify concerns about governmental acquisition of private data by allowing data obtained by one government to be readily transferred to many others.

[26] *See* Aziz Z. Huq, *The Negotiated Structural Constitution*, 114 COLUM. L. REV. 1595, 1640–42 (2014); Roderick M. Hills, Jr., *The Political Economy of Cooperative Federalism: Why State Autonomy Makes Sense and "Dual Sovereignty" Doesn't*, 96 MICH. L. REV. 813, 817 (1998); *see also* ERIN RYAN, FEDERALISM AND THE TUG OF WAR WITHIN 271 (2011).

[27] *See* Huq, *supra* note 26, at 1642–43; Hills, *supra* note 26, at 858–61; *see also* RYAN, *supra* note 26, at 92.

[28] For a general discussion of this property, see, for example, Charles I. Jones & Christopher Tonetti, *Nonrivalry and the Economics of Data*, 110 AM. ECON. REV. 2819, 2819 (2020), explaining that "data is nonrival," and thus "at a technological level . . . infinitely usable": it "can be used by any number of firms or people simultaneously, without being diminished." One caveat is in order here: whereas each piece of data is itself nonrival, a state's capacity to collect new data is not. Sharing current data stores can certainly reduce the state's ability to gather more data in the future — as when, as Mikos shows, states that share immigration data cause members of the immigrant community to avoid the kinds of interactions with the state that would generate more data going forward. *See* Mikos, *supra* note 3, at 123.

[29] José Parra-Moyano, Karl Schmedders & Alex Pentland, *Shared Data: Backbone of a New Knowledge Economy*, *in* BUILDING THE NEW ECONOMY: DATA AS CAPITAL 35, 38 (Alex Pentland, Alexander Lipton & Thomas Hardjono eds., 2021).

of each piece of data relative to simply trading data in distinct sets. Finally, data is nonfungible, and governments often seek to expand data supplies not because they lack for data generally but because they need more specific data about more specific people or problems.[30]

Because data transactions are generally not structured by Congress, searching for these programs in the U.S. Code alone would not reveal the full scope of this market. This account thus draws on a range of legal sources, from statutes and regulations to intergovernmental agreements, to letters between governments and grant documents. Data, it shows, is a mobile source of governmental power around which our domestic governments have developed complex and novel forms of intergovernmental exchange.

A. Discrete Transactions

Some intergovernmental data transactions are discrete. They are much more like a simple exchange of goods than the broadscale data pooling programs discussed below. They can be very narrow, limited to information about just one person or event, as when federal and state law enforcement agents agree to share data they gather about a target being investigated for both federal and state crimes.[31] Or they can stretch more broadly, encompassing information about a set of activities or group of people, as when state and federal police departments form joint policing task forces to collaboratively investigate an area of criminal activity (drug-, firearm-, and terrorism-related crimes are the most common) and share their corresponding information.[32]

But discrete data exchanges are not always modest in scope. Two recent federal requests for state data had a breathtaking sweep. In 2017, President Trump inaugurated a "Presidential Advisory Commission on Election Integrity," with a mandate to investigate voter fraud by assessing, among other things, instances of improper registration and double voting.[33] Because the states administer federal elections, the Commission sought vast stores of state registration and voting data, including each registrant's first and last name, address, date of birth, political affiliation, voting history, and the last four digits of their social

---

[30] *Cf. id.* at 37.

[31] Indeed, while under J. Edgar Hoover's stewardship, the FBI used monetary incentives for individual police officers to encourage this kind of targeted information exchange. Daniel Richman, *The Past, Present, and Future of Violent Crime Federalism*, 34 CRIME & JUST. 377, 388 (2006).

[32] *See, e.g.*, Fahey, *supra* note 18, at 2346 (describing task forces); Program-Funded State and Local Task Force Agreement Between Drug Enf't Admin. and Tempe Police Dep't 1 (Sept. 30, 2013), http://documents.tempe.gov/sirepub/view.aspx?cabinet=published_meetings&fileid=172021 66 [https://perma.cc/V4L9-BDPF] (describing goal of task force to "gather and report intelligence data relating to trafficking in narcotics and dangerous drugs").

[33] Exec. Order No. 13,799, 82 Fed. Reg. 22,389, 22,389 (May 11, 2017).

security number.[34] The Commission requested data covering every registered voter — an estimated 200 million people.[35] The Commission was ultimately disbanded when states refused — as is their constitutional entitlement, as I argue in Part III — to supply the requested data.[36]

In the lead-up to the 2020 Decennial Census, the Department of Commerce, which oversees the Census Bureau, announced its intention to disaggregate its population count according to citizenship status.[37] One express goal, President Trump explained in a memorandum, was to exclude noncitizens from the constitutionally required count of "persons" used to apportion seats in the House of Representatives.[38] To count the number of citizens and noncitizens, the Bureau initially sought to add a citizenship question to its flagship Census Questionnaire, distributed to households across the country.[39] After the Supreme Court effectively blocked that effort, President Trump issued an Executive Order instructing the Department of Commerce to gather granular citizenship data through state and federal "administrative records" — general data used for other purposes across governments.[40] To meet that directive, the Census Bureau requested sweeping access to state DMV records, including, for each person in the database, "name, address, date of birth, sex, race, eye color[,] and citizenship status."[41] Like the ill-fated Election Commission, the Census Bureau's efforts met resistance from

---

[34] *See, e.g.*, Letter from Kris W. Kobach, Vice Chair, Presidential Advisory Comm'n on Election Integrity, to Kim Wyman, Wash. Sec'y of State 1–2 (June 28, 2017), https://www.sos.wa.gov/_assets/office/peic-letter-to-washington.pdf [https://perma.cc/K5M3-WXPU]. Letters to all fifty states are on file with the author.

[35] Michael Wines & Rachel Shorey, *Even Some Republicans Balk at Trump's Voter Data Request. Why the Uproar?*, N.Y. TIMES (July 7, 2017), https://www.nytimes.com/2017/07/07/us/politics/voter-fraud-commission.html [https://perma.cc/5CZ4-5J3Z].

[36] *See* Jessica Taylor, *Trump Dissolves Controversial Election Commission*, NPR (Jan. 3, 2018, 8:06 PM), https://www.npr.org/2018/01/03/575524512/trump-dissolves-controversial-election-commission [https://perma.cc/GJZ2-XRUU].

[37] Emily Baumgaertner, *Despite Concerns, Census Will Ask Respondents if They Are U.S. Citizens*, N.Y. TIMES (Mar. 26, 2018), https://www.nytimes.com/2018/03/26/us/politics/census-citizenship-question-trump.html [https://perma.cc/Y48Z-8ETX].

[38] Excluding Illegal Aliens from the Apportionment Base Following the 2020 Census, 85 Fed. Reg. 44,679, 44,679 (July 21, 2020).

[39] Dep't of Com. v. New York, 139 S. Ct. 2551, 2562 (2019).

[40] Exec. Order No. 13,880, 84 Fed. Reg. 33,821, 33,821 (July 11, 2019).

[41] Tara Bahrampour, *Census Bureau's Request for Citizenship Data from DMVs Raises Privacy, Accuracy Concerns*, WASH. POST (Oct. 17, 2019), https://www.washingtonpost.com/local/social-issues/census-bureaus-request-for-citizenship-data-from-dmvs-raises-privacy-accuracy-concerns/2019/10/17/aa8771f2-f114-11e9-89eb-ec56cd414732_story.html [https://perma.cc/PUF7-MG5U]; *see also* Press Release, U.S. Census Bureau, U.S. Census Bureau Statement on State Data Sharing Agreements (Oct. 15, 2019), https://www.census.gov/newsroom/press-releases/2019/state-data-sharing-agreements.html [https://perma.cc/3FDF-ZZJJ]. In making the request, the Bureau was exercising its broad statutory authority, delegated by the Secretary of Commerce, to "acquire, by purchase or otherwise, from States" information required for the census. 13 U.S.C. § 6(b).

some states, which expressed skepticism about such a large-scale transfer of a sensitive state database.[42]

B. Repeat Transactions

Data exchange in repeat transactions has also reached an eye-popping scale. In virtually every ongoing federal-state policy program — from large-scale ones like Medicaid, supplemental nutrition assistance, and housing support, to smaller, targeted initiatives — data exchange is embedded in the program's design and participation is often predicated on a state's willingness to contribute program-relevant data. This data facilitates eligibility determinations,[43] the distribution of federal funds,[44] financial auditing,[45] and enforcement of the contract-like commitments that legally structure cross-governmental programs. Some federal programs also encourage or mandate *intra*state information sharing between two separate federal-state programs as a condition of participation.[46]

---

[42] Bahrampour, *supra* note 41.

[43] For instance, state and local housing agencies share information about recipients of low-income housing benefits with the federal government. *See, e.g.*, OFF. OF HOUS., U.S. DEP'T OF HOUS. & URB. DEV., TENANT RENTAL ASSISTANCE CERTIFICATION SYSTEM (TRACS): PRIVACY IMPACT ASSESSMENT 13–14 (2009), https://www.hud.gov/sites/documents/TRACS.PDF [https://perma.cc/L67K-YN4C]. State and federal agencies, likewise, exchange information about potential beneficiaries for other important public benefits programs. *See, e.g.*, Computer Matching Agreement Between Dep't of Health & Hum. Servs. Ctrs. for Medicare & Medicaid Servs. and State-Based Administering Entities for Determining Eligibility for Enrollment in Applicable State Health Subsidy Programs Under the Patient Protection and Affordable Care Act 1 (Apr. 2, 2016), https://www.hhs.gov/sites/default/files/cma-1601.pdf [https://perma.cc/K2NM-L2AH]; Computer Matching Agreement Between U.S. Dep't of Health & Hum. Servs., Admin. for Children & Families, Off. of Child Support Enf't, and State Agency Administering the Supplemental Nutrition Assistance Program 2 (Aug. 16, 2019) (on file with the Harvard Law School Library).

[44] For instance, the Adoption and Foster Care Analysis and Reporting System (AFCARS), which includes 183 pieces of information about each placement of a child in foster care by a state agency that receives federal funding, is used to determine funding levels, evaluate eligibility, prepare "Outcomes Report[s]," conduct "Child and Family Service Reviews," and support longer-term programmatic planning. *About AFCARS*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.acf.hhs.gov/cb/resource/about-afcars [https://perma.cc/PYE5-H4PB] (describing uses of databases); *see also* 45 C.F.R. §§ 1355.40–.45 (2020) (describing reporting requirements, including types of information that must be reported).

[45] *See, e.g.*, 42 U.S.C. § 1397m-3(a)(2) (requiring elder justice program grantees "to provide the Secretary with such information as the Secretary may require to conduct an evaluation or audit" of the program).

[46] *See, e.g.*, 42 U.S.C. § 674(a)(3)(C)(iii) (requiring states that receive federal support for the state's child welfare agency and for the Temporary Assistance for Needy Families program to facilitate data exchange between the programs); Information Memorandum from U.S. Dep't of Health & Hum. Servs., Admin. for Children & Families, to States, Tribes, and Territories Administering the Temporary Assistance for Needy Families (TANF) Program et al. 3 (Sept. 21, 2015), https://www.acf.hhs.gov/sites/default/files/documents/ofa/tanf_acf_im_2015_02.pdf [https://perma.cc/H53T-YTKE] (reminding "states, tribes, and territories administering TANF that they are permitted under federal law to determine their own confidentiality rules regarding the safeguarding and disclosure of client information").

In addition to conditioning participation in cooperative programs on a state's willingness to supply program-related data, the federal government has also conditioned participation in one cooperative program on a state's willingness to contribute unrelated data to another program. For instance, a Department of Defense appropriations statute conditioned significant federal funding for public schools on the schools' provision of the "names, addresses, and telephone listings" of students to the Department for defense recruitment purposes.[47]

Finally, the states and federal government exchange data outside jointly administered programs to support initiatives that each level of government pursues individually. For instance, they exchange large quantities of financial information to facilitate each government's tax administration.[48]

C. Data Pooling Programs

The most significant forms of intergovernmental data exchange, however, occur under the auspices of permanent data pooling programs, through which data is aggregated across levels of government for officials in each level to access. Many are striking in scope. The National Directory of New Hires, for instance, contains information on almost all American employees.[49] Private employers provide each new hire's name, address, Social Security number, and wages to state agencies, which in turn pass that information on to the federal government for inclusion in the database.[50] The database's primary use is to facilitate wage withholding for individuals who have failed to pay child support.[51] But it is now also used to verify eligibility for a suite of public benefits

---

[47] National Defense Authorization Act for Fiscal Year 2002 § 544, 10 U.S.C. § 503(c)(1)(A)(ii). The Department of Defense also collects information from state DMVs for its broader recruitment database, "Joint Advertising, Market Research & Studies," about which little is publicly known; however, this practice was disclosed on a standard form through which agencies seek approval from the National Archives and Records Administration to dispose of records. *See* Request for Records Disposition Authority from the Off. of the Sec'y of Def. to the Nat'l Archives & Recs. Admin 2 (Sept. 3, 2014), https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-defense/office-of-the-secretary-of-defense/rg-0330/daa-0330-2014-0008_sf115.pdf [https://perma.cc/P5HE-9N4D]. Although information on the database is now scarce, the Department of Defense appears to have touted the database's reach around the time of its creation, with "information about approximately 30 million people," including roughly ninety percent of the American high school–aged population each year. *See* Complaint at 7, Hanson v. Rumsfeld, No. 06-CV-3118 (S.D.N.Y. Apr. 24, 2006).

[48] *See* INTERNAL REVENUE SERV., INTERNAL REVENUE MANUAL § 11.3.32 (2020) [hereinafter INTERNAL REVENUE MANUAL], https://www.irs.gov/irm/part11/irm_11-003-032 [https://perma.cc/B8MM-AB8M]; *see also* Erin Adele Scharff, *Laboratories of Bureaucracy: Administrative Cooperation Between State and Federal Tax Authorities*, 68 TAX L. REV. 699, 714–17 (2015) (describing tax information sharing system).

[49] *See* 42 U.S.C. § 653a.

[50] *Id.* § 653a(b), (g)(2).

[51] *Id.* § 653a(g)(1).

programs whose benefits are conditioned on employment.[52] The CDC's National Notifiable Diseases Surveillance System, likewise, consolidates reams of information about a large variety of suspected and confirmed diseases first identified by thousands of local and state public health agencies.[53]

Likely the nation's largest information pooling system is the National Crime Information Center (or NCIC) and its complex of crime-related databases, which anchors the intergovernmental exchange of information for day-to-day policing. Any person who has been subject to a traffic stop — or seen one in a movie — knows about the NCIC in practice if not in name. When police officers run a name, driver's license, or license plate, they search the NCIC, a sprawling repository of information about crime across levels of government to which "virtually every criminal justice agency nationwide" has access and contributes data.[54] The NCIC supports "millions of transactions *each day*."[55] And a survey of states estimated that the entire sweep of networked criminal history databases contains files on 110 million people.[56]

The NCIC pools cross-governmental crime-related information in twenty-one categories — ranging from stolen property to wanted persons to parolees to lists of suspected gang members.[57] But it is also networked — in the kind of untidy way that reflects accretion over time — with many other large intergovernmental data initiatives. The Interstate Identification Index, accessed through the NCIC interface, collects arrest and criminal histories as well as fingerprints.[58] The

---

[52] *Id.* § 654(h)(2); *see* 42 U.S.C. § 1320b-7(b) (listing programs for which verification is permitted, including Medicaid, Unemployment Insurance, and the Supplemental Nutrition Assistance Program).

[53] State contributions to the data pool were, somewhat surprisingly, not initially structured by Congress but instead grew out of the initiative of local public health authorities. *See History and Modernization of Case Surveillance*, CTRS. FOR DISEASE CONTROL & PREVENTION (Sept. 24, 2021), https://www.cdc.gov/nndss/about/history.html [https://perma.cc/UG8V-XCAJ]. Notably, the regulations implementing the federal statute that safeguards private health information, the Health Insurance Portability and Accountability Act — often recognized for its robust privacy protections — exempts from its core privacy protection intergovernmental data sharing that is "for the purpose of preventing or controlling disease, injury, or disability," including "public health surveillance." 45 C.F.R. § 164.512(b)(1)(i) (2020).

[54] *National Crime Information Center*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/cjis/ncic [https://perma.cc/MU64-UZDM]. State and local police directives clarify how the NCIC operates. *See, e.g.*, BALT. POLICE DEP'T, POLICY 1301: NATIONAL CRIME INFORMATION CENTER (NCIC) 2 (2017), https://www.baltimorepolice.org/transparency/bpd-policies/1301-national-crime-information-center-ncic [https://perma.cc/7LD3-LU6C].

[55] *National Crime Information Center*, *supra* note 54 (emphasis added).

[56] BECKI R. GOGGINS & DENNIS A. DEBACCO, BUREAU OF JUST. STAT., U.S. DEP'T OF JUST., SURVEY OF STATE CRIMINAL HISTORY INFORMATION SYSTEMS, 2016, at 2 (2018), https://www.ojp.gov/pdffiles1/bjs/grants/251516.pdf [https://perma.cc/P2JC-U2XL].

[57] *National Crime Information Center*, *supra* note 54.

[58] FED. BUREAU OF INVESTIGATION, U.S. DEP'T OF JUST., INTERSTATE IDENTIFICATION INDEX/NATIONAL FINGERPRINT FILE OPERATIONAL AND TECHNICAL MANUAL § 1, at

International Justice and Public Safety Network, somewhat incongruously shortened to Nlets (a too-popular-to-change acronym tracking an earlier iteration of the organization's name), allows officers who use the NCIC to contact the originating state to verify information.[59] Nlets is a private organization owned by the states and is furtive about its work, but several state participants have said publicly that it conducts almost 1.5 billion transactions annually.[60] And the Combined DNA Index System contains over twenty million DNA profiles from missing persons, crime victims, crime scenes, arrestees, and persons convicted of crimes, among others.[61] The NCIC databases have also developed interfaces with databases managed by the Department of Homeland Security (DHS) for the purpose of exchanging immigration-related "biometric and biographic data."[62] The National Instant Criminal Background Check System facilitates background checks — run either by the federal government or by an administering state — on prospective firearm purchasers, and can query the NCIC, Interstate Identification Index, and immigration databases, as well as the System's own index of people ineligible to purchase a firearm under either federal or state law.[63] This criminal justice data ecosystem can be accessed both by criminal justice agencies across levels of government and by non–criminal justice agencies and, in some cases, by private firms.

But the NCIC is not the only sprawling intergovernmental data ecosystem created to facilitate crime-related information exchange. The National Commission on Terrorist Attacks upon the United States (or 9/11 Commission) made a series of recommendations to improve

---

1–2 (2005), https://dojmt.gov/wp-content/uploads/Interstate-Identification-Index-Fingerprint-File-Manual.pdf [https://perma.cc/6RER-VGEZ] ("Generally, records are provided to requesters within seconds of requests transmitted over the FBI's NCIC network to [the Index]." *Id.* at 1.).

[59] *See Information Sharing Resources and Initiatives*, U.S. DEP'T OF JUST. (July 7, 2017), https://www.justice.gov/interpol-washington/information-sharing-resources-and-initiatives [https://perma.cc/SVM8-PNXS].

[60] *Georgia Crime Information Center*, GA. BUREAU OF INVESTIGATION, https://gbi.georgia.gov/georgia-crime-information-center [https://perma.cc/H8YG-C2U3]; *National Law Enforcement Telecommunication System*, S.D. DEP'T OF PUB. SAFETY, https://dps.sd.gov/safety-enforcement/sd-lets/nlets [https://perma.cc/U94M-5UG9].

[61] *CODIS — NDIS Statistics*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics [https://perma.cc/582B-Z22D]; *see Federal DNA Database*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/federal-dna-database [https://perma.cc/8C2R-RU24] (indicating that this DNA system can be accessed through the NCIC).

[62] *See* Memorandum of Understanding Among the Dep't of Homeland Sec., the Dep't of Just., Fed. Bureau of Investigation, Crim. Just. Info. Servs. Div., and the Dep't of State Bureau of Consular Affs. for Improved Information Sharing Services 1 (July 1, 2008), https://www.ice.gov/doclib/foia/secure_communities/dhsfbiinteroperabilitymoujuly2008.pdf [https://perma.cc/SP3V-299C].

[63] FED. BUREAU OF INVESTIGATION, U.S. DEPT. OF JUST., NATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM (NICS) 2019 OPERATIONS REPORT 1–2 (2019), https://www.fbi.gov/file-repository/2019-nics-operations-report.pdf/view [https://perma.cc/SQ8G-Z27H].

terrorism-related information sharing between the federal government and the states.[64]

In contrast to the NCIC, which is managed by the FBI but composed largely of state and local data, cities and states have contributed significant physical infrastructure to this vertical information sharing initiative by helping to erect "fusion centers." There are now seventy-nine such institutions.[65] Rather than share information through technological systems alone, fusion centers also facilitate information exchange by co-locating governmental *personnel* — literally placing representatives from agencies across levels of governments together — from obvious agencies like local police departments, the FBI, and DHS, to less obvious ones like local health, fire, and even corrections departments.[66] Officials are then cross-authorized to access the information in each other's possession and directed to work jointly to analyze and investigate relevant leads.[67] This gives the staffers at fusion centers access to enormous stores of unclassified and classified data held by participating governments.[68]

Although instituted as a response to terrorism-related information sharing needs, states and cities have leveraged fusion centers to support other, more localized objectives. In a 2018 report, DHS indicated that just one of the seventy-eight surveyed fusion centers focused exclusively on counterterrorism efforts, while fifty had "primary missions" focused

---

[64] THE NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT § 13.3 (2004), https://govinfo.library.unt.edu/911/report/911Report.pdf [https://perma.cc/WKA7-KCT4] (recommending an "all-source" approach to information, which is rooted in information sharing, *id.* at 416).

[65] MAJORITY STAFF OF H. HOMELAND SEC. COMM., 115TH CONG., ADVANCING THE HOMELAND SECURITY INFORMATION SHARING ENVIRONMENT: A REVIEW OF THE NATIONAL NETWORK OF FUSION CENTERS 7, 10 (2017), https://www.hsdl.org/?abstract&did=805450 [https://perma.cc/8F74-QN9Q].

[66] U.S. DEP'T OF HOMELAND SEC., 2017 NATIONAL NETWORK OF FUSION CENTERS FINAL REPORT 2 (2018) [hereinafter DHS, 2017 FUSION CENTERS REPORT], https://www.hsdl.org/?view&did=817528 [https://perma.cc/8YTD-UGHB] (summarizing types of personnel present at seventy-seven fusion centers and finding representatives from law enforcement, national security agencies, and the National Guard, as well as functions spanning from corrections, probation, and parole, to public health and fire services).

[67] *See, e.g.*, Memorandum of Understanding Between Las Vegas Metro. Police Dep't, Fed. Bureau of Investigation, U.S. Dep't of Homeland Sec., et al. Regarding the Establishment and Operation of the S. Nev. Counter-Terrorism Ctr., Clark Cnty., Nev. 1 (Feb. 1, 2016) [hereinafter S. Nev. Counter-Terrorism Ctr. MOU] (on file with the Harvard Law School Library).

[68] Danielle Keats Citron & Leslie Meltzer Henry, *Visionary Pragmatism and the Value of Privacy in the Twenty-First Century*, 108 MICH. L. REV. 1107, 1116 (2010) (reviewing DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008)) ("[F]usion centers analyze vast databases of private- and public-sector information, including traffic tickets, property records, motor-vehicle registrations, immigration records, tax information, public-health data, car rentals, credit reports, postal services, utility bills, insurance claims, suspicious-activity reports, and data brokers' digital dossiers.").

on counterterrorism, as well as "All-Hazards" and "All-Crimes."[69] What states and local governments characterize as "All-Hazards" or "All-Crimes" can vary widely. An earlier report analyzing the missions of seventy-eight fusion centers found that sixty-seven included gang-related work; sixty-six included narcotics; fifty-one included healthcare and public health; forty-four worked with corrections, parole, or probation; and forty-two included identify theft and document fraud, among many more areas of focus.[70] In essence, the federal government gets antiterrorism support from fusion centers, while cities and states get extensive federal data to support day-to-day criminal and non–criminal justice functions.

Some data pooling efforts are more tailored, focusing on a particular objective or group of people. The National Practitioner Data Bank collects information from state medical licensing boards on malpractice and disciplinary actions for a range of medical practitioners.[71] And the National Adult Mistreatment Reporting System is a voluntary database in which all fifty states pool information about the perpetrators of elder abuse.[72]

But a narrower focus does not necessarily mean a more modest impact. The FBI pools "hundreds of millions of photos" from state DMVs for use in facial recognition searches.[73] And the National Instant

---

[69] U.S. DEP'T OF HOMELAND SEC., 2018 NATIONAL NETWORK OF FUSION CENTERS FINAL REPORT 2 (2018) [hereinafter DHS, 2018 FUSION CENTERS REPORT], https://www.dhs.gov/sites/default/files/publications/2018_national_network_of_fusion_centers_final_report.pdf [https://perma.cc/8BGL-MBG4]; *see also* Slobogin, *supra* note 3, at 1749 (noting that fusion centers "are focused on virtually any kind of 'threat'"); *id.* at 1750 ("As one fusion center trainer put it, 'If people knew what we were looking at, they'd throw a fit.'").

[70] U.S. DEP'T OF HOMELAND SEC., 2014 NATIONAL NETWORK OF FUSION CENTERS FINAL REPORT 10 (2015), https://www.dhs.gov/sites/default/files/publications/2014%20National%20Network%20of%20Fusion%20Centers%20Final%20Report_1.pdf [https://perma.cc/F3NH-ZCGY].

[71] This data pool has not always proven successful at accomplishing its objectives. *See* Tracy Weber & Charles Ornstein, *Dangerous Caregivers Missing from Federal Database*, PROPUBLICA (Feb. 15, 2010, 3:04 AM), https://www.propublica.org/article/federal-health-professional-disciplinary-database-remarkably-incomplete [https://perma.cc/3SG5-SGLX] (reporting significant gaps in databases); *see also* Letter from Kathleen Sebelius, Sec'y, Dep't of Health & Hum. Servs., & Mary K. Wakefield, Adm'r, Health Res. & Servs. Admin., to State Governors (Feb. 12, 2010), https://assets.propublica.org/legacy/images/uploads/series/NPDB-HIPDB-Dear-Governor.pdf [https://perma.cc/2HBC-7G8P] (acknowledging data gaps).

[72] *Background & History*, NAT'L ADULT MALTREATMENT REPORTING SYS., https://namrs.acl.gov/Learning-Resources/NAMRS-Background.aspx [https://perma.cc/74LE-LJUY]. This data pool is not directly authorized by statute, but implements a recommendation by the Elder Justice Coordinating Council, which was chartered by the elder justice provisions of the Affordable Care Act. *See* Elder Justice Act of 2009, Pub. L. No. 111-148, § 6703, 12 Stat. 782, 786–90 (2010).

[73] U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-579T, FACE RECOGNITION TECHNOLOGY (2019) [hereinafter FACE RECOGNITION TECHNOLOGY REPORT (2019)], https://www.gao.gov/assets/700/699489.pdf [https://perma.cc/3RL8-HLSV] (statement of Gretta L.

Criminal Background Check System (NICS), which, as noted above, conducts gun-purchase background checks, processed over 27.5 million transactions in 2016 alone.[74] Nor do area-specific data pools always act in isolation. The suite of federal trusted traveler programs, for instance, "allows for expedited processing of preapproved, low-risk travelers at certain ports of entry" provided that the traveler undergo vetting against several intergovernmental data pools.[75]

D. Data Sharing Mandates

Although most cross-governmental data sharing happens voluntarily and is often given in exchange for something of value — whether money, policy commitments, or other data — the federal government has sought to mandate data sharing in some high-profile cases, including by creating the impression that states have agreed to share when they have not. Constitutional federalism principles generally prevent the federal government from commandeering state resources or policy apparatuses.[76] But there has long been a suggestion, never directly addressed by the Supreme Court, that there may be an "information sharing exception" to the anti-commandeering rule.[77] The federal government does not frequently test that possibility, but it has attempted to do so in the immigration context under both Democratic and Republican administrations, finding creative ways to effectively compel cities and states to share sizable amounts of immigration-related data.

Because cities and states have many more interactions with community members than do federal immigration agents, federal immigration policymakers across administrations have sought to obtain information from state and local police to assist their immigration enforcement efforts. Through formal and informal programs, federal agents have sought readouts of day-to-day law enforcement encounters, biometrics

---

Goodwin, Director, Homeland Security and Justice, U.S. Government Accountability Office); *see id.* at 4; *see also infra* note 93.

74 Douglas E. Lindquist, Assistant Dir., Crim. Just. Info. Servs. Div., Fed. Bureau of Investigation, Statement Before the Senate Judiciary Committee (Dec. 6, 2017), https://www.fbi.gov/news/testimony/national-instant-criminal-background-check-system-nics [https://perma.cc/5YLS-CQKM] ("To encourage states to make information available, Congress has provided grant incentives and the NICS Program works closely with other federal partners to support grant opportunities for state and tribal entities. States are also making incredible strides in providing information to the NICS Indices: in the last 10 years, the number of records contributed by states increased from just over 1 million records to 7.3 million — or over 600 percent.").

75 ABIGAIL F. KOLKER, CONG. RSCH. SERV., R46783, TRUSTED TRAVELER PROGRAMS 1 (2021); *see also id.* at 3 ("TSA uses the submitted information to conduct security threat assessments of individuals using law enforcement, immigration, and intelligence databases, including a fingerprint-based criminal history records check through the FBI.").

76 New York v. United States, 505 U.S. 144, 175 (1992).

77 *See infra* section III.B.1, pp. 1059–64.

on arrestees, names of individuals in state and local custody, lists of individuals on probation, data from DMV offices about noncitizen drivers, and information about appearances in state and municipal courts.[78] DHS's express goal is to leverage the many ways that cities and states track those who interact with their criminal justice systems to locate and detain individuals on immigration grounds.[79]

The Secure Communities program, started in 2008, sought to encourage states to forward arrestees' biometric data — typically fingerprints — so that federal officials would know when a person of interest was in state or local custody.[80] As is common of intergovernmental data programs (and is discussed in greater detail below), Secure Communities was initiated not through legislation but through ostensibly voluntary agreements.[81] Those agreements contained termination provisions allowing either party to end their participation at will.[82] When several states exercised those termination rights, however, the federal government announced its view that the program was not voluntary after all and that it would "terminate all existing Secure Communities" agreements *but* continue to take state data without them.[83]

Another immigration-related data sharing effort induces states to surrender their data nonconsensually in even more creative fashion. Initiated by statute, that program, best known by its place of codification at 8 U.S.C. § 1373, prohibits states from "in any way restrict[ing]" their employees or officials "from sending to, or receiving from, [the federal government] information regarding the citizenship or immigration status, lawful or unlawful, of any individual."[84] It does not direct states *to* share data; it instead restricts their ability to prevent their employees

---

[78] *See infra* section II.C.3, pp. 1050–53.

[79] *See, e.g.*, U.S. Immigr. & Customs Enf't, Directive No. 11072.1, Civil Immigration Enforcement Actions Inside Courthouses (Jan. 10, 2018) (noting that because persons "entering courthouses are typically screened," conducting enforcement actions there may "reduce safety risks to the public, targeted alien(s), and ICE officers").

[80] Fahey, *supra* note 18, at 2344–45.

[81] *See infra* section II.B, pp. 1040–45.

[82] *E.g.*, Memorandum of Agreement Between U.S. Dep't of Homeland Sec., Immigr. & Customs Enf't, and the N.Y. State Div. of Crim. Just. Servs. 4 (Dec. 28, 2010) [hereinafter N.Y.-ICE Memorandum], https://www.ice.gov/doclib/foia/secure_communities-moa/r_new_york.pdf [https://perma.cc/HXU6-8PGP].

[83] Letter from John Morton, Dir., U.S. Immigr. & Customs Enf't, to Jack Markell, Governor of Del. 1 (Aug. 5, 2011) [hereinafter Letter from John Morton] (on file with the Harvard Law School Library); *see also* Shankar Vedantam, *No Opt-Out for Immigration Enforcement*, WASH. POST (Oct. 1, 2010), https://www.washingtonpost.com/wp-dyn/content/article/2010/09/30/AR2010093007268.html [https://perma.cc/23XA-F8UY] ("Participation in . . . Secure Communities, was widely believed to be voluntary — a perception reinforced by a Sept 7 letter sent to Congress by Homeland Security Secretary Janet Napolitano. . . . But the Immigration and Customs Enforcement agency now says that opting out of the program is not a realistic possibility — and never was.").

[84] 8 U.S.C. § 1373(a).

from sharing data.[85] A state that does not consent to its data being shared with the federal government, in short, is powerless to stop an employee from responding to a federal request to do just that.

But with the rise of "sanctuary cities" — which generally refuse, unless forced, to turn over information to federal immigration officials — the federal government has deployed still more strategies to mandate the sharing of information related to immigration. The federal government, in particular, has aggressively sought information about when noncitizens who are incarcerated in state or local facilities will be released, which it uses to schedule concurrent immigration enforcement efforts. To obtain that nonpublic information from jurisdictions that decline to provide it voluntarily, Immigration and Customs Enforcement (ICE) then began issuing subpoenas demanding the information it once sought voluntarily and threatening information custodians (sheriffs and wardens) with judicial proceedings for contempt if they declined.[86] This tactic, though rare, has been used in other areas as well.[87]

* * *

As this Part makes evident, our domestic governments are bartering, exchanging, and aggregating data of intimate character on a sweeping scale. Because data is an increasingly potent source of governmental power — and because intergovernmental trade allows our governments to gain access to information more efficiently than direct collection from individuals — the very presence of this market is important. It reveals

---

[85] *See* H.R. REP. No. 104-725, at 383 (1996) ("The conferees intend to give State and local officials the authority to communicate with the [Immigration and Naturalization Service (INS)] regarding the presence, whereabouts, or activities of illegal aliens. This provision is designed to prevent any State or local law, ordinance, executive order, policy, constitutional provision, or decision of any Federal or State court that prohibits or in any way restricts any communication between State and local officials and the INS.").

[86] *E.g.*, Press Release, U.S. Immigr. & Customs Enf't, ICE Serves 5 Immigration Subpoenas in Oregon for Criminal Alien Information from Local Law Enforcement (Feb. 21, 2020), https://www.ice.gov/news/releases/ice-serves-5-immigration-subpoenas-oregon-criminal-alien-information-local-law [https://perma.cc/AE8S-WW69] (justifying use of subpoena because "[u]nder Oregon's sanctuary laws, county and law enforcement officials are prohibited from providing ICE with nonpublic information about criminal aliens"); Press Release, U.S. Immigr. & Customs Enf't, ICE Issues Subpoenas to Obtain Information Refused Under Connecticut's Sanctuary Policies (Feb. 13, 2020), https://www.ice.gov/news/releases/ice-issues-subpoenas-obtain-information-refused-under-connecticuts-sanctuary-policies [https://perma.cc/RHJ4-AXAN] (describing subpoenas issued to Connecticut, New York City, and Denver); Conrad Wilson, *Oregon Was 1st Sanctuary Community in US to Respond to ICE Subpoenas*, OR. PUB. BROAD. (Feb. 26, 2020, 1:30 AM), https://www.opb.org/news/article/oregon-ice-subpoenas-sanctuary-cities-washington-county-sheriff [https://perma.cc/HGV8-MSUL] ("It's a new use of subpoenas to use them with law enforcement agencies. We've historically not needed to use them." (quoting Bryan Wilcox, ICE Deputy Field Director, Seattle)).

[87] *See* Mikos, *supra* note 3, at 116–20 (documenting, inter alia, the Equal Employment Opportunity Commission's use of subpoenas to obtain state employment records when investigating federal discrimination claims; the Drug Enforcement Administration's use of subpoenas to investigate medical marijuana industries in states where it is legal for federal drug crimes; and subpoenas of state agencies by federal grand juries).

a powerful pathway to governmental data access. Moreover, because constraints on how data is used are often shaped by the processes through which that data is acquired, this market also raises potent questions about how data that moves across governmental boundaries is governed.

II. GOVERNANCE IN THE INTERGOVERNMENTAL DATA MARKET

Federalism facilitates the intergovernmental data market. As a system of government that, at its most basic, is composed of autonomous levels of government, federalism affords our domestic governments the power to both collect data from their constituents and participate in data transactions with their sister governments. But federalism does not provide ready descriptive or normative frameworks for thinking about what happens to our data next. When data moves between governments, how is that data managed? What legal constraints do our governments impose on data access, use, management, and security, both as a condition of sharing that data, and after it comes under the control of another government? What rights, entitlements, and even basic information do individuals have about their data as it changes governmental hands? What institutions — federal, state, or both — make those judgments?

As this Part shows, once data is on the move, our conventional governmental separateness gives way to a system of intensely complex power amalgamation between levels of government. For in addition to separating power between governments, federalism can also facilitate the reintegration of the power each government independently possesses. The idea that power dispersed among governments can become integrated — as when any level of government through exchange or pooling joins the data it has gathered with the data gathered by a sister government — though a departure from the usual way we think about federalism, is not a novel idea. Writing about the often-analogous separation of powers among the federal government's coordinate branches, Justice Jackson reminded us in his famous *Youngstown* concurrence that "[w]hile the Constitution diffuses power the better to secure liberty, it also contemplates that practice will integrate the dispersed powers into a workable government."[88] What is novel is understanding, as this Part elaborates, the specific predicates of just such a workability determination: a detailed understanding of how powers are drawn together across governments and how, once integrated, they are institutionally and procedurally organized.

As in the private sector where, as Professor Julie Cohen has noted, "perhaps the most noteworthy attribute of the personal data economy

[88] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635 (1952) (Jackson, J., concurring).

has been its secrecy," understanding how data that moves between governments is governed requires significant legal and institutional excavation because, as I show, data exchange programs are generally not organized by clearly legible and transparent forms of law and policymaking, like, most obviously, congressional statutes.[89] Although many forms of intergovernmental interaction *are* initiated by Congress — think of the major "cooperative federalism" programs from the New Deal to present[90] — Congress rarely structures, and is sometimes totally absent from, the intergovernmental data market. There is no section of the U.S. Code that sets the rules of the federal or state governments' participation in data exchange or specifies how the resulting data stores should be managed. Many statutes cited by federal and state officials as authority for the data sharing programs barely contemplate them. Others do so in broad and sweeping terms, providing little guidance or limitation — especially with respect to data privacy. And what scholars call "omnibus" privacy statutes — which are designed to protect the data originator's interests across agencies and policy areas — either explicitly or implicitly exempt from their strictures intergovernmental data exchange. This leaves federal agencies and their state counterparts to decide what data to share, on what terms to share it, which protections to include, whether to create ongoing exchange programs, and how to govern them, often without express statutory authorization.[91]

I show that in this field of striking legislative minimalism, our governments nevertheless rely on formal legal devices to structure data programs. But they are the nonstandard lawmaking devices that I have elsewhere called "intergovernmental agreements" — something of a treaty for domestic federalism, which sets forth the legal terms and conditions of the data transactions, but also memorializes some of the only legal restrictions on how that data will be used.[92] These devices, however, are not the end of the data exchange governance, but the beginning, for our governments increasingly place their data into pools that must be jointly managed on an ongoing basis. The legal framework for this joint management is similarly opaque, resting on a multiplicity of authorities, crisscrossing federal and state governments, and resulting from organic structural negotiations between governments over time. They thus require something of an institutional reconstruction to see

---

[89] JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 62 (2019).

[90] See, for example, the Social Security Act, the Clean Air Act, Title VI of the Civil Rights Act of 1964, and, most recently, the Patient Protection and Affordable Care Act.

[91] This strikes a notable contrast to the ways that intergovernmental interactions centered on other kinds of governmental assets are managed. The federal government's financial assets, most importantly, must be appropriated by Congress, a process that requires at least some thought about how the funded program, whether a federal initiative or one conducted in collaboration with state and local governments, should be structured and regulated.

[92] Fahey, *supra* note 18, at 2329.

even their most basic contours. Drawing together a range of public and nonpublic sources, I sketch the outlines of several different such institutions, which I call "cross-governmental bureaucracies." Given how little we have previously known about these institutions, my goal is not to evaluate their workability or desirability — that must come in program-by-program and institution-by-institution increments. My goal is instead to provide a general roadmap for locating and peering into the unorthodox forms these institutions take.

These cross-governmental bureaucracies have a blended legal character, spanning governmental boundaries just like the data they manage. They are flexible, negotiated, and innovative, but also transient in form and function and concerningly independent from their sources of authority and accountability. They give us a sense of the kind of infrastructure that federalism can facilitate when it reintegrates, in Justice Jackson's terms, forms of power that were once diffused across governments.

A. Statutory Minimalism

Perhaps the defining structural feature of intergovernmental data markets is that — contrary to the conventional understanding of cooperative federalism and intergovernmental projects — they are largely unregulated by Congress.

Take, as an example, the controversy that erupted in 2019 over the FBI's facial recognition database. Over several years, the FBI had developed the capacity to conduct facial recognition searches on hundreds of millions of state-collected photographs.[93] The searchable photos were pooled from federal and state law enforcement sources like mug shots but also from civil sources like driver's license photos. The origin of this data pool remains murky. What is clear is that the effort scaled up when the FBI began entering into intergovernmental agreements with

---

[93] The size of this data pool is difficult to precisely pinpoint. In 2016, the Government Accountability Office (GAO) estimated that the FBI had the capacity to search *411 million* photographs through a network of databases that drew primarily from the states and the federal passport systems. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 15–16 (2016) [hereinafter FACE RECOGNITION TECHNOLOGY REPORT (2016)], https://www.gao.gov/assets/gao-16-267.pdf [https://perma.cc/T5TU-AZTH]. By 2019, that number exceeded *641 million*. *See* FACE RECOGNITION TECHNOLOGY REPORT (2019), *supra* note 73, at 6. There were only 146 million passports in circulation in 2019, so they can account for only a fraction of that number. *See Reports and Statistics: U.S. Passports*, U.S. DEP'T OF STATE, https://travel.state.gov/content/travel/en/about-us/reports-and-statistics.html [https://perma.cc/4A5W-3Q7W]; *see also Law Enforcement's Use of Facial Recognition Technology: Hearing Before the H. Comm. on Oversight and Gov't Reform*, 115th Cong. 12 (2017) [hereinafter *Facial Recognition Hearing* (2017)] (statement of Diana Maurer, Director, Homeland Security and Justice Issues, U.S. GAO) (indicating that the FBI has in its own systems "over 50 million images" and has assembled a network "with total potential access to over 400 million images" across federal and state agencies).

states to secure ongoing access to their DMV photos.[94] The FBI then searched those photographs — both for its own investigations and on behalf of city and state law enforcement agencies — using experimental technology that tries to match photographs of unknown persons to those in existing databases.[95] Existing facial recognition technology, meanwhile, has many known defects. When a federal agency vetted vendors of facial recognition technology, for instance, it found a significant rate of false positives that disproportionately affected women, people of color, the young, and the elderly.[96]

What's most striking for our purposes about this behemoth data pool is the bipartisan surprise and alarm expressed in Congress and state legislatures after the program was publicized in a series of Government Accountability Office reports[97] and, then, on the front page of *The Washington Post*.[98] It was clear that few legislators knew about it and fewer, it seemed, thought they had authorized it.[99] Many expressed deep concerns: about the sheer size of the database, about its experimental technology, and about its use of civil information for criminal purposes without ordinary safeguards like the existence of "reasonable suspicion."[100] In the wake of the *Post*'s reporting, the House Oversight and

---

[94] *See infra* note 108.

[95] *See, e.g.*, FACE RECOGNITION TECHNOLOGY REPORT (2016), *supra* note 93, at 10–11; FACE RECOGNITION TECHNOLOGY REPORT (2019), *supra* note 73, at 1–2; Harwell, *supra* note 5; Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org [https://perma.cc/6H2P-LAAE].

[96] PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, U.S. DEP'T OF COM., NISTIR 8280, FACE RECOGNITION VENDOR TEST (FRVT), PART 3: DEMOGRAPHIC EFFECTS (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [https://perma.cc/63TX-NKG9].

[97] *See* FACE RECOGNITION TECHNOLOGY REPORT (2016), *supra* note 93; FACE RECOGNITION TECHNOLOGY REPORT (2019), *supra* note 73.

[98] Harwell, *supra* note 5.

[99] *See, e.g.*, *id.* ("Neither Congress nor state legislatures have authorized the development of such a system . . . ."); *Facial Recognition Technology: Part I, Its Impact on Our Civil Rights and Liberties*: *Hearing Before the H. Comm. on Oversight and Reform*, 116th Cong. 17 (2019) [hereinafter *Facial Recognition Technology Civil Rights Hearing* (2019)] (statement of Rep. Jim Jordan) ("I guess what troubles me too is just the fact that no one in an elected position made a decision . . . ."); *id.* at 20 (statement of Rep. Michael Cloud) (echoing "the concerns of information being shared without any sort of accountability" by elected officials); *Facial Recognition Hearing* (2017), *supra* note 93, at 112 (statement of Rep. Paul Mitchell) ("So law enforcement all got together and said, 'It's okay, and we're going to do that.'"); *see also* Elizabeth Hewitt, *Updated: FBI Can Access Vermont DMV Facial Recognition Information*, VTDIGGER (Oct. 18, 2016), https://vtdigger.org/2016/10/18/report-fbi-access-vermont-dmv-facial-recognition-information [https://perma.cc/BTZ3-F36M] ("I [have] just never been made aware that is available." (quoting Vermont State Sen. Joe Benning)).

[100] *See Facial Recognition Hearing* (2017), *supra* note 93, at 113 (statement of Professor Alvaro Bedoya, Executive Director, Center on Privacy and Technology, Georgetown Law School) ("The State agency has to have a criminal justice purpose but is not required to have reasonable suspicion to search the FBI's database."); Drew Harwell, *Both Democrats and Republicans Blast Facial-Recognition Technology in a Rare Bipartisan Moment*, WASH. POST (May 22, 2019),

Reform Committee — one of the most powerful investigative committees in Congress — held a pair of tense hearings, during which members from both parties pressed the FBI and expert witnesses on the program's source of authorization.

Much of the attention was trained on how the FBI gained such broad access to so many state DMV databases. When queried about its authority to use state (civil) DMV licensing photographs to conduct federal (criminal) investigations, the FBI's representative tentatively identified a federal statute enacted to protect the *privacy* of state DMV records, the Driver's Privacy Protection Act of 1994.[101] That statute was enacted in response to the advent of a lucrative revenue stream for states in selling DMV data, including photographs, to marketers, insurers, and other private companies.[102] The Act requires states to obtain express consent before selling or sharing an individual's data.[103] But it also sets out several exemptions to that consent requirement, including allowing DMVs to share information with "any . . . entity acting on behalf of a Federal, State, or local agency in carrying out its functions" without an individual's consent.[104] Seizing on that exception from the consent requirement, the FBI argued to Congress that the Act allows the sharing of driver's license photos when they are "utilized for law enforcement purposes."[105] In essence, the FBI appeared to be saying that, because the Act does not *prohibit* DMVs from sharing information (without consent) with the FBI, it should be understood to affirmatively *authorize* such transfers. One member of Congress described that as a "very shaky legal ground" for a program that gives the FBI "ubiquitous access to" DMV photos "across 50 states."[106] Indeed, it is black-letter administrative law that an agency "has no power to act . . . unless and until Congress confers power upon it."[107] Reading the absence of a prohibition as a conferral of authorization turns that basic principle on its head.[108]

---

https://www.washingtonpost.com/technology/2019/05/22/blasting-facial-recognition-technology-lawmakers-urge-regulation-before-it-gets-out-control [https://perma.cc/Y6CY-AKWK].

101 18 U.S.C. §§ 2721–2725; *see Facial Recognition Hearing* (2017), *supra* note 93, at 119 (statement of Kimberly Del Greco, Deputy Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation) (noting that the FBI considers the Driver's Privacy Protection Act as authorization).

102 Reno v. Condon, 528 U.S. 141, 143–44 (2000).

103 18 U.S.C. § 2721(a)(2).

104 *Id.* § 2721(b)(1).

105 *Facial Recognition Hearing* (2017), *supra* note 93, at 118 (statement of Del Greco).

106 *Id.* at 119 (statement of Rep. Gerry Connolly).

107 La. Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 374 (1986).

108 Nevertheless, an assessment of the state-by-state intergovernmental agreements that operationalized this program, *see infra* section II.B, pp. 1040–45, reveals that while most states cited an independent source of state statutory authority to enter into the agreement, some cited only the nonprohibition in the Driver's Privacy Protection Act. *See, e.g.*, Memorandum of Understanding Between

The same question could be asked of the states — had *they* authorized the transfer of DMV data to the FBI? Republican Congressman Jim Jordan asked exactly that, inquiring whether the "state legislature and the Governor actually [had] pass[ed] legislation saying it was okay for the FBI to access every single person in their state who has a driver's license."[109] As one expert explained: "No, and that is the problem. This was all in secret, essentially."[110] Congressman Jordan captured the terrain well: "So some unelected person at the FBI talks to some unelected person at the state level and they say yes, go ahead . . . [h]ere is [data from] 10 million folks . . . [.]"[111]

That a complex data sharing initiative as significant as this one could spring into being without a structuring federal statute is surprising, but it is quite ordinary in this context. And even where Congress has more explicitly authorized the data sharing in question, it rarely provides the kind of detailed roadmap that is standard for other cooperative federalism programs. Indeed, Congress has in all but a few cases declined to make the kind of normative trade-offs or institutional design choices that sensitive data pools require — instead leaving those decisions to federal and state administrative actors.[112]

1. Data Sharing Statutes. — The National Crime Information Center is a textbook example of how Congress approaches intergovernmental data pools. As described above, the NCIC compiles information from a network of databases from all fifty states, dozens of federal agencies, and thousands of local criminal justice agencies into the Interstate Identification Index — a massive database that is searched millions of times a day by officials across the country. Though the data comes from nearly all state and local governments, the NCIC is overseen by the FBI and its Criminal Justice Information Services Division, which is the Bureau's largest division, eclipsing even its core enforcement departments.[113]

---

the Fed. Bureau of Investigation, Crim. Just. Info. Servs. Div., and the Ala. Dep't of Pub. Safety Concerning the Search of Probe Photos Against the Ala. Dep't of Pub. Safety Photo Repository 2 (Mar. 24, 2014) (on file with the Harvard Law School Library); Memorandum of Understanding Between the Fed. Bureau of Investigation, Crim. Just. Info. Servs. Div., and the Ark. Dep't of Fin. & Admin. Concerning the Search of Probe Photos Against the Ark. Dep't of Fin. & Admin. Facial Recognition Database 2 (Sept. 12, 2013) (on file with the Harvard Law School Library); Memorandum of Understanding Between the Fed. Bureau of Investigation, Crim. Just. Info. Servs. Div., and the Vt. Dep't of Motor Vehicles Concerning the Search of Probe Photos Against the Vt. Dep't of Motor Vehicles Photo Repository 2 (May 8, 2013) (on file with the Harvard Law School Library).

109 *Facial Recognition Technology Civil Rights Hearing* (2019), *supra* note 99, at 15 (question of Rep. Jordan).

110 *Id.* (statement of Neema Singh Guliani, Senior Legislative Counsel, ACLU).

111 *Id.* (statement of Rep. Jordan).

112 *See infra* notes 141–148 and accompanying text (describing exceptions to this general trend).

113 *Criminal Justice Information Services (CJIS)*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/cjis [https://perma.cc/38W3-Q4ZN].

Despite the scale of the NCIC, and the enormous sensitivity of the personal data compiled within its databases, it is hard to identify a federal statute that appears to contemplate data collection of this magnitude. The FBI routinely cites as authorization for the NCIC a 1924 appropriations statute allocating funds for the Attorney General to "acquire, collect, classify, and preserve identification, criminal identification, crime, and other records" and "exchange such records" with "authorized officials of the Federal Government, . . . the States, . . . Indian tribes, cities, and penal and other institutions."[114] The NCIC is, of course, not mentioned by name, nor could it have been in the contemplation of the Congress that crafted that statute. Today's twelve-million-transaction-per-day digital juggernaut bears little resemblance to the exchange of carbon copies that the 1924 Congress funded. In the early years of the NCIC, many pushed Congress to comprehensively regulate its content, security, privacy, and management structure. But the only legislative success was narrow: a law focused on inducing states to send not just arrest information to the system, but also the final disposition of the individual's case.[115] (Arrest information alone can create the misleading impression that a person who was released without charge or acquitted has a criminal history.) One-off provisions of federal law have subsequently directed that new data be added to the NCIC,[116] additional federal departments be given access,[117] and state efforts to achieve "full participation" be funded.[118] But Congress has not stepped in to comprehensively regulate.[119]

---

[114] 28 U.S.C. § 534(a)(1), (a)(4). The provision originated in the Act of May 28, 1924, Pub. L. No. 68-153, ch. 204, tit. II, 43 Stat. 205, 217. Six years later, Congress created a division in the FBI dedicated to information management and assigned these tasks to it. *See* Act of June 11, 1930, Pub. L. No. 71-337, ch. 455, 46 Stat. 554, 554 (codified at 5 U.S.C. § 340 (1946)).

[115] *See* Crime Control Act of 1973, Pub. L. No. 93-83, § 524(b), 87 Stat. 197, 215–16 (asking states to include "to the maximum extent feasible" the final disposition of an arrestee's case, to "reasonably design[]" procedures to keep information up to date, and to allow individuals to correct inaccuracies). *But see* Donald L. Doernberg & Donald H. Zeigler, *Due Process Versus Data Processing: An Analysis of Computerized Criminal History Information Systems*, 55 N.Y.U. L. REV. 1110, 1138–39 (1980) ("Although well-intentioned, this legislation was not designed either to serve as a blueprint for reform of criminal history information systems or to require effective changes in existing practices.").

[116] *See, e.g.*, 8 U.S.C. § 1252c(a)–(b) (including federal information about any "alien illegally present in the United States" who was "previously . . . convicted of a felony," and was deported or otherwise left the country, *id.* § 1252c(a)); 28 U.S.C. § 534(a)(2)–(3) (including federal information about missing and unidentified persons); *id.* § 534(f)(2)(B) (including state and local information about protection orders).

[117] *See, e.g.*, 8 U.S.C. § 1105(b)(1) (allowing immigration authorities to access the NCIC "for the purpose of determining whether or not a visa applicant or applicant for admission has a criminal history record indexed in any such file"); 42 U.S.C. § 1437d(q)(1)(A) (authorizing access to the NCIC by public housing agencies "regarding the criminal conviction records of adult applicants").

[118] 34 U.S.C. § 40301(b)(4)–(5).

[119] My intent is not to suggest that, as a matter of administrative or constitutional law, the NCIC is legally improper. The goal is only to contrast Congress's involvement in this area with most other federalism-rich areas, in which it takes a heavier hand.

This is not an ordinary case of broad congressional delegation to a federal agency. When Congress steps back in this federalism-rich area, the President is not the only political or administrative actor to step in. The architecture of the NCIC, from its high-level design — what information it contains, which governmental entities contribute to it, and for what purposes it can be accessed — to its detailed operational and privacy rules, is set out in intergovernmental agreements and a cross-governmental bureaucracy, which I describe below.

Congress has used a similarly light touch with other sweeping intergovernmental data programs.[120] And these programs, thus, follow a similar pattern: Without Congress, federal agencies and state governments develop their own cooperative structures and governance approaches.

As we saw with the facial recognition collaboration between the FBI and state DMVs, states likewise frequently embark on large data sharing programs without legislative authorization. As Professor Christopher Slobogin documents with respect to fusion centers, in "most states, fusion centers are not explicitly authorized by statute" but instead purport to "derive their authority from general statutes creating state police agencies or memoranda of understanding among partner agencies."[121]

2. Privacy Statutes. — Given the significant privacy issues raised by intergovernmental data exchange, one might expect that any gaps present in these programs' authorizing statutes would be filled by the federal government's data privacy statutes. In fact, the two main federal privacy statutes have remarkable blind spots to intergovernmental data sharing.

Together, the Privacy Act of 1974[122] and the E-Government Act of 2002[123] establish the transstatutory privacy regime for personal data

---

120 For instance, as authorization for the Secure Communities program, the Department of Homeland Security cites a provision of federal law that instructs the President to ensure data interoperability (essentially, consistent formatting) between federal law enforcement and immigration databases. *Secure Communities*, U.S. IMMIGR. & CUSTOMS ENF'T (Feb. 9, 2021), https://www.ice.gov/secure-communities [https://perma.cc/268N-8FDW] (citing 8 U.S.C. § 1722(a)(2) as authority). The single-sentence provision does not mention or even allude to a sweeping data sharing initiative. *See* 8 U.S.C. § 1722(a)(2). By comparison, the statute authorizing the federal government to participate in fusion centers appears positively expansive, spanning eight pages in the Statutes at Large. *See* Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 511, 121 Stat. 266, 317–24 (codified at 6 U.S.C. § 124h). But by the standards of a typical cooperative federalism program, its text is slender and its directives broad. As indication, the Department of Homeland Security's first Privacy Impact Assessment for its fusion center initiative notes that the 9/11 Commission Act simply "codif[ied] many of the interactions the Department was already undertaking with fusion centers." U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE DEPARTMENT OF HOMELAND SECURITY STATE, LOCAL, AND REGIONAL FUSION CENTER INITIATIVE 4 (2008), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf [https://perma.cc/YYY6-4GQF].

121 Slobogin, *supra* note 3, at 1750 (quoting THE CONST. PROJECT, RECOMMENDATIONS FOR FUSION CENTERS: PRESERVING PRIVACY & CIVIL LIBERTIES WHILE PROTECTING AGAINST CRIME & TERRORISM 6 (2012)).

122 5 U.S.C. § 552a.

123 Pub. L. No. 107-347, 116 Stat. 2899 (codified as amended in scattered sections of 44 U.S.C.).

held by the federal government.[124] Those Acts set out high-level information management directives, but also permit significant agency discretion by instructing agencies to identify and mitigate privacy risks themselves, rather than attempting to predict and manage them legislatively.

The Privacy Act prohibits, subject to exceptions discussed below, the dissemination of an individual record without the written consent of the record's subject.[125] It makes agencies account for their disclosures.[126] It instructs them to allow individuals to correct inaccuracies in governmental records.[127] It requires them to collect only information "relevant and necessary" to accomplish the purposes specified in statutes and executive orders.[128] And, where the information may adversely determine an individual's rights or benefits, it tells agencies to "collect information to the greatest extent practicable *directly* from the subject."[129]

Recognizing that rigid rules can be circumvented by technological advances, however, the Acts generally stop there and try to mitigate additional privacy risks by imposing procedural requirements on agencies. To that end, agencies must publish a "system of records notice," or SORN, when describing new (or revising old) "system[s] of records" — that is, a notice that describes the system's use and governing practices.[130] They must also conduct a "Privacy Impact Assessment" before initiating most efforts to collect individual information.[131] By statutory mandate and long-standing federal guidance, the Assessments must specify what information will be collected and its intended use, outline who will have access to it, identify its privacy and security risks, and set forth mitigation measures.[132]

---

[124] Of course, more targeted statutes also establish protections for some discrete forms of data. *See, e.g.*, DNA Identification Act of 1994, 34 U.S.C. §§ 12591–12593, 40701–40706; Tax Reform Act of 1976, 26 U.S.C. § 6103 (tax return privacy); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (educational record privacy); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of the U.S. Code) (health information privacy). The Privacy Act also establishes special protection for one piece of data — the Social Security number. 5 U.S.C. § 552a note (Disclosure of Social Security Number).

[125] 5 U.S.C. § 552a(b). In ways not relevant here, that prohibition is more specific than this gloss conveys: It applies only to information held in a "system of records," meaning databases using a name or an identifying symbol to retrieve information. *See id.* § 552a(a)(5).

[126] *Id.* § 552a(c).

[127] *Id.* § 552a(d).

[128] *Id.* § 552(e)(1).

[129] *Id.* § 552(e)(2) (emphasis added).

[130] *Id.* § 552a(e)(4).

[131] E-Government Act of 2002, Pub. L. No. 107-347, § 208(b), 116 Stat. 2899, 2921–22 (codified at 44 U.S.C. § 3501 note (Federal Management and Promotion of Electronic Government Services)).

[132] *Id.*; Memorandum from Joshua B. Bolten, Dir., Off. of Mgmt. & Budget, to the Heads of Exec. Dep'ts & Agencies (Sept. 26, 2003), https://obamawhitehouse.archives.gov/omb/memoranda_m03-22 [https://perma.cc/B78R-CA8X].

Many commentators have highlighted the gaps, enforcement problems, and design flaws in this regime.[133] What is important for our purposes is that it is virtually ignorant of, and only minimally restrains, intergovernmental data exchange. SORNs and Privacy Impact Assessments, for instance, require agencies to specify the source of the information they are seeking to gather, but this requirement can be discharged by simply enumerating — as most do — a long list of potential sources that includes state, local, tribal, and territorial governments.[134] The public disclosures rarely specify what data the federal government obtains from each of these sources, nor do they normally cross-reference the contract-like agreements that lay out their terms.

Moreover, the Privacy Act's flagship consent requirement — that an agency may not disseminate a record without the consent of the record's subject — has several limitations and exceptions that constrain its reach to intergovernmental data sharing. The most relevant limitation of the consent requirement is its application only when the federal government is the party surrendering data. When a federal agency *shares* records with state and local governments, the Privacy Act requires it to obtain consent from the data's subject (with the exceptions discussed below). When the federal government *receives* information, however, the Privacy Act imposes no similar requirement. Consistent with the Privacy Act, then, the federal government can — and does — obtain large quantities of information from cities and states for reasons that depart from the purposes for which the data was collected *and* without the consent of the data's subject.[135] The legislative history does not disclose the rationale behind this exception, but it is in tension with one way of understanding the objective of the Act: to ensure that the federal government uses information only for the purposes for which it was collected and about which the subject has notice.[136] And certainly the federal government could say to states: we would like you to share your data, but please gain the consent of the data's subject first.

---

[133] *See, e.g.*, Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 249 (2011) ("The dominant critique [of U.S. privacy law] denounces the existing patchwork of privacy statutes as weak, incomplete, and fractured."); Schwartz & Solove, *supra* note 1, at 1824 ("[T]he Privacy Act remains an antiquated law that misses the significance of the computer search revolution . . . ."); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 584 (1995) ("The excessively broad scope of some of these exemptions weakens the Privacy Act's attempt to set obligations for agencies' processing of personal data.").

[134] *See, e.g.*, System of Records Notice for Department of Homeland Security Criminal Arrest Records and Immigration Enforcement Records Systems, 81 Fed. Reg. 72,080, 72,089 (Oct. 19, 2016); U.S. DEP'T OF HOUS. & URB. DEV., *supra* note 43, at 7.

[135] Hence, the DMV information is shared for all kinds of federal purposes unrelated to licensing the operation of a motor vehicle. *See supra* pp. 1031–34.

[136] H.R. REP. NO. 93-1416, at 9 (1974), *reprinted in* S. COMM. ON GOV'T OPERATIONS & SUBCOMM. ON GOV'T INFO. & INDIVIDUAL RTS. OF THE H. COMM. ON GOV'T OPERATIONS,

The Act's consent requirement also has two exceptions that limit its applicability to data that moves across governmental boundaries. The first exception is for "routine uses." Agencies, in short, are excused from obtaining a subject's consent when disseminating a record for uses "compatible with the purpose for which it was collected," as long as those routine uses are disclosed in advance.[137] Federal agencies have generally conceptualized their "routine uses" very broadly.[138] And they have smoothed the way for data sharing with states and local governments without the subject's consent by simply announcing in advance that the data's "routine uses" encompass use by state and local agencies.[139] The Act does not specifically authorize that practice, but it is now well entrenched that "routine uses" of federal data for Privacy Act purposes can include uses by federal agencies as well as state and local ones.

The second exception that limits the applicability of the Privacy Act here is the Act's exemption for information sharing for purposes of "civil or criminal law enforcement activity."[140] Because many of the largest data pooling programs are related to law enforcement in at least some way, the Privacy Act's hands-off approach to those initiatives allows administrative actors to essentially self-regulate.

There is no inherent difficulty in legislatively regulating the privacy aspects of information sharing. Indeed, two exceptions to the general trend of statutory minimalism prove that it can be done. The Computer Matching and Privacy Protection Act of 1988[141] requires federal agencies to establish data sharing agreements when they consult *either* federal or state databases to cross-check information.[142] But the scope of

---

94TH CONG., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, S. 3418 (PUBLIC LAW 93-579), at 302 (J. Comm. Print 1976) (noting that the principle that an "individual should be able to prevent information from being . . . used for other than authorized purposes without his or her consent" is embodied in the Privacy Act).

137 These disclosures must be made in a systems of record notice, or SORN. 5 U.S.C. § 552a(a)(7) (defining "routine use"); *id.* § 552a(b)(3) (exempting routine uses disclosed in SORNs).

138 Todd Robert Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 980 (1991) ("Federal agencies continue to circumvent the nondisclosure provision through broadly worded routine use notices.").

139 *See, e.g.*, Publication of Notice of Systems of Records, a Proposed New Routine Use, New Category of Records and an Amendment of a Current Category of Records, 71 Fed. Reg. 35,342, 35,344 (June 19, 2006) (specifying disclosure to "a national, State, county, municipal, or other publicly recognized charitable or income security administration agency . . . when necessary to adjudicate a claim under the retirement, insurance, unemployment, or health benefits programs" of various federal agencies); Notice of Modified Systems of Records for the FBI Central Records System, 63 Fed. Reg. 8,659, 8,682 (Feb. 20, 1998) ("Information in this system may be disclosed as a routine use to any state or local government agency directly engaged in the criminal justice process . . . where access is directly related to a law enforcement function of the recipient agency . . . .").

140 5 U.S.C. § 552a(b)(7).

141 Pub. L. No. 100-503, 102 Stat. 2507 (codified at 5 U.S.C. § 552a note).

142 *Id.* § 552a(o).

the statute is limited, applying only when an agency is verifying a person's eligibility for federally funded public benefits.[143] Still, these mandated agreements are unusual because Congress has said specifically what they must include.[144] As discussed below, intergovernmental agreements are the standard legal device used to structure data exchange programs, and most are far more fluid and informal than these congressionally mandated agreements.

Another sector-specific statute, the DNA Identification Act of 1994,[145] takes a rare heavy hand in structuring the intergovernmental exchange of DNA for law enforcement purposes. It mandates that the FBI certify state laboratories that place DNA in the national database.[146] It limits access to the information in the database (though it allows access by any "criminal justice agenc[y] for law enforcement identification purposes").[147] And it creates criminal penalties for the mishandling of DNA information.[148]

Most states do not have omnibus privacy frameworks, but even the few states that have passed comprehensive privacy statutes seem to follow Congress's lead and ignore intergovernmental information sharing.[149] California's data privacy law is notable because it is so comprehensive. But even that law *authorizes* cross-governmental information sharing in broad terms, providing that information may be shared without the data subject's consent or notice "if required by state *or* federal law."[150] This deference to federal information sharing *requirements* is striking in light of the constitutional framework I discuss below, which protects state governments from just that kind of federal mandate, in the data world and beyond.[151]

B. Contractual Lawmaking

The fact that intergovernmental data transfers and data pooling programs operate largely without Congress's constraint is surprising. These complex initiatives are subject to the same normative trade-offs, pressures from organized interest groups, and ambitions of efficiency and

---

143 *See id.*

144 *See id.*

145 34 U.S.C. §§ 12591–12593, 40701–40706.

146 *Id.* § 12592(b).

147 *Id.* § 12593(b). Also of note, Congress has affirmatively regulated how tax information may be shared with states for purposes of joint tax administration. *See* INTERNAL REVENUE MANUAL, *supra* note 48, § 11.3.32.1.1; *see also infra* note 171 (noting that the IRS is authorized to negotiate specialized data sharing agreements with the states).

148 34 U.S.C. § 12593(c).

149 Schwartz, *supra* note 133, at 557 ("Unlike federal law, state data protection law usually does not employ an omnibus law that sets fair information practices for governmental entities.").

150 CAL. CIV. CODE § 1798.24(f) (West 2021) (emphasis added).

151 *See infra* Part III, pp. 1054–70.

efficacy as any other large-scale intergovernmental program. They could not occur without some form of legal structuring to plan and organize them. The legal instruments that play that role here are not uncommon, but they are unfamiliar. States, cities, and the federal government transfer, exchange, and pool data — and establish the institutions to manage those data flows — in quasi-contractual ways, using legal instruments that I have previously called "intergovernmental agreements."[152]

These are formal written agreements entered into by the federal government and a counterparty state or city. They have "will" and "shall" clauses, conditions and attestations, terms stipulating their effective period and how they can be terminated, signature lines, and sometimes a bit of fuddy language about consideration.[153] But they serve purposes that ordinary contracts do not. They "speak not just inwardly to their governmental counterparties but also outwardly to the shared constituents of those governments" because they contain rules that define the entitlements of both their governmental parties and "polities they jointly govern."[154] They perform, in short, both the commitment-making function of contracts and the lawmaking function of ordinary statutes.

Intergovernmental agreements serve a range of important and still not fully understood functions in the ordinary warp and weft of governance in our federalist system, but given Congress's light touch in managing data, their role is particularly vital here. In more familiar federalism programs, intergovernmental agreements are an important step in the program's execution. After the basic terms of a federal-state program — say, Medicaid — are worked out in Congress, and the implementing agency promulgates regulations in the Federal Register setting out the detailed conditions of state participation, the agency forges an agreement with the state or city counterparty.[155] Tactically, that agreement often serves as a further round of administrative law and policymaking.[156] It can more specifically articulate the terms of the federal government's offer; reflect a state's regulatory plan for meeting those terms; and indicate the federal government's assent to it.[157] More theoretically, even the most mundane intergovernmental agreements also perform a significant *constitutional* function. Because Congress may

---

[152] *See generally* Fahey, *supra* note 18. These agreements can be styled in a range of ways, as contracts, compacts, memoranda of agreement, state plans, data sharing agreements, and everything in between. *Id.* at 2337–38.

[153] *See generally id.*

[154] *Id.* at 2337.

[155] *See id.* at 2341.

[156] *See id.* at 2339–43.

[157] *Id.* at 2399 ("While some terms of these agreements flow directly from the text of federal or state statutes, most do not. Some are negotiated . . . . Some are chosen by state officials from a 'menu' of federally authorized options . . . . [O]thers consist of a state's own proposals . . . which form the basis of the state's obligations once they are approved by the federal government.").

not commandeer states into joining its programs, intergovernmental agreements memorialize the state's voluntary choice to participate in them.[158]

The intergovernmental agreements used to structure data programs serve all of those functions and then some. Most distinctively, in Congress's absence, they perform significant *legislative* functions, rather than primarily *administrative* ones. They distribute roles and responsibilities among participating governments, specifying what each gives and gets.[159] They erect program architectures, defining goals, creating institutions, and specifying processes for data pooling programs. And, most profoundly, they serve as the legal instrument, and their negotiation as the legal process, through which coordinating governments make core normative trade-offs. How did the facial recognition program discussed at the beginning of this Part come to be without affirmative action by Congress and state legislatures? Through twenty-one negotiations between the FBI and state public safety agencies and DMVs, and the enactment of twenty-one separate intergovernmental agreements.[160]

The same is true of the NCIC — and has been for decades. After early efforts to regulate a young NCIC failed in the early 1970s,[161] the Department of Justice entered into individual agreements with each state, in which the state indicated (and DOJ approved) how it planned to approach its own data gathering, privacy, and security issues and what data it would send to the central database.[162] Where centralized structuring proved elusive, the parties shifted to a strategy of lawmaking by mutual agreement. These original agreements continue to be cited as part of the program's law today. They have also been supplemented by a growing network of additional agreements that govern new aspects of the program as it evolves.[163]

This pattern is also reproduced in fusion centers, the federal-state-local centers designed to co-locate intelligence analysts from across

---

158 *See infra* Part III, pp. 1054–70. Indeed, intergovernmental agreements are often cited as the jurisdictional hook for the federal government to effectively regulate states and cities because they commonly include clauses committing the subfederal government to comply not just with existing regulations but also with future ones. *See* Fahey, *supra* note 18, at 2391–92.

159 For instance, Secure Communities exchanged data (on the state side) for a policy commitment (on the federal side) to focus federal enforcement on the most serious immigration offenders. *See, e.g.*, N.Y.-ICE Memorandum, *supra* note 82, at 2–3.

160 *See supra* note 108.

161 *See* Doernberg & Zeigler, *supra* note 115, at 1134–39.

162 *See, e.g.*, STATE OF KAN., CRIMINAL HISTORY RECORD INFORMATION PLAN (1976).

163 *See* U.S. DEP'T OF JUST., CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SECURITY POLICY, VERSION 5.9, at 15–17 (2020) (noting that "[b]efore exchanging [criminal justice information], agencies shall put formal agreements in place that specify security controls," which come in a range of formats, from "State and Federal Agency User Agreements," *id.* at 15, to "Criminal Justice Agency User Agreements," to "Interagency and Management Control Agreements," *id.* at 16, and "Agency User Agreements," *id.* at 17).

levels of government and "fuse" together their respective antiterrorism and criminal information. The agreements that establish these centers are not usually disclosed publicly, but those that are look like charters of sorts, constituting and envisioning what form these novel joint institutions will take. The agreement between the City of Las Vegas, State of Nevada, FBI, DHS, and various other agencies creating the Las Vegas fusion center — styled the Southern Nevada Counter Terrorism Center — announces the "intent of the Participating Agencies to centralize and co-locate" staff and to "establish a framework for the organization" of the Center.[164] It then envisions its own governance structure in the form of a cross-governmental Board of Governors, with particular composition, voting rights, and decisionmaking processes.[165]

Intergovernmental agreements also sit at the foundation of the less formal data sharing programs. In the early 2000s, Kansas set up the Crosscheck program, designed to allow participating states to exchange voter registration data, identify individuals registered in multiple states, and prevent voter fraud.[166] This perilously informal program was structured through intergovernmental agreements, whose slapdash creation ultimately precipitated the program's downfall.[167] The agreements omitted security protocols for the sensitive data (which included Social Security numbers) that Crosscheck transmitted between states, articulating security commitments at only the highest level of generality.[168] The program was halted in 2019 by a lawsuit that alleged that Kansas had failed to adopt even minimal security procedures like encryption, password protection, multi-factor authentication, and a secure file-transfer protocol.[169] The district court noted pointedly that "no

---

[164] *See, e.g.*, S. Nev. Counter-Terrorism Ctr. MOU, *supra* note 67, at 1.

[165] *Id.* at 2–3; *see also* DHS, 2017 FUSION CENTERS REPORT, *supra* note 66, at 14 (surveying governance structures of several dozen fusion centers).

[166] *See Thornburgh Signs Four-State Agreement*, CANVASSING KAN., Mar. 2006, at 1, https://www.kssos.org/forms/communication/canvassing_kansas/marcho6.pdf [https://perma.cc/Y8FU-8Q8T].

[167] *See* Memorandum of Understanding for Interstate Voter Registration Data Comparison 2 (May 2014) (on file with the Harvard Law School Library).

[168] *See id.*

[169] Moore v. Kobach, 359 F. Supp. 3d 1029, 1035 (D. Kan. 2019); *see* Press Release, ACLU of Kansas, ACLU of Kansas Settlement Puts "Crosscheck" out of Commission for Foreseeable Future; Program Suspended Until Safeguards Added (Dec. 10, 2019), https://www.aclukansas.org/en/press-releases/aclu-kansas-settlement-puts-crosscheck-out-commission-foreseeable-future-program [https://perma.cc/C2UL-DGJP]. Since Crosscheck's collapse, a newer intergovernmental initiative, the Electronic Registration Information Center (ERIC) — formed to enable states to check their voter rolls against those of sister states — has gained prominence. *See Who We Are*, ELEC. REGISTRATION INFO. CTR., https://ericstates.org/who-we-are [https://perma.cc/MSQ3-9JRR]. ERIC, though much more institutionally sophisticated, likewise rests on an intergovernmental agreement made between its member states and the organization. *See* ELEC. REGISTRATION INFO. CTR., BYLAWS AND MEMBERSHIP AGREEMENT (2020), https://ericstates.org/wp-content/uploads/2020/02/ERIC_Bylaws_01-2020.pdf [https://perma.cc/M6U8-D2HR].

provision of the Memorandum of Understanding" facilitating the program "restricts unsecured transmissions."[170]

Information exchange that arises as an adjunct to federal-state programs and through one-off transactions is likewise structured through intergovernmental agreement.[171] In 2020, when the Census Bureau sought state data to make its citizenship tabulations, it entered into agreements with state DMVs, each reflecting different terms and conditions, specifying what data each state would send and at what price, what privacy protections the Bureau would afford, and under what conditions the data could be shared further.[172]

Understanding the outsized significance of intergovernmental agreements in the data sharing context deepens our understanding of their significance — and their complexity. As structuring devices for evolving intergovernmental programs that transact in novel governmental powers — especially those enabled by technological advancement — they offer valuable flexibility. As lawmaking devices for protecting core liberties in the interstitial spaces between governments, especially when Congress has stayed its hand, they raise serious concerns. In the data sector, these agreements follow, perhaps even more universally, the trend common to other intergovernmental agreements: they are not ordinarily made public, and their custodians sometimes go to significant lengths (as I can attest) to keep them from disclosure.[173] They also lack an accepted and accessible process for creation. Moreover, because

---

[170] *Kobach*, 359 F. Supp. 3d at 1033.

[171] For a nice discussion of these agreements within one major agency, see, for example, OFF. OF THE CHIEF TECH. OFFICER, U.S. DEP'T OF HEALTH & HUM. SERVS., THE STATE OF DATA SHARING AT THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES 18–19 (2018) (noting that changes to data practices in major programs often "require renegotiating existing agreements and receiving cooperation among state and territory partners"). Even the exchange of information between federal and state tax administrators, which is explicitly authorized and constrained by Congress, is operationalized by an "Agreement on Coordination of Tax Administration" called the "Basic Agreement," which is standard across states, and an "Implementing Agreement," which may be tailored to each state. INTERNAL REVENUE MANUAL, *supra* note 48, § 11.3.32.3 (describing the "Basic Agreement"); *id.* § 11.3.32.4 (describing the "Implementing Agreement" and noting that the "agreement will supplement the basic agreement by specifying the detailed working arrangements and items to be exchanged, including tolerances and criteria for selecting those items, as agreed to by the state"); *see also* Scharff, *supra* note 48, at 700–01.

[172] *See* Memorandum of Understanding Through Which the U.S. Census Bureau Is Acquiring Administrative Data from the Iowa Dep't of Transp. 2 (Mar. 5, 2020) (on file with the Harvard Law School Library); Memorandum of Understanding Through Which the U.S. Census Bureau Is Acquiring Administrative Data from the S.C. Dep't of Motor Vehicles 2 (July 2, 2020) (on file with the Harvard Law School Library) (specifying the initial payment and providing that if the Census Bureau requested additional data, it would tender additional payments).

[173] *See* Fahey, *supra* note 18, at 2401 ("[I]ntergovernmental agreements are not subject to any rules that ensure ease of access or access at all. Some are posted publicly on the websites of federal agencies. Others are published in the state regulatory compilation or made available on state websites. But many are not. There certainly exists no rule requiring that intergovernmental agreements be made available, and no general repository for such agreements at any level of government, hindering those they impact from learning of their content. Indeed, many such agreements are kept confidential." (footnotes omitted)).

intergovernmental agreements are often made by the parties who want to *use* the data, rather than the parties whose data it is, it will come as no surprise that they have great potential to underprotect privacy interests. Most significantly, though, they can serve as institution-creating documents — as charter-like instruments, which I explore next.

C. Cross-Governmental Bureaucracy

In the absence of a legislative guide, intergovernmental agreements can serve as something of an enabling act for cross-governmental data programs. And the larger, more sustained, and more permanent the program, the more infrastructure it requires. This section describes the unorthodox forms of ongoing management our levels of government have devised, in intergovernmental agreements and atop them, to manage and oversee joint data programs on a day-to-day basis. This is not a thorough catalog of the administrative structures that guide these data pools. My goal in this first look is instead to excavate examples that reflect the possibilities, drawbacks, and complexities of these institutions. They are *flexible*, enabling different governments to participate in common governing projects. They are *innovative*, using governing forms and processes without parallel in either federal or state administrative apparatuses. But they also, in many cases, have an *independence* that is striking, and not for the good. Although it is administrative law 101 that agencies are creatures of legislative (and in some state governments, constitutional) delegation, the institutions I discuss below generally lack a close tether to ordinary sources of political authority and accountability. And they are frequently *opaque*. They decline to publicize their inner workings, and tracing the authority under which they make policy is extremely challenging and in some cases not possible.

What is clear is that these unorthodox institutions further emphasize both the novelty and complexity of data pooling programs. Scholars have emphasized the increasing interdependence between the federal government and the states for some time.[174] These institutions give us a taste of what that integration looks like not just in theory, but on the ground.

1. Neither "Federal" nor "State": Fusion Centers. — As entrée into these institutions, consider the claim made repeatedly by the small group of scholars who write about fusion centers that they are "state-run" agencies.[175] This claim is often made despite the absence of any clear

---

[174] *See* sources cited *supra* note 26.

[175] Slobogin, *supra* note 3, at 1749; *see* Waxman, *supra* note 3, at 308 (describing fusion centers as "state-operated"); Daniel Poniatowski, Comment, *A Constructive Problem: Redemption of Unlawful Arrests via Fusion Centers*, 2014 WIS. L. REV. 831, 834 ("Fusion centers are also creatures of state, local, and tribal governments . . . ."). Even Professors Danielle Citron and Frank Pasquale,

reasoning to that effect or citation to a credible legal document substantiating that status. The available legal sources, instead, point in many directions. It is true that fusion centers are not part of the federal administrative apparatus and that they have no federal enabling acts or other legislative charters. But nor are they ordinarily supported by specific legislation in the states; their state participants instead draw their authority from "general statutes creating state police agencies or memoranda of understanding among partner agencies."[176] And in authorizing the Department of Homeland Security to provide support to them, Congress defines "fusion centers" as though the federal government is a constitutive member, not a mere advisor on the outside, as a "collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information."[177]

They are, moreover, staffed by personnel from federal, state, and local governments and funded jointly by all participating governments.[178] The federal government, as a consequence of this funding and the access that fusion centers have to federal data, has asserted the right to regulate certain fusion center operations.[179] Whereas many fusion centers are physically housed within state and local law enforcement agencies, over forty percent, an annual survey of these centers reports, are "colocated" in field offices of the FBI.[180] The closest things many fusions centers have to founding documents are the often-undisclosed intergovernmental agreements that structure them.[181] These are not, in short, obviously state institutions or obviously state run.

Their frequent characterization as creatures of state government, then, appears to stem from a category problem: Even as our governments co-manage joint assets — like data pools — and integrate their governance more than ever before, we still strive to assimilate their actions into a frame of separate federal and state governance. Agencies

---

who have recognized the difficulty of achieving accountability in fusion centers because administrative law is "built to address actions of individual agencies rather than the interactions of a network of agencies," Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1446 (2010–2011) (emphasis omitted), nevertheless characterize fusion centers as local institutions, explaining that "states and localities run fusion centers," *id.* at 1449.

176 THE CONST. PROJECT, *supra* note 121, at 6 (describing authority structure in the states). The federal government's participation in fusion centers is, counter the usual trend, authorized by statute in the 9/11 Commission Act.

177 6 U.S.C. § 124h(j)(1).

178 *See* DHS, 2018 FUSION CENTERS REPORT, *supra* note 69, at 4 (showing that these centers, on the whole, get roughly a third of their funding from the federal government).

179 *See Homeland Security Grant Program*, U.S. DEP'T OF HOMELAND SEC. (Aug. 9, 2021), https://www.dhs.gov/homeland-security-grant-program-hsgp [https://perma.cc/J98D-A37R] (conditioning the receipt of grant funds by any fusion center on compliance with, inter alia, certain privacy guidance).

180 *See* DHS, 2017 FUSION CENTERS REPORT, *supra* note 66, at 2.

181 *See id.* at 14; S. Nev. Counter-Terrorism Ctr. MOU, *supra* note 67, at 1–3.

are either *state* agencies or *federal* agencies. Fusion centers, along with the other formal and informal administrative structures I describe below, however, invite us to imagine a new category of *cross-governmental* institutions — ones that sit in federalism's interstitial spaces.

2. Formal Structure: The NCIC's Governance Multiplicity. — The National Crime Information Center is powered by no fewer than three distinctive multi-governmental bureaucracies, each serving a different function and reflecting a different set of institutional arrangements, revealing the flexibility and innovation (whether successful or not) of these governance institutions.

(a) Day-to-Day Management. — The FBI characterizes the NCIC's day-to-day governance as a "shared management concept," but that bureaucratic term masks an extraordinarily detailed set of arrangements.[182] The FBI maintains the database, but it "share[s] responsibility for the operation and management of all systems" with "local, state, tribal, and federal data providers and system users."[183] This shared oversight is operationalized by an intergovernmental board, the Criminal Justice Information Services (CJIS) Advisory Policy Board (itself supervising five additional "working groups").[184] The Advisory Policy Board has thirty-five members, who range from heads of state and local criminal justice agencies to delegates from contributing federal agencies to representatives of nongovernmental criminal justice associations.[185] The working groups have representatives from all fifty states and many local jurisdictions.[186]

The Board plainly possesses significant *functional* power. Its members, after all, generate, contribute, and use the data that is the lifeblood of the NCIC and can choose to withdraw their participation at any time. But, as is characteristic of administrative law in the cross-governmental space, the Board's *formal* power is less clear. For separation-of-powers reasons, advisory committees adjuncted to federal administrative agencies are ordinarily confined to issuing nonbinding guidance.[187] And

---

[182] *The CJIS Advisory Process: A Shared Management Concept*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/cjis/the-cjis-advisory-process [https://perma.cc/T7RG-BYK6].

[183] *Id.*

[184] *Id.* The Board is an outgrowth of an advisory board established in 1969 when the NCIC included only a few states, which — in turn — reflects the NCIC's origins in a system created by the National Association of Chiefs of Police. *See NCIC Turns 50: Centralized Database Continues to Prove Its Value in Fighting Crime*, FED. BUREAU OF INVESTIGATION (Jan. 27, 2017), https://www.fbi.gov/news/stories/ncic-turns-50 [https://perma.cc/SR3D-CXGJ] ("Working with the International Association of Chiefs of Police, the FBI created an advisory board of state and local police to develop nationwide standards . . . .").

[185] *The CJIS Advisory Process: A Shared Management Concept*, *supra* note 182.

[186] *Id.*

[187] *See* Federal Advisory Committee Act, Pub. L. No. 92-463, § 2(b)(6), 86 Stat. 770, 770 (Oct. 6, 1972) (codified at 5 U.S.C. app.); *see also* Jay S. Bybee, *Advising the President: Separation of Powers*

within the federal administrative state, the Advisory Policy Board's formal role appears to be limited to just that: providing nonbinding advice to the FBI Director, who may theoretically accept or disregard it.[188]

But its name notwithstanding, the CJIS Advisory Policy Board is not an ordinary federal advisory committee. Unlike ordinary federal advisory committees, the Board has an independent and nonfederal source of authority: the intergovernmental agreements that structure the NCIC. The intergovernmental agreement that all NCIC users (including all state and local law enforcement agencies) must sign "incorporate[s] by reference" the "Minutes of the CJIS Advisory Policy Board meetings," the "bylaws for the CJIS Advisory Policy Board and Working Groups," and NCIC Standards "as recommended by the CJIS Advisory Policy Board."[189] The agreements that structure participation in the NCIC, in other words, commit its users to following the Advisory Policy Board's guidance, whatever its status as independent federal agency action.[190]

(b) Access for Non–Criminal Justice Purposes. — The NCIC's governance is further complicated by a second bureaucracy that oversees a precise, but significant, function of the NCIC: the exchange of criminal justice data for purposes unrelated to criminal law enforcement, like civil background checks, housing applications, and vetting for public sector employment. Not all states that use the NCIC endorse access to it for purposes outside of the criminal justice context. The states that *do* wish to share their NCIC data for non–criminal justice purposes have, thus, enacted an interstate compact to govern their exchange of data for those purposes specifically.[191] The National Crime Prevention

---

and the Federal Advisory Committee Act, 104 YALE L.J. 51, 56 (1994) (noting that "[advisory committees] have no authority to bind the government" but are instead focused on the "search, production, and distribution of the truth" (quoting Letter from President Herbert Hoover to W.C. Thompson (Jan. 1930))).

188 *The CJIS Advisory Process: A Shared Management Concept*, *supra* note 182 (describing the process through which the Board communicates with "the Director to apprise him of [its] recommendations on agenda items and to secure his concurrence with these recommendations").

189 U.S. DEP'T OF JUST., NCIC 2000 OPERATING MANUAL § 4.2 (2000) (emphasis omitted) (on file with the Harvard Law School Library) [hereinafter NCIC 2000 OPERATING MANUAL].

190 *The CJIS Advisory Process: A Shared Management Concept*, *supra* note 182.

191 National Crime Prevention and Privacy Compact Act of 1998, Pub. L. No. 105-251, § 212, 112 Stat. 1,870, 1,874 (codified at 34 U.S.C. § 40316); *see also* NAT'L CRIME PREVENTION & PRIV. COMPACT COUNCIL, FREQUENTLY ASKED QUESTIONS REGARDING THE NATIONAL CRIME PREVENTION AND PRIVACY COMPACT ACT OF 1998, at 2 (2015) [hereinafter COMPACT FAQS], https://ucr.fbi.gov/cc/library/compact-frequently-asked-questions [https://perma.cc/P72Z-RWED]. *Interstate* compacts are a specialized form of intergovernmental agreement, which are constitutionally governed by the Compacts Clause. U.S. CONST. art. 1, § 10, cl. 3 (requiring congressional approval for interstate compacts); *see* Virginia v. Tennessee, 148 U.S. 503, 520–22 (1893) (allowing compacts that do not affect federal power to proceed without congressional approval). The intergovernmental agreements discussed in the last section are between states and the *federal government* and therefore not subject to the Compacts Clause.

and Privacy Compact was approved and joined by Congress in 1998 and became effective the following year when the first states ratified it.[192] Today, it has thirty-four members.[193]

The Compact, in turn, established a governing council comprised of state representatives and federal agencies.[194] Significantly, unlike the CJIS Advisory Policy Board, the Council *is* vested with binding administrative authority — though the basis of this authority is again hard to assimilate into an ordinary federal (or, for that matter, state) administrative law frame. The Compact itself is the instrument that allows the Council to "promulgate rules and procedures" governing the exchange of information for non–criminal justice purposes.[195] And although the Council does not identify as, and almost certainly could not be considered, a federal agency (since it is comprised largely of nonfederal representatives), the Compact directs the Council to borrow the federal government's administrative infrastructure, promulgating the rules it issues in the Federal Register.[196] The Compact further provides that disputes between its parties, over its meaning or concerning "any rule or standard" it promulgates, must be heard in the first instance by the Council itself through a "hearing" after which a decision may follow only by "a majority vote of the members of the Council."[197] (I am not aware of any efforts to seek judicial review of rules made by the Compact Council, nor is it obvious what law would govern such a challenge.) It also vests judicial oversight over any appeal in the federal courts, but does not specify — and there do not appear to be any cases testing — what law would apply to an administrative challenge in such a setting.[198]

(c) Telecommunications and Verification. — Completing the dizzying network of intergovernmental bureaucracies that oversee the exchange of criminal justice information is the secretive Nlets telecommunications network. Nlets allows states to directly access the state-level databases that feed into the NCIC in order to verify the information obtained through NCIC searches and conduct other state-to-state data transfers and comparisons.[199] It also allows some participants to access

---

[192] *See* National Crime Prevention and Privacy Compact Act of 1998 § 214; COMPACT FAQS, *supra* note 191, at 2.

[193] *The National Crime Prevention and Privacy Compact Act of 1998*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/cjis/compact-council [https://perma.cc/7XQT-V4GF].

[194] National Crime Prevention and Privacy Compact Act of 1998 art. VI.

[195] *Id.* art. VI(a)(1).

[196] *Id.* art. VI(e).

[197] *Id.* art. XI(a).

[198] *See id.* art. XI(c).

[199] NCIC 2000 OPERATING MANUAL, *supra* note 189, § 3.5 (indicating that Nlets "is the recommended network for hit confirmation" between the "agency that received the hit and the agency that enters the record").

additional databases not present in the NCIC.[200] Nlets is not housed in either the state or federal government, but is instead a private not-for-profit organization founded by the states and governed by participating law enforcement agencies.[201] It is already challenging to conceptualize government-owned corporations as legal institutions when they exist within the boundaries of a *single* government. Those challenges are multiplied when, like Nlets, they exist between and across governments. The most significant consequence of Nlet's distinctive public/private form is the organization's highly furtive behavior — it does not disclose comprehensive information about its activities, funding, or policies and publicly discusses its activities at only the highest level of generality. It acts, in short, like a private entity, not a government institution, though it serves as gatekeeper to a sweeping amount of government data.

3. Informal Administration: Street-Level Bureaucracy and Immigration Data. — But data of significance and in significant volumes often moves between federal, state, and local custody not through centrally managed programs, but at the periphery: through line-level implementers, or what Michael Lipsky calls "street-level bureaucrats."[202] Since Lipsky's path-marking manuscript on the policymaking power of these actors, administrative law scholars have trained significant attention on how frontline government officials exercise discretion and on the "agency behavior" that discretion "add[s] up to" "when taken in concert."[203] This section illustrates the ways that street-level bureaucrats use their discretion over the data they manage to jointly initiate and oversee data transactions with their counterparts in other levels of government.[204] Line-level actors can, in effect, forge intergovernmental data sharing

---

[200] *What We Do*, NLETS, https://nlets.org/about/what-we-do [https://perma.cc/UQG8-ZQCJ]; *see also Message Keys*, NLETS, https://nlets.org/resources/maps/message-keys/key [https://perma.cc/8A7Y-Y5FJ] (noting, for instance, that users can access data held by Interpol).

[201] *Who We Are*, NLETS, https://nlets.org/about/who-we-are [https://perma.cc/9HLT-YZVC].

[202] *See generally* MICHAEL LIPSKY, STREET-LEVEL BUREAUCRACY: DILEMMAS OF THE INDIVIDUAL IN PUBLIC SERVICES (1980).

[203] *Id.* at 13; *see also* Shannon Portillo & Danielle S. Rudes, *Construction of Justice at the Street Level*, 10 ANN. REV. L. & SOC. SCI. 321, 324–26 (2014) (summarizing social science literature).

[204] As Professor Nestor Davidson has recently documented, scholars have historically paid little attention to local administrative law as a legal domain. Nestor M. Davidson, *Localist Administrative Law*, 126 YALE L.J. 564, 574–75 (2017). So it is no surprise that the same expanse of white space characterizes administrative perspectives on the relationships among federal, state, and local agents. Federalism scholars have periodically mentioned "picket-fence federalism" — a term used to capture the axis of interconnection that administrative agents (the *pickets*) forge between federal, state, and local governments (the *rails*), but those accounts remain largely theoretical. *See, e.g.*, Jessica Bulman-Pozen & Heather K. Gerken, *Uncooperative Federalism*, 118 YALE L.J. 1256, 1270 (2009) ("[S]o powerful are these connections that state and federal administrators of a single program may band together on the basis of their functional specialties and bureaucratic culture . . . ."); Roderick M. Hills, Jr., *The Eleventh Amendment as Curb on Bureaucratic Power*, 53 STAN. L. REV. 1225, 1236 (2001).

programs through informal relationships with their counterparts in other governments.

This process is particularly vivid in the immigration context. Because the number of federal immigration enforcement agents is dwarfed by the number of state and local police, the collaboration of local law enforcement is an enticing force-multiplication strategy for federal policymakers.[205] Across at least three presidential administrations, the federal government has placed access to the immigration information held by state and local police at the core of its immigration strategy. But as discussed above, states and cities have increasingly resisted formal proposals to collaborate on both normative grounds (out of a desire to protect members of their communities regardless of immigration status) and efficacy grounds (arguing that community members will be less cooperative with local police if they fear federal immigration consequences). As local elected officials have held back cooperation, federal immigration agents have shifted their strategy to forging data exchange projects with line-level bureaucrats instead.

These line-level data sharing initiatives can take many forms. The previously mentioned "sanctuary city" litigation is at bottom about immigration-related data sharing. The statute the federal government is seeking to enforce — and whose constitutionality is under challenge — is 8 U.S.C. § 1373. It prohibits states from, in turn, prohibiting their employees from sharing information with ICE.[206]

Section 1373 does not stand up its own data exchange program. Rather, it intervenes in local and national street-level bureaucracies to encourage the agents on each government's margin to develop information-exchange initiatives of their own. By making it unlawful for states or cities to prohibit their officers from sharing information with ICE, § 1373 *detaches* local police from the immigration-related information controls of their state and city administrators and policymakers, instead empowering the individual employee to write data policy on her own. In turn, it encourages ICE to go directly to the street-level officials rather than negotiating an information-exchange program with state or local policymakers.[207] As discussed below, that process is

---

[205] *Compare* Waxman, *supra* note 3, at 291 ("There are more than 700,000 local police officers from about 17,000 state and local law enforcement agencies."), *with* CONNOR BROOKS, U.S. DEP'T OF JUST., NCJ 251922, FEDERAL LAW ENFORCEMENT OFFICERS, 2016 — STATISTICAL TABLES, at 3 (2019), https://bjs.ojp.gov/content/pub/pdf/fleo16st.pdf [https://perma.cc/6HMX-HL8S] (counting 12,400 agents with Immigration and Customs Enforcement and 43,724 agents with Customs and Border Protection as of 2016).

[206] 8 U.S.C. § 1373(a), (b)(3) ("[A] Federal, State, or local government entity or official may not prohibit, or in any way restrict, any government entity or official from sending to, or receiving from, [ICE] information regarding the citizenship or immigration status, lawful or unlawful, of any individual." *Id.* § 1373(a)).

[207] A notable exception is the Secure Communities program, which was initially structured with the consent of high-level officials in state and local jurisdictions, and which I discuss further *infra* section III.A, pp. 1055–58.

often conducted by federal decisionmakers who are bureaucratically congruent to their state targets: by low-level ICE agents and field offices who have relationships with the individual state and local police officers that § 1373 empowers to share information. Important information initiatives and projects, thus, can be the brainchild of street-level bureaucrats on both sides.

Information about immigration enforcement, including how federal agents collaborate with local police, is not routinely made public. But documents obtained by the American Immigration Council through the Freedom of Information Act provide a window into at least some of these initiatives. A compilation of initiatives proposed by the ICE Atlanta Field Office (under pressure to meet annual deportation targets) and approved for use in the field reveals the breadth and creativity of programs conceived by ICE field agents and their local criminal justice counterparts to share immigration-related information.[208]

Seeking information from police encounters that do not result in arrest, Atlanta field agents proposed, for instance, an initiative to join local police at traffic checkpoints — fixed locations used to randomly stop vehicles and administer DUI tests. In the proposal, when local police find evidence of a traffic or criminal violation at the checkpoint, vehicles are then sent to a "secondary location" at which ICE is also present to "interview all individuals we deem necessary."[209]

ICE agents have also found other ways to obtain data from local police encounters that do not result in arrest. For instance, ICE sought to form a task force with a local police department to mine notes from such encounters, arguing that "[t]here are a tremendous number of local law enforcement encounters that occur on a daily basis where the individual is the subject of a traffic ticket or warning or a field interview and is *not* taken into custody."[210] The Field Office explained that, if it could "look at the data from these types of encounters and run them through our databases," it was "likely to identify a number of aliens."[211] It observed that the "average midsize police department issues between 250 and 400 traffic tickets per week and completes 50+ field interview cards," which "is a lot of data that is being collected that ICE could look into."[212]

---

[208] *See* Email from [redacted] to [redacted] (May 4, 2012, 8:08 AM), https://assets.documentcloud.org/documents/603861/ice-documents.pdf [https://perma.cc/8ADM-R46W].

[209] Memorandum from U.S. Immigr. & Customs Enf't, Enf't & Removal Operations, Atlanta Field Off., on Prospective Criminal Apprehension Initiatives 4 (Apr. 18, 2012) [hereinafter ICE Atlanta Field Office Memo], https://assets.documentcloud.org/documents/603861/ice-documents.pdf [https://perma.cc/9MMQ-WFCV].

[210] *Id.* at 8.

[211] *Id.*

[212] *Id.* at 7–8.

Understanding that police are not the only local law enforcement officials who may have immigration-related information, the Field Office also sought to direct information requests to other relevant local officials. For instance, it proposed asking the probation and parole departments in local counties to share information on current and former foreign-born individuals on probation, which officers would then vet for individuals eligible for deportation.[213] And it suggested contacting Georgia's county solicitors (who prosecute county-level misdemeanor offenses) to obtain "current rosters for their General Sessions Court Cases" to "vet the lists for any foreign born criminal aliens and . . . try to apprehend" them.[214]

Finally, the Field Office proposed several initiatives that would tap a long-standing conduit of state information to federal officials: the state DMV. It proposed working with the Georgia DMV's License & Theft Division to use the state's facial recognition technology to "screen potential fraud cases" (of interest because of the assumption that noncitizens may use fraudulent documents when applying for a license) to identify individuals wanted by ICE.[215] It suggested obtaining a "list of temporary driver licenses issued to foreign-born applicants."[216] And it advocated soliciting a list of individuals whose license applications were denied "due to lacking proof of residency" to develop a "foreign-born target base" to "be vetted further" for individuals with past criminal convictions.[217]

* * *

These structures reveal that intergovernmental data sharing is not a simple exchange of governmental goods. It precipitates a subsequent process of intergovernmental data oversight and, in some cases, the creation of integrated governmental institutions to manage data on an ongoing basis. Much about these institutions remains to be discovered. What is clear is that a person who wants to know how "the government" stewards her data — because she is concerned about her privacy, or worried about her data's security, or believes her data is incomplete or misleading, or thinks it was obtained or is being used unlawfully — would face an almost insurmountable task. She would have to peer into institutions that traverse governmental boundaries; see the logic of institutions that do not coherently divulge how they function or even sometimes what they do — a logic that the officials who inhabit these institutions may not fully know themselves; consult structuring

---

213 *See id.* at 6.
214 *Id.* at 7.
215 *Id.* at 5.
216 Email from [redacted] to [redacted], *supra* note 208, at 2.
217 ICE Atlanta Field Office Memo, *supra* note 209, at 5.

agreements that are not always disclosed and are never easy to locate; and query decisions not fully domesticated by either federal or state law.

These intergovernmental practices thus raise challenging questions about the institutions that govern us. Ordinarily, questions of institutional design and federal-state interaction would find outer guideposts in the Constitution. The next Part considers the structural constitutional issues that arise from data sharing, but also explores the limits of existing constitutional doctrine to confront the full scope of federalism-inflected problems these arrangements produce.

III. DOCTRINE FOR THE INTERGOVERNMENTAL DATA MARKET

The transactions documented in Part I resemble in important ways other, now-familiar forms of intergovernmental negotiation. Our governments routinely establish "cooperative federalism" programs by trading governmental assets, typically money and administrative capacity.[218] Constitutional doctrines derived from the text and function of the Spending Clause, the Tenth Amendment, and structural federalism principles set forth the "rules of engagement" for these initiatives.[219] Most importantly, they ensure that federal-state collaborations are created voluntarily by both governmental parties.

Those rules of engagement are the most obvious source of constitutional guardrails for data federalism, but they require adaptation. Does the anti-commandeering rule, which prohibits the federal government from requiring states to "enact or administer a federal regulatory program," also disallow federal efforts to require data sharing?[220] Do doctrines that structure how the federal government and states negotiate spending programs — like the anti-coercion rule and the *Pennhurst* clear statement rule — regulate the formation of data programs too, even if they entail no expenditure of funds?

The task of deciding how, and whether, these rules apply to data transactions has generally confounded the few courts to have attempted it. And, because the roadmap is so thin, even colorable constitutional claims are not pressed in many data-related disputes. This Part begins by setting forth that roadmap — understanding the ways data transactions complicate the straightforward application of these doctrines and arguing that they should apply nonetheless.

But those doctrines, in the end, police only one form of structural harm that can arise in intergovernmental data programs — harm related to the voluntariness of the government-government relationship. As Part II illustrates, however, there are many structural problems that can

---

[218] *See* Fahey, *supra* note 18, at 2336–52.

[219] *Id.* at 2335 n.17 (collecting sources).

[220] Printz v. United States, 521 U.S. 898, 926 (1997).

arise not because of tension between governments at a program's conception, but because of the institutions they readily and voluntarily create: institutions that can escape accountability and transparency, avoid legal oversight, and empower governments at the expense of their constituents, among many other potential concerns. Even fully applying the anti-commandeering, anti-coercion, and *Pennhurst* clear statement rules to data sharing will leave many of the unusual structural arrangements precipitated by data federalism untouched by constitutional doctrine. I therefore conclude by reflecting on the limits of existing federalism doctrine to address the full scope of structural problems data federalism may raise.

A. The Constitutional Significance of Data Transactions

To see some of the potential constitutional stakes of data federalism, consider the federal government's efforts to obtain the data cities and states collect about their immigrant populations. Sanctuary cities generally decline federal invitations to share immigration-related data. But — as discussed above — 8 U.S.C. § 1373, a law enacted by the Clinton Administration and enforced by every administration through the Trump presidency, and the portfolio of increasingly aggressive tactics used to enforce it, try to prohibit states from choosing to withhold that information. The law plainly tries to take, without consent, immigration-related data from states and cities. Ordinarily, federal directives to states would raise questions of unconstitutional commandeering. But in one of its early commandeering cases, the Supreme Court suggested that the rule may have an "information-sharing exception," which would exempt data transactions from its protections.[221] Some of the few courts to address data transactions, moreover, have embraced that exception — seemingly offering the federal government carte blanche to requisition state data even as those courts concede that it may not take other state assets.[222]

When states and cities have expressed an unwillingness to share immigration-related data with the federal government, the federal government has used aggressive tactics that in the context of state-federal grant programs would be scrutinized as unconstitutional

---

[221] *See id.* at 917–18.

[222] *See, e.g.*, United States v. Brown, No. 07 Cr. 485, 2007 WL 4372829, at *5 (S.D.N.Y. Dec. 12, 2007) (noting that a since-repealed statute requiring states to contribute information about sex offenders to a national database was not unconstitutional because it "merely requires state officials to provide information regarding sexual offenders — information that the state officials will typically already have through their own state registries — to the federal government" (citing *Printz*, 521 U.S. at 918)); Freilich v. Bd. of Dirs. of Upper Chesapeake Health, Inc., 142 F. Supp. 2d 679, 696–97 (D. Md. 2001). A few, by contrast, have rejected a possible information sharing exception. *See, e.g.*, City of Philadelphia v. Sessions, 309 F. Supp. 3d 289, 330 (E.D. Pa. 2018) ("Defendant relies on dicta from *Printz* [for the proposed exception]. This snippet is actually part of a paragraph in which the Court summarized the Government's (failed) arguments . . . ." (citation omitted)), *aff'd sub nom.* City of Philadelphia v. Att'y Gen., 916 F.3d 276 (3d Cir. 2019).

coercion and deception. Consider the Secure Communities program, a DHS initiative designed to allow the agency access to an enormous quantity of state and local data about noncitizens. It would be difficult to overstate the significance of Secure Communities to federal immigration enforcement and, by the same token, to state and local interactions with immigrant communities. As elaborated above, the program, which was established in 2008, had two central components. First, it had a data sharing component, in which the federal government obtained data from state and local governments regarding individuals arrested by state and local police and checked that data against federal immigration databases.[223] Second, it had a prioritization component, in which the federal government prioritized removable individuals with serious criminal records for enforcement action over removable individuals without a criminal history. The formal, written agreements that initiated the program traded one component (the federal prioritization commitment) for another (the state and local arrestee data).[224]

The data sharing initiative was initially portrayed by DHS as entirely voluntary, a characterization heavily emphasized by the Obama Administration during President Obama's first year in office. But when state and local jurisdictions — cities and counties like San Francisco, California and Arlington County, Virginia, as well as the states of Illinois, New York, and Massachusetts — sought to exercise the termination clauses in their formal agreements (which allowed either party to withdraw with thirty days' notice[225]), then–DHS Secretary Janet Napolitano terminated all of the agreements.[226] She did not, however, scuttle the program. Instead, she announced that it would continue *involuntarily* going forward. "We don't consider Secure Communities an opt-in, opt-out program," she said during a press conference.[227]

That is the kind of language that would immediately trigger talk of federal overreach in a more traditional federal-state program. But states did not press this claim in court. One reason perhaps is the federal government's deliberate efforts to ward off such a challenge. Perhaps not wanting to bet on the potential information sharing exception to the anti-commandeering rule, DHS tried to head off a charge of commandeering by pointing out that states were not required to send any new information to DHS — or, indeed, to send *any* information directly to

---

223 *Secure Communities*, *supra* note 120.

224 *See* N.Y.-ICE Memorandum, *supra* note 82.

225 *See id.*

226 Tyrese Griffin, *Undeterred by Government Reversal, Communities Keep up Fight to Opt out of Immigration Program*, WASH. INDEP. (July 31, 2020), https://washingtonindependent.com/100029/undeterred-by-government-reversal-communities-keep-up-fight-to-opt-out-of-immigration-program [https://perma.cc/95KW-Z6UL]; *see* Gretchen Gavett, *Why Three Governors Challenged Secure Communities*, PBS (Oct. 18, 2011), https://www.pbs.org/wgbh/frontline/article/why-three-governors-challenged-secure-communities [https://perma.cc/83T7-72JD].

227 Griffin, *supra* note 226.

DHS at all — because of the technical way the data sharing component of Secure Communities actually worked. States sent arrestee biometric data, as they long have, to the National Crime Information Center as part of its voluntary program for sharing general policing data with the FBI and jurisdictions across the country. The FBI, in turn, operationalized Secure Communities by forwarding that data to DHS. It is true, DHS conceded, that states and cities had no say in whether the FBI forwarded their data to DHS. But, DHS maintained, they were not being commandeered because the data was supplied to the *FBI* willingly and "no agreement with the state is legally necessary for one part of the federal government to share it with another part."[228]

But what about the other constitutional doctrines that courts have used to protect states and localities when entering into cooperative federalism programs? The anti-coercion rule, which arose in the context of federal-state grant programs, prohibits the federal government from using financial inducements that "pass the point at which 'pressure turns into compulsion'" to secure state participation in grant programs.[229] And the *Pennhurst* clear statement rule requires the federal government to state "condition[s] on the grant of federal moneys . . . unambiguously" so that states can "knowingly accept[] the terms" of the joint program.[230]

The effort to operationalize Secure Communities by leveraging the preexisting NCIC program mirrors almost exactly the constellation of inducements that the Supreme Court found to be unconstitutionally coercive in its most recent anti-coercion case, challenging the Affordable Care Act's Medicaid expansion.[231] The Medicaid expansion offered states additional funding for Medicaid — an enormous and decades-long program that had become deeply embedded in state governance — in exchange for their commitment to expand their programs to cover incremental populations. But the additional funding to cover new populations was not the only inducement for participating in the expansion. "Instead of simply refusing to grant the new funds to States that will not accept the new conditions, Congress . . . also threatened to withhold those States' *existing* Medicaid funds," a condition that an unusual seven-Justice coalition found unconstitutional.[232]

But, if we substitute data for money, that is just what DHS did in linking Secure Communities to the NCIC: It conditioned continued state

---

[228] Letter from John Morton, *supra* note 83, at 1 (highlighting that the data is supplied by state and local law enforcement "voluntarily . . . to the federal government").

[229] NFIB v. Sebelius, 567 U.S. 519, 580 (2012) (opinion of Roberts, C.J.) (quoting South Dakota v. Dole, 483 U.S. 203, 211 (1987)).

[230] Pennhurst State Sch. & Hosp. v. Halderman, 451 U.S. 1, 17 (1981).

[231] *NFIB*, 567 U.S. at 579–80 (opinion of Roberts, C.J.).

[232] *Id.* (emphasis added) (joined by Breyer and Kagan, JJ.); *see id.* at 681 (Scalia, Kennedy, Thomas, and Alito, JJ., dissenting) ("If the anti-coercion rule does not apply in this case, then there is no such rule.").

access to a deeply-rooted, long-standing data pool — described as the "lifeblood of law enforcement" — on states' agreement to participate in the new and incremental Secure Communities program.[233] By connecting the NCIC and Secure Communities, the federal government essentially said: "If you do not agree to your data being used for Secure Communities, you cannot participate in the NCIC either." As *The Washington Post* correctly observed at the time, the "only way a local jurisdiction could opt out of [Secure Communities] is if a state refused to send fingerprints to the FBI."[234] Or, in DHS's words, "a jurisdiction cannot choose to have the fingerprints it submits to the federal government processed *only* for criminal history checks."[235]

DHS's retroactive recharacterization of Secure Communities as part of the NCIC also draws attention to a potential *Pennhurst* problem: Was it "unambiguous" when states agreed to participate in the NCIC that the NCIC may later be used to advance initiatives like Secure Communities?[236]

The rub is that to even get into court, an anti-coercion or *Pennhurst* claim would require a city or state challenger to convince the judge that those rules apply beyond the context of federal grant programs — that they apply when the federal government is using data, not money, as coercive leverage, and including deceptively ambiguous terms in data sharing agreements, rather than grant conditions.

Because money was central to the origination of those doctrines, states, cities, and courts have hesitated to invoke and enforce structural constitutional rules in the data context, even where — as in the Secure Communities and sanctuary cities contexts — it is apparent that states and cities are not sharing their data voluntarily. That hesitation is not surprising, at least as a descriptive matter, given that the process of adapting old rules to new technologies can be halting in many contexts. As I show in the next section, however, most of the justifications for declining to apply structural constitutional rules to intergovernmental data exchange do not withstand scrutiny.

---

[233] FBI, This Week Podcast, *NCIC Enters Its 50th Year*, FED. BUREAU OF INVESTIGATION (Feb. 16, 2017) https://www.fbi.gov/audio-repository/ftw-podcast-ncic-50th-anniversary-021617.mp3/view [https://perma.cc/62YK-EZ8H] (statement of John Derbas, Deputy Assistant Director, Criminal Justice Information Services Division).

[234] Vedantam, *supra* note 83.

[235] *Secure Communities*, *supra* note 120.

[236] The answer to that question is almost certainly no: The NCIC was initiated decades before Secure Communities and, as noted earlier, the NCIC is thin on legal structuring, excepting the initial agreements states submitted in the mid-1970s. And Secure Communities is a program of the Department of Homeland Security, which was not the federal counterparty to state and local NCIC agreements.

B. Data Federalism's Rules of Engagement

A literal doctrine parser could find ammunition for excluding data transactions from the anti-commandeering, anti-coercion, and *Pennhurst* clear statement rules. When the anti-commandeering rule was first described in the mid-1990s, it involved the federal government's effort to compel state legislative and executive action — to effectively requisition states' *administrative* and *regulatory* power by mandating they be used to federal ends.[237] Those cases left uncertain the degree to which the federal government could forcibly commandeer other forms of state power or other kinds of state assets.

The anti-coercion and *Pennhurst* clear statement rules, meanwhile, suffer from a different problem. They originated in disputes involving programs enacted pursuant to the Constitution's Spending Clause, which governs how the federal government makes expenditures. And the Court has yet to apply them in cases where the federal government uses other forms of power as leverage or attaches ambiguous conditions to programs centered on exchanges of nonmonetary powers, leaving open whether they apply to transactions involving data.

In answering these questions, I do not argue from constitutional first principles. If there is an area of constitutional doctrine that cannot be methodologically pigeonholed, it is federalism doctrine. The opinions that form the core of these doctrines cite originalist sources, textualist support, intertextual logic, structural inference, and — like so many federal separation-of-powers cases — practice over time. In this initial effort to situate data federalism in constitutional doctrine, I take these doctrines on their own terms and ask whether their basic logic can apply to data and data transactions. This initial analysis of data federalism is thus in the spirit of common law constitutionalism.[238]

1. The Anti-commandeering Rule. — The anti-commandeering rule bars the federal government from requisitioning elements of state and local government for use in federal programs.[239] Since the rule's origination in a pair of Rehnquist Court opinions, *New York v. United States*[240] in 1992 and *Printz v. United States*[241] in 1997, however, courts and commentators have flirted — with little reflection or specific justification — with a so-called "information-sharing exception" to the rule, which would allow state data, unique among other assets, to be taken

---

[237] Printz v. United States, 521 U.S. 898, 926 (1997).

[238] *See generally* David A. Strauss, *Common Law Constitutional Interpretation*, 63 U. CHI. L. REV. 877 (1996).

[239] *Printz*, 521 U.S. at 926.

[240] 505 U.S. 144 (1992).

[241] 521 U.S. 898.

on command.[242] But Parts I and II show that there is little basis for distinguishing data from other assets in this way, and thus no principled reason to exempt it from the anti-commandeering rule's sweep.

The proposed exception stems from an aside by Justice Scalia in his majority opinion in *Printz*, the second canonical anti-commandeering case. In the first anti-commandeering case, *New York*, Congress had instructed each state to enact a regulatory program to dispose of the low-level radioactive waste produced within the state.[243] If a state refused, the federal government required the state government to "take title" to the relevant waste, in effect absolving private producers of liability for the dangerous refuse by transferring it to the state.[244] The Court concluded that both the initial instruction and the penalty impermissibly "'commandeer[ed]' state governments into the service of federal regulatory purposes" by "command[ing] state legislatures to legislate" according "to Congress' instructions."[245]

When *Printz* arose five years later, the Court applied the anti-commandeering rule to a different congressional effort to command assistance from state governments. There, instead of directing state legislatures to enact law, Congress instructed state administrative officials to help operationalize a federal program by performing a series of federally prescribed administrative tasks, including searching state databases.[246] The Court held that Congress could not "compel[] [the] enlistment of state executive officers for the administration of federal programs," just as it could not so compel state legislatures.[247]

But Justice Scalia, writing for the Court, reserved judgment about programs that "require only the provision of information to the Federal Government" because such programs "do not involve the precise issue before us here, which is the forced participation of the States' executive in the actual administration of a federal program."[248] *Printz* did not clarify what features might distinguish the commandeering of information from the commandeering of state executive apparatuses. But the Court's impetus for making that reservation provides a clue. The Court's observation about data commandeering responds to an argument in the federal government's brief: that it would be disproportionate to strike down federal programs that required only "limited local assistance" in the form of "the collection, reporting, and dissemination of

---

[242] *See, e.g.*, Mikos, *supra* note 3, at 134 ("The conventional wisdom is that constitutional federalism doctrines do not prohibit the federal government from forcing the states to disclose information.").

[243] *New York*, 505 U.S. at 151–52.

[244] *Id.* at 175.

[245] *See id.* at 162, 175, 179.

[246] *Printz*, 521 U.S. at 904–05.

[247] *Id.* at 905.

[248] *Id.* at 918; *see also* Brief for the United States at 31, *Printz*, 521 U.S. 898 (Nos. 95-1478, 95-1503), 1996 WL 595005.

information" on commandeering grounds.[249] Such programs, the federal government reasoned, "enlist local officials in *limited*, nonpolicymaking aspects of the implementation of federal law," and so are unlikely to "undermine the functioning of the States."[250]

The federal government's argument, in short, was that forced data sharing could not significantly affect our system of federalism because it is by its nature limited and has no meaningful effect on policymaking. In her concurring opinion, Justice O'Connor echoed that claim, noting that the Court was right to "refrain[] from deciding whether other *purely ministerial* reporting requirements imposed by Congress on state and local authorities pursuant to its Commerce Clause powers are similarly invalid."[251] In dissent, Justice Stevens picked up the same thread, arguing that the "enactment of statutes that *merely* involve the gathering of information . . . do not raise even arguable separation-of-powers concerns."[252]

Professor Robert Mikos has offered one persuasive response to this argument — that to commandeer data, the federal government must generally also commandeer state legislative and executive functions, which *New York* and *Printz* expressly prohibit. Enforcing federal law, Mikos observes, includes not just policing, prosecution, and punishment, but also investigative tasks like "gathering and reporting information — via inspections, investigations, surveillance, etc. — about regulated activities."[253] Requiring states to gather and report information, at least when that investigative work is performed by administrative officials, thus mandates exactly the enforcement of federal law by state officials that *Printz* proscribes. Data commandeering, Mikos adds, also imposes substantially the same economic and political costs that troubled the Court in *New York* and *Printz*: It requires states to expend resources to collect the data the federal government seeks, and it diminishes their policymaking authority and political accountability by making them complicit in federal programs.[254] Some of the courts that have considered the vitality of the information sharing exception since *Printz* — largely in the high-profile "sanctuary cities" litigation — have, relying in part on the kind of reasoning that Mikos advances, correctly rejected the government's arguments that such an exception exists.[255]

---

[249] Brief for the United States, *supra* note 248, at 11.

[250] *Id.* (emphasis added).

[251] *Printz*, 521 U.S. at 936 (O'Connor, J., concurring) (emphasis added).

[252] *Id.* at 960 n.22 (Stevens, J., dissenting) (emphasis added).

[253] Mikos, *supra* note 3, at 158; *see id.* at 158–59.

[254] *See id.* at 159–64.

[255] *See* City of Chicago v. Sessions, 321 F. Supp. 3d 855, 866–73 (N.D. Ill. 2018), *aff'd sub nom.* City of Chicago v. Barr, 961 F.3d 882 (7th Cir. 2020); City of Philadelphia v. Sessions, 309 F. Supp. 3d 289, 325–31 (E.D. Pa. 2018), *aff'd in part, vacated in part sub nom.* City of Philadelphia v. Att'y Gen., 916 F.3d 276 (3d Cir. 2019). The "sanctuary cities" litigation has given rise to substantial academic commentary, some of which likewise argues that there should be no information sharing exception. *See, e.g.*, Bernard W. Bell, *Sanctuary Cities, Government Records, and the Anti-*

But other courts have accepted them, so there remains work to be done.[256]

In light of the data sharing practices canvassed in this Article, there are additional reasons there can be no data sharing exception to the anti-commandeering rule.

First, the argument that data is too trivial a resource to be "commandeered" is plainly wrong in light of the breadth and import of data exchange across governments documented in Part I. The data revolution was well underway in 1997, so the dismissive characterizations of data sharing mandates by the Solicitor General and Justices O'Connor and Stevens were out of step even when they were made, and they surely cannot be taken seriously today. The sharing of sensitive data about individuals to further consequential policy programs cannot in almost any case be characterized as a "nonpolicymaking" act. Just the basic decision to share data at all *is* quintessential policymaking. It is a choice to enable governmental action that requires data aggregation, whether that action is data analytics, tracking and investigation, or verifications and validations. The terms on which governments transfer data only deepen the policymaking character of data sharing. When data is shared, it sheds the protections — against insecurity, inaccuracy, and improper use — that its initial custodian placed upon it, unless those protections are carefully negotiated in the kind of intergovernmental agreement discussed above. The process, then, of structuring data sharing programs is its own policymaking process (a step that *mandatory* data sharing would almost certainly bypass).[257] Both the decision to share and the choice of sharing terms are thus policymaking acts.

Second, seeing how our governments transact in data as a discrete governmental asset — one that can be alienated, transferred, and used to advance a range of policy ends — suggests a simpler reason that the anti-commandeering framework should apply to data mandates. When the federal government tries to mandate data sharing, it is doing something akin to taking other concrete state assets, like money or land.[258] It is true that the anti-commandeering cases confront federal efforts to

---

commandeering Doctrine, 69 RUTGERS U. L. REV. 1553, 1560, 1580–91 (2017) (arguing that 8 U.S.C. § 1373, the statute that bars states from limiting immigration-related information sharing, unconstitutionally commandeers states by depriving them of control over their employees); Nathaniel F. Sussman, Note, *On Immigration, Information, and the New Jurisprudence of Federalism*, 93 S. CAL. L. REV. 129, 130–31 (2019).

256 United States v. Brown, No. 07 Cr. 485, 2007 WL 4372829, at *5–6 (S.D.N.Y. Dec. 12, 2007), *aff'd*, 328 F. App'x 57 (2d Cir. 2009); Freilich v. Bd. of Dirs. of Upper Chesapeake Health, Inc., 142 F. Supp. 2d 679, 696–97 (D. Md. 2001), *aff'd sub nom.* Freilich v. Upper Chesapeake Health, Inc., 313 F.3d 205 (4th Cir. 2002).

257 *See* Mikos, *supra* note 3, at 128–33.

258 Indeed, the Enclave Clause assumes as much by explicitly requiring "the Consent of the Legislature of the State" for the federal government to assume jurisdiction over state land needed for federal "Forts, Magazines, Arsenals, dock-Yards, and other needful buildings." U.S. CONST. art. I, § 8, cl. 17.

take more abstract state goods — like state legislative and executive authority — but the logic of those cases applies even more strongly to coercive and uncompensated takings of state assets.

Indeed, we could hypothesize that courts have avoided applying the anti-commandeering rule to data not because it represents a more conceptually intricate case of commandeering but because it represents a more conceptually simple one — and sometimes simplifying doctrines to their basics is even more difficult than complexifying them. Data takings are best analogized to a kind of Commandeering 1.0: the snatching up and carting away of a state asset. *New York* and *Printz* take commandeering into institutional context and develop a kind of Commandeering 2.0: the direction of state infrastructure to federal ends. If that's true, we should not need to demonstrate, as Mikos takes great pains to do but everyday litigants may find too resource intensive, that data takings cannot be effectuated without commandeering legislative or executive processes, à la *New York* and *Printz*. A more straightforward showing that the federal government has taken a valuable state asset should be sufficient. In the private sector, we increasingly appreciate that data can act as an asset, a currency, and a discrete source of corporate power.[259] Parts I and II of this Article show that the governmental sector should be no different.

Finally, the use of voluntary data sharing agreements documented in this Article reveals that our governments have in most cases over time understood data to be a governmental good that requires voluntary surrender. As many scholars have argued, and courts have agreed, historical practice is relevant to answering questions about how the Constitution distributes power among coordinate branches of the federal government and between the federal government and the states.[260] Because "[l]ong settled and established practice is a consideration of great weight in a proper interpretation of constitutional provisions," we can consult the settled practice between the states and federal government with respect to data sharing.[261] This Article provides the historical understanding necessary to conclude that data sharing has been generally viewed by the federal government and the states as a *voluntary* practice — one requiring the kind of consent that is characteristic of other forms of cooperative endeavor to which the anti-commandeering

---

[259] Tim Gillis et al., *Indirect Tax Compliance in an Era of Big Data*, 13 TAX PLAN. INT'L INDIRECT TAXES, no. 6, 2015, at 2, https://assets.kpmg/content/dam/kpmg/pdf/2015/08/indirect-tax-in-an-era-of-big-data.pdf [https://perma.cc/3MAF-7A5S] (noting that "data has become a core asset of the 21st century business enterprise").

[260] *See, e.g.*, NLRB v. Noel Canning, 573 U.S. 513, 543–45 (2014); Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 610–11 (1952) (Frankfurter, J., concurring). *See generally* Curtis A. Bradley & Trevor W. Morrison, *Historical Gloss and the Separation of Powers*, 126 HARV. L. REV. 411 (2012); Curtis A. Bradley, *Doing Gloss*, 84 U. CHI. L. REV. 59 (2017).

[261] The Pocket Veto Case, 279 U.S. 655, 689 (1929).

rule clearly applies.[262] Of course, when the Supreme Court has given significant weight to practice over time, it has tended to be persuaded by practices that are centuries — rather than decades — long. But the shorter lifespan of these practices should not weigh against them, for they extend the entire history of data sharing in the computer age.[263]

Of course, seeing the distinct dynamics of data federalism and the properties that distinguish data from the other forms of power our governments trade does not cut in just one direction. Data's non-rivalrous character, in particular, could provide fodder for a more potent possible *defense* of an information sharing exception to the anti-commandeering rule than Justices and commentators have previously offered. Because a state's access to its own data is not diminished by the federal government's access to the same data, it could be said that data commandeering has no harm. The problem with that argument, as the "sanctuary cities" cases illustrate so well, is that it conflates the non-rivalrous character of the data itself with the rivalrous character of the data's governance regimes. A state that collects data about immigrant populations by promising confidentiality, as New York did when it offered driver's licenses to undocumented populations,[264] will find its promises impossible to keep if the federal government requisitions the city's data for enforcement purposes. Indeed, data's non-rivalrous character makes the need to safeguard a government's control over its data governance regimes even more pressing. That is because each new actor or institution that can access data multiplies the risk that a data's governance regime will be compromised.

Together, then, these arguments suggest that the anti-commandeering rule should, on its own terms, apply to federal efforts to requisition state data.

2. The Anti-coercion & Pennhurst *Clear Statement Rules.* — If the anti-commandeering rule applies to data transactions, and the federal government may not take state data by force, it seems intuitive that it cannot circumvent the rule by engaging in coercive or deceptive conduct with respect to an ostensibly voluntary transaction in data. But questions about the applicability of the anti-coercion and *Pennhurst* rules — which would ensure that data exchanges that appear voluntary are, in

---

[262] The few and notable exceptions have been overtly resisted by states and cities, suggesting that they have not acquiesced in the federal government's deviation from the norm.

[263] Indeed, a commitment to voluntary participation was present both in early data exchanges that predated the age of computing, *see, e.g.*, Richman, *supra* note 31, at 388 (describing incentives for local police to voluntarily pass information to the FBI in the mid-twentieth century); *see also History and Modernization of Case Surveillance*, *supra* note 53 (describing the origin of the CDC's disease surveillance system in the voluntary reporting of state and local health departments in the late nineteenth and early twentieth centuries), and in those at the dawn of the computing age, *see supra* notes 161–163 and accompanying text (describing the NCIC's origination in voluntary agreements).

[264] Tracey Tully & Michael Gold, *Long Lines as Undocumented Immigrants in N.Y. Rush to Get Licenses*, N.Y. TIMES (Dec. 16, 2019), https://www.nytimes.com/2019/12/16/nyregion/undocumented-immigrant-drivers-license-ny-nj.html [https://perma.cc/77YF-BHX8].

fact, voluntary — have received essentially no scholarly treatment. And those questions may be the more consequential ones. As Part I shows, most federal-state data programs at least present themselves as voluntary transactions, not mandatory ones. So issues attending the legitimacy of that voluntary character have many more occasions to arise. Indeed, as I discuss in the next section, there are high-profile and ostensibly voluntary data transactions of large scale and consequence that would fail to satisfy the anti-coercion and *Pennhurst* rules if they did apply here.

The dearth of attention to these questions is perhaps attributable to the assumption that the anti-coercion and *Pennhurst* rules apply only where the Spending Clause is at issue and federal funds are on offer. This premise looms so large because, as I discuss in Part IV, many assume as a matter of course that all cooperative programs involve the exchange of federal funds. Because we have not seen data collaborations as part of the general sweep of cooperative federalism, it is no surprise that few have thought to ask whether these rules apply to them — much less argue either that they should or should not.

The simple fact that data transactions resemble transactions in funding is strong evidence that the same rules should apply. But before making that argument in depth, and given the absence of any real attention to this issue in the literature, I sketch the most charitable argument that these rules should *not* apply here — an argument not wholly without merit, even if it is not, in my view, persuasive.

To see the argument that these doctrines should be limited to federal spending and grantmaking, consider first the genealogy of the anti-commandeering rule, on the one hand, and the anti-coercion and clear statement rules, on the other. The anti-commandeering rule arises not from a specific enumerated power, but from the Tenth Amendment and structural federalism principles that apply to the Constitution as a whole.[265] The rule operates, as a result, as an external constraint on all federal powers that do not clearly exempt it.[266] Whether Congress is

---

[265] Printz v. United States, 521 U.S. 898, 932 (1997) (noting that permitting commandeering would "compromise the [Constitution's] structural framework of dual sovereignty"); New York v. United States, 505 U.S. 144, 187 (1992) ("Much of the Constitution is concerned with setting forth the form of our government . . . : It divides power among sovereigns and among branches of government precisely so that we may resist the temptation to concentrate power in one location . . . .").

[266] The Fourteenth and Fifteenth Amendments, for instance, specifically contemplate that Congress will issue directives that could commandeer state governments in the service of prohibiting unconstitutional discrimination. *See, e.g.*, U.S. CONST. amend. XIV, §§ 1, 5 (allowing Congress to "enforce, by appropriate legislation," § 5, the Amendment's instruction that "No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; . . . deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws," § 1); *id.* amend. XV, § 2 (allowing Congress to "enforce this article by appropriate legislation"); *see also* EEOC v. Wyoming, 460 U.S. 226, 243 n.18 (1983) ("[W]hen properly exercising its power under § 5 [of the Fourteenth

using its Commerce Clause power or its foreign affairs power, its naturalization power or its bankruptcy power, it is presumptively constrained by the anti-commandeering rule.

But the anti-coercion and *Pennhurst* clear statement rules have a different origin. They arose specifically in the context of Congress's Spending Clause authority to levy taxes and spend the proceeds for the "general Welfare."[267] And it is possible to see them as limitations the Spending Clause places on Congress's power to spend, not as limitations the Constitution places on the federal government's relationship to state governments more broadly.

But the anti-coercion and clear statement rules also perform an important state-protective function: By ensuring that states voluntarily agree to joint programs, they safeguard the basic state autonomy to direct their own policymaking, an interest states have whether Congress is proposing a joint initiative pursuant to its spending power or any other constitutional source of authority. The question is thus whether the anti-coercion and *Pennhurst* rules are triggered only when Congress spends, or are present any time the states and federal government negotiate a cooperative program.

The argument that these rules are rooted primarily in — and should be limited to — contexts in which we are concerned that a federal offer may exceed an enumerated grant of authority traces to *South Dakota v. Dole*,[268] the foundational case setting out the anti-coercion rule. As *Dole* explains, the Spending Clause is an expansive grant of federal power: Because its language authorizing Congress to spend for the general welfare is so broad, Congress's power to spend monies "for public purposes" allows it to attain "objectives not thought to be within Article I's 'enumerated legislative fields'" by simply imposing substantive conditions on the receipt of federal funds.[269] Although Congress could not, for example, require local education departments to adopt a federal curriculum, it could condition federal funds on their adoption of that curriculum. That result is acceptable because a state's autonomous choice to accept federal funds and use them within federal parameters is viewed as just that — the state's exercise of its own powers.

However, when the state is coerced, *Dole* suggests, the state is *not* meaningfully using its own powers; instead, the state, acting without

---

Amendment], Congress is not limited by the same Tenth Amendment constraints . . . ."); *cf.* Fitzpatrick v. Bitzer, 427 U.S. 445, 456 (1976) (holding similarly in the adjacent area of state sovereign immunity because the sections of the Fourteenth Amendment "by their own terms embody limitations on state authority").

267 U.S. CONST. art. 1, § 8, cl. 1; *see* Pennhurst State Sch. & Hosp. v. Halderman, 451 U.S. 1, 17 (1981).

268 483 U.S. 203 (1987).

269 *Id.* at 207 (quoting United States v. Butler, 297 U.S. 1, 65–66 (1936)).

self-determination, is a compulsory agent of Congress. In *Dole*'s terms, the states cannot be said to be autonomously choosing to advance Congress's objectives if the "financial inducement" is "so coercive as to pass the point at which 'pressure turns into compulsion.'"[270] Nor, as *Pennhurst* elaborates, can the states be said to be acting voluntarily if Congress hides their obligations in grant conditions that are not stated "unambiguously," so that they can "exercise their choice . . . cognizant of the consequences of their participation."[271] Because "legislation enacted pursuant to the spending power is much in the nature of a contract" — that is, "in return for federal funds, the States agree to comply with federally imposed conditions" — the "legitimacy of Congress' power to legislate under the spending power thus rests on whether the State voluntarily and knowingly accepts the terms of the 'contract.'"[272] These rules, on this account, perform a federal-limiting function: They prevent Congress from using its Spending Clause power to circumvent its other enumerated powers.

The second function these rules perform, however — the state-protective function — is not rooted in logic specific to the Spending Clause. It is instead rooted in basic principles of constitutional structure and the long-standing practice of voluntary federal-state projects. Even if Congress is acting well within its enumerated powers — say, delegating authority to enforce federal immigration law to the states — the anti-coercion and *Pennhurst* rules should still safeguard the ability of states to accept such delegations voluntarily. In the first case to actually find a violation of the anti-coercion rule, the Supreme Court's high-profile decision in *NFIB v. Sebelius*,[273] the Court emphasized this state-protective function far more than it did *Dole*'s federal-limiting rationale.[274] And it eliminated any doubt that the anti-coercion and *Pennhurst* rules are applicable even where there would otherwise be no question of Congress's authority to regulate, including outside the Spending Clause context.

NFIB's analysis makes the broad applicability of these rules clear in two ways. First, the Chief Justice's opinion for the first time drew a clear thread between the anti-coercion and *Pennhurst* rules, on the one hand, and the anti-commandeering rule, on the other. The Chief Justice's opinion grounded all three rules in the "insight"[275] from *New York* that if Congress could "require the States to govern according to

---

[270] *Id.* at 211 (quoting Steward Mach. Co. v. Davis, 301 U.S. 548, 590 (1937)).
[271] *Pennhurst*, 451 U.S. at 17.
[272] *Id.* (citing *Steward Mach. Co.*, 301 U.S. at 585–98; Harris v. McRae, 448 U.S. 297 (1980)).
[273] 567 U.S. 519 (2012).
[274] *See id.* at 577–78 (opinion of Roberts, C.J.).
[275] *Id.* at 577.

Congress' instructions,"[276] the Constitution's basic "two-government system" would collapse into "one central government."[277] Thus, the state-protective function dictates that the Constitution is violated whether "Congress directly commands a State to regulate or indirectly coerces a State."[278] Congress may not "commandeer[] a State's legislative or administrative apparatus," it cannot "exert a power akin to undue influence," and it may not impose ambiguous conditions.[279]

The Chief Justice's analysis is perhaps not earth-shattering, but it has outsized importance for our purposes. It clarifies that the federal government is constrained from commanding, coercing, or manipulating the states no matter what form of federal power undergirds the joint effort on offer. These rules, in short, are functional. Where Congress innovates the methods by which it threatens state autonomy — by suggesting it will withhold data (rather than money) if the states do not do as it instructs, or by hiding terms in contracts for data instead of contracts for funding — these rules stand at the ready.

A second and more interesting conceptual move further emphasizes the point. The Chief Justice's opinion also foregrounds the analogy between federal-state joint efforts and private contracts, an analogy that the Court has often flirted with.[280] This foregrounding is important, but as my earlier work on federalism and contract law argues, it does not go far enough. Spending Clause programs are not just analogous to contracts; they often give rise to *actual* contracts.[281] And, important for our purposes, these contract-like instruments are not limited to the Spending Clause context. The federal government and the states enter into a wide range of intergovernmental agreements on a voluntary basis — mutually assenting to their terms, as any private contracting parties do. Some of those exchanges involve money, but many do not.

This legal reality makes clear why these rules must apply to data. Just as contract law polices the relationship between the parties — almost entirely without respect to what things of value are being exchanged — so too does the law of agreement-making between governments focus on the relationship between the parties, not the powers being exchanged. Whatever the currency offered, the status of each government as voluntary counterparty to the transaction is what matters.

---

[276] *Id.* (quoting New York v. United States, 505 U.S. 144, 162 (1992)).

[277] *Id.*

[278] *Id.* at 578.

[279] *Id.* at 577–78 (quoting Steward Mach. Co. v. Davis, 301 U.S. 548, 590 (1937)); *id.* at 583.

[280] *Id.* at 576–77 ("We have repeatedly characterized . . . Spending Clause legislation as much in the nature of a *contract.* The legitimacy of Congress's exercise of the spending power thus rests on whether the State voluntarily and knowingly accepts the terms of the 'contract.'" (citations and internal quotation marks omitted) (quoting Barnes v. Gorman, 536 U.S. 181, 186 (2002); Pennhurst State Sch. & Hosp. v. Halderman, 451 U.S. 1, 17 (1981))).

[281] Fahey, *supra* note 18, at 2354–68 (describing the many contract-like doctrines courts apply to these agreements and the view they embody — of two parties engaging in voluntary exchange for a wide range of goods); *see also Pennhurst*, 451 U.S. at 17.

C. Data and the Limits of Existing Constitutional Doctrine

Given the pace of intergovernmental data exchange and the unusual federal-state institutions that have arisen to manage it, it is worth reflecting on the kinds of structural issues that federalism's rules of engagement do not address in our architectures of data federalism.

First, and most basically, because those doctrines regulate only the bare-bones voluntariness of the government-to-government relationship, they do not address what happens when our governments eagerly participate in joint ventures — when, as Justice Jackson says, they act to reintegrate their dispersed powers. Provided that they are voluntary, current federalism doctrine has little to say about how our governments structure their joint initiatives. But if the Constitution "diffuses power the better to secure liberty," and it also contemplates that "practice will integrate the dispersed powers into a workable government," it would be odd for there to be no constitutional significance to how that power is reintegrated beyond the constraints of the anti-commandeering, anti-coercion, and *Pennhurst* rules.[282]

Put differently, although the Court frequently says that federalism "protects the liberty of the individual from arbitrary power" by "denying any one government complete jurisdiction over all the concerns of public life," it has no doctrines that subject aggregations of power that governments freely choose to heightened scrutiny.[283] And data management is an area in which the risks to individual liberty from power aggregation are always present in concrete ways. The more data each government can access — and the more of data's complementary properties each government can exploit — the greater the risk the government violates the privacy of a data subject, improperly surveils her, discloses her data without permission or allows it to be accessed by unauthorized users, uses her data in a discriminatory way, or denies her a right or benefit because of a correctable flaw in her data.

Second, because federalism's rules of engagement focus on the government-to-government relationship, they do not address the relationship between our governments acting jointly and the polities they cooperatively govern. The Court has repeatedly explained that the "Constitution does not protect the sovereignty of States for the benefit of the States or state governments as abstract political entities, or even for the benefit of the public officials governing the States," but "for the protection of individuals."[284] And the federalism cases discussed above are concerned about how intergovernmental interactions can enable opportunism by governmental officials by allowing them to circumvent accountability and public oversight. In the anti-commandeering cases,

---

[282] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635 (1952) (Jackson, J., concurring).

[283] Bond v. United States, 564 U.S. 211, 222 (2011).

[284] New York v. United States, 505 U.S. 144, 181 (1992); *accord Bond*, 564 U.S. at 222; *see also* Murphy v. NCAA, 138 S. Ct. 1461, 1477 (2018).

for instance, the Court has been concerned that federal directives to state governments will obscure accountability. But those concerns end where non-coercive collaborations begin, even though our governmental officials can of course use intergovernmental collaboration to shield their activities from accountability as well. It is striking how little public engagement, or stakeholder input, the cross-governmental NCIC bureaucracy allows — more striking because legislative bodies like Congress play such a minimal oversight role. It is instead the governmental officials who benefit most from expanding data stores who are principal decisionmakers making those expansions happen.[285] This kind of too-cooperative federalism could easily provide avenues for governmental officials to aggrandize their own power vis-à-vis their constituents.

Finally, although federalism's rules of engagement regulate aspects of the contractual lawmaking process used to structure data sharing initiatives, they do not address some of the most pressing questions this form of joint governmental lawmaking raises.[286] It has no cross-cutting procedural requirements, and the processes used to craft these documents are often shielded from public view. They are not codified, as are ordinary laws and regulations. The role that each government plays in their creation is often obscured by the contractual formalism of the final product. If, as the Court emphasizes, our constitutional federalism structure is intended to provide "two distinct and discernable lines of political accountability: one between the citizens and the Federal Government; the second between the citizens and the States," and if intergovernmental interactions must allow constituents "some means of knowing which of the two governments to hold accountable for the failure to perform a given function," then the lack of tools for assessing just those concerns in processes of contractual lawmaking is notable.[287]

These questions are certainly not ready for judicial prime time. One theme of data federalism is that its practices are still evolving and many are not yet publicly known. It will take time for discrete issues to come to the attention of courts and for the structural constitutional questions they raise to be thoroughly aired. But the possibility that some of the institutions documented in Part II may raise issues of constitutional significance should not be as remote as their novelty might suggest.

---

[285] That policing decisions are made primarily by police themselves and obscured from the stakeholders those decisions affect is no surprise. As Professor Barry Friedman has documented, federal, state, and local policing — from line-level activities to broader policing policy — are characterized by a "pervasive secrecy." Barry Friedman, *Secret Policing*, 2016 U. CHI. LEGAL F. 99, 100.

[286] For an extensive discussion of these issues, see Fahey, *supra* note 18, at 2398–406.

[287] United States v. Lopez, 514 U.S. 549, 576–77 (1995) (Kennedy, J., concurring).

IV. THEORIZING DATA FEDERALISM

A. Data as Power

At its most basic, federalism divides power between levels of government. It invites "power" to act as "the rival of power"[288] in order to secure "a healthy balance."[289] Theories of federalism understand what constitutes a "healthy balance" differently — some are skeptical that we are able to measure balance at all — but it remains true that distributing power is not just the objective, but also a defining characteristic of federalism.[290] Historically, because the Supreme Court has treated the allocation of power between levels of government as fixed, analyzing the formal powers the Constitution once granted each level of government instead of asking what functional powers each has come to possess today, we have missed opportunities to evaluate how our system actually balances power.[291] And even the scholars who acknowledge correctly that governmental power in a federalist system is dynamic, fluid, and negotiated across time tend to focus on intergovernmental exchanges of just a few forms of conventional governmental power — the *regulatory* power granted to each level of government by the Constitution, the *monetary* power exchanged in vast sums by our levels of government through federal grant programs, and the *administrative* power that stems from the capacity of states and cities to implement federal programs and which they offer in trade for federal grants.[292]

---

[288] THE FEDERALIST NO. 28, at 176 (Alexander Hamilton) (Clinton Rossiter ed., 2003).

[289] Gregory v. Ashcroft, 501 U.S. 452, 458 (1991).

[290] Some emphasize the checking function of federalism's distribution of power. *See, e.g.*, Printz v. United States, 521 U.S. 898, 922 (1997) ("The different governments will control each other, at the same time that each will be controlled by itself." (quoting THE FEDERALIST NO. 51, *supra* note 288, at 320 (James Madison))). Others focus on the related anti-tyranny function. *See, e.g.*, *Ashcroft*, 501 U.S. at 458–59 (noting Alexander Hamilton's view that "the new federalist system would suppress completely 'the attempts of the government to establish a tyranny'" (quoting THE FEDERALIST NO. 28, *supra* note 288, at 176 (Alexander Hamilton))). Others focus on how federalism's dispersion of power secures liberty. *See, e.g.*, THE FEDERALIST NO. 51, *supra* note 288, at 318 (James Madison) (explaining that the "separate and distinct exercise of the different powers of government" is "essential to the preservation of liberty"); THE FEDERALIST NO. 28, *supra* note 288, at 177 (Alexander Hamilton) ("It may safely be received as an axiom in our political system that the State governments will, in all possible contingencies, afford complete security against invasions of the public liberty by the national authority.").

[291] *See Lopez*, 514 U.S. at 552 (describing the "constitutionally mandated division of authority . . . 'adopted by the Framers'" (quoting *Ashcroft*, 501 U.S. at 458)); United States v. Morrison, 529 U.S. 598, 620 (2000) (similar); Bond v. United States, 572 U.S. 844, 856 (2014) (describing the "Constitution's division of responsibility between sovereigns").

[292] Together, these forms of power exchange are the building blocks of the standard cooperative federalism program: Congress wants to regulate an area constitutionally reserved for the states (for example, education) so it envisions a cooperative program in which federal spending authority and state education authority are joined together and, within that program, the states receive federal funds in exchange for implementing an education program that accomplishes federal objectives. There is a growing scholarly literature placing this sort of familiar program in constitutional frame by describing the ways it represents a bargain over money and regulatory authority. *See generally, e.g.*, RYAN, *supra* note 26; Fahey, *supra* note 18; Huq, *supra* note 26.

We have largely neglected to theorize the reality that as the technologies of governance evolve, so too do the forms of power our governments give and get from one another. As data has become a significant source of power for governments, it has also become a source of intergovernmental currency, inducement, leverage, and coercion. Intergovernmental data markets thus show that the division of governmental power in our federalist system is doubly dynamic: Not only is the *distribution* of governmental power always changing, but so too are the *forms* of power governments use and exchange. This insight challenges and complicates federalism theory in multiple respects, suggesting that it is time to renew conversations about power and federalism.

That federalism conversations have not confronted the flow of terabytes of data between governments suggests that we have missed a significant determinant of whether power is, in fact, balanced between those governments. But we should also take this as a call to do some searching for additional forms of power that our governments use and trade: to develop a more subtle and imaginative understanding of the full portfolio of powers we should be talking about. Of course, it is difficult to imagine any single account of federalism tallying, tracing, and netting out every form of power our governments possess, use, and trade. But it is easy to imagine looking beyond the conventional powers when analyzing intergovernmental interactions in discrete contexts and policy areas.

Understanding that governments trade in powers beyond the traditional set expands our understanding of the techniques that governments can use to influence each other. As I have argued, data can serve significant functions in intergovernmental interactions that current doctrine sees only in money: It can be appropriately leveraged to encourage states to participate in federal programs, but it can also be used as a cudgel to the same end, thus "pass[ing] the point at which 'pressure turns into compulsion.'"[293]

But seeing data's significance to federalism raises a deeper and more important point about federalism's relationship to different forms of power. Each form of power has discrete properties that differently affect how our governments relate to one another and whether their interactions promote a power-balanced system. Data is a particularly provocative, and especially challenging, case study in these differences because it strikes a stark contrast to the conventional forms of power that are an assumed premise of many federalism accounts.

First, data's non-rivalrous character makes it a particularly easy asset to transfer between governments. A government can share data without diminishing its own access to that data. As a consequence, unlike other forms of power that our governments bargain over and

---

[293] NFIB v. Sebelius, 567 U.S. 519, 580 (2012) (opinion of Roberts, C.J.) (quoting South Dakota v. Dole, 483 U.S. 203, 211 (1987)); *see supra* pp. 1056–58.

trade — money, most obviously — intergovernmental data exchange does not shift control over a particular node of power from one government to another. It *duplicates* that power *in* the other. Data federalism, then, is not a traditional federalism story of divided power; indeed, federalism in the data world can act as a power *multiplier* rather than a power *divider*. Instead of diffusing power to protect individual liberty, it aggregates power and diffuses access. Even the tiniest police department in the tiniest town in America can access the concentrated data power of every police department across the nation. And federalism is the reason. But because the power-distributing function is so core to what federalism does, federalism lacks the analytical tools to explain — much less justify or constrain — that destabilizing result.

Data's character as a complementary good — each piece of data becomes more valuable when aggregated with other harmonizing data — also shapes how data power is distributed among our levels of government. While data's non-rival character *reduces the costs* of sharing, data's complementary character *increases the value* of sharing. Those forces together mean that absent external constraints, governments have strong incentives to coordinate with their sister governments to concentrate power and expand access to the joint store, rather than jealously guard their respective powers and pit them against one another to secure balance, as conventional federalism theory suggests.[294] Questions about the aggregation of data power are familiar to privacy scholars, but scholars of federalism, too, should take note: If federalism is to encourage the division of power, we have to understand the incentives unique to each form that power takes and tailor our structural interventions to them.

Finally, unlike money, data is nonfungible. Governments do not want data for its own sake; they want data that tells them something about *particular* people and *particular* problems. Data, put another way, is most valuable when it is deanonymized and connected to the person who originated it; indeed, this Article has focused on data that contains just that kind of personal identifying information. This fact has many potential implications, but one is particularly significant to the ground-laying work of this Article: As data moves across governmental boundaries, it remains connected to the individual who originated it and the government that collected it. Even governments with only minimal commitments to privacy, then, retain an interest in safeguarding their data as it is put to use by their sister governments, for the originating governments are likely the most salient custodians from the perspective of their constituents. This helps explain why our governments oversee their data pools through intricate multi-governmental administrative structures — why each government continues to want to participate in the governance of the data it shares. And it affirms our

---

[294] *See* THE FEDERALIST NO. 28, *supra* note 288, at 176–77 (Alexander Hamilton); *Ashcroft*, 501 U.S. at 458.

need to trace the unusual federalism interactions that we observe today to the specific form of powers they arose to manage.

B. Federalism Outside Congress

Over the last decade, academic accounts of federalism have increasingly rejected the outdated assumption that the federal government and the states operate in separate spheres, instead embracing the premise that the federal government and the states govern together in a much wider range of contexts than was once understood.[295] Although even a decade ago many "scholars often wr[o]te as if cooperative federalism d[id] not exist," today what many call cooperative federalism (but is perhaps better termed *joint governance*) is not only federalism's dominant form, but also the literature's central focus.[296] Because the federal government is generally believed to be the dominant player in these joint initiatives, federalism scholars often begin with the federal government to understand how our levels of government together make and implement policy.[297] Federalism, Professor Heather Gerken has memorably declared, is "the new nationalism."[298]

In this world, much can be learned about the power the states and federal government each exercise, the ends to which they are applying their joint energies, and the institutions that facilitate their partnerships by looking first at the work product of Congress. Indeed, there is a growing scholarly consensus that Congress plays *the* central role in structuring interactions between the federal government and the states today.[299] It is Congress that enacts sweeping policy and regulatory initiatives and Congress that invites states to help implement them. Congress decides what funds to offer states and what administrative commitments to ask for in return. Congress sets out the sites

---

[295] *See, e.g.*, *supra* note 204.

[296] Heather K. Gerken, *Our Federalism(s)*, 53 WM. & MARY L. REV. 1549, 1562 (2012); *see* Bulman-Pozen & Gerken, *supra* note 204, at 1262 & n.14. As Professors Heather Gerken and Jessica Bulman-Pozen have shown, in the context of jointly administered programs, the states often resist federal policy from within, in a model of "*uncooperative federalism*," which nonetheless arises in a project of joint governance. Bulman-Pozen & Gerken, *supra* note 204, at 1258; *see also* William Baude, *Rethinking the Federal Eminent Domain Power*, 122 YALE L.J. 1738, 1823 (2013) (preferring the term "interactive federalism" to "cooperative federalism").

[297] *See, e.g.*, Gluck, *supra* note 16.

[298] Heather K. Gerken, Feature, *Federalism as the New Nationalism: An Overview*, 123 YALE L.J. 1889, 1889 (2014).

[299] *See, e.g.*, Gluck, *supra* note 16, at 542 (describing a "legislation-focused theory of federalism" that is "concerned less with formal state sovereignty or the assumed policy benefits of federalism and concerned more with congressional intent and questions about how national power is created and elaborated"); Jessica Bulman-Pozen, *Federalism as a Safeguard of the Separation of Powers*, 112 COLUM. L. REV. 459, 461 (2012) (arguing that federalism buttresses Congress's power within the federal government because the states "rely[] on congressionally conferred authority and cast[] themselves as Congress's faithful agents").

of interaction and processes through which disputes will be resolved.[300] These superstatutes — think of the Affordable Care Act, but before that the Clean Air Act,[301] the Telecommunications Act of 1996,[302] and the Social Security Act of 1935[303] — do not just create opportunities for cooperative federalism; they also structure the forms of interaction between the states and federal government and their respective powers across their projects of joint governance. This is a federalism, Gluck has emphasized, that "comes by grace of Congress."[304]

Centering contemporary federalism in Congress also has significant normative implications. The influential process school of federalism, first articulated by Professor Herbert Wechsler in the mid-century and since advocated by a wide range of scholars, sees the states' ability to represent their interests in Congress as a central legitimating force behind cooperative federalism programs.[305] Noticing that important cross-governmental initiatives arise outside Congress forces us to find new ways to understand their legitimacy.

This Article contests Congress's dominance in American federalism. It reveals not only consequential one-off data transactions but also major data pooling programs that are far less disciplined by statute than the usual cooperative federalism programs. Many of the statutes cited as authority for the data sharing programs that I describe here either do not contemplate those programs' existence or authorize them in such sweeping terms that they permit almost any form of transaction, in almost any volume, on almost any terms. Even federal privacy statutes either directly or by operation exempt intergovernmental data exchange from important restraints.

The intergovernmental data market, in other words, has not "come by grace of Congress" at all. This poses challenges and opportunities for federalism scholarship. It presses us to evaluate how intergovernmental interactions that are not guided by the federal legislature come

---

[300] *See* Gluck, *supra* note 16, at 538–42; *see also* Bulman-Pozen & Gerken, *supra* note 204, at 1267; Gerken, *supra* note 298, at 1904.

[301] *See, e.g.*, John P. Dwyer, *The Practice of Federalism Under the Clean Air Act*, 54 MD. L. REV. 1183, 1184–86 (1995).

[302] *See, e.g.*, Philip J. Weiser, *Federal Common Law, Cooperative Federalism, and the Enforcement of the Telecom Act*, 76 N.Y.U. L. REV. 1692, 1694 (2001).

[303] KAREN M. TANI, STATES OF DEPENDENCY: WELFARE, RIGHTS, AND AMERICAN GOVERNANCE, 1935–1972, at 12–14 (2016).

[304] Gluck, *supra* note 16, at 542.

[305] *See* Herbert Wechsler, *The Political Safeguards of Federalism: The Role of the States in the Composition and Selection of the National Government*, 54 COLUM. L. REV. 543 (1954); Garcia v. San Antonio Metro. Transit Auth., 469 U.S. 528, 550–51, 551 n.11 (1985) (citing and adopting Wechsler's view); *see also* Jesse H. Choper, *The Scope of National Power Vis-à-Vis the States: The Dispensability of Judicial Review*, 86 YALE L.J. 1552 (1977); Ernest A. Young, *Two Cheers for Process Federalism*, 46 VILL. L. REV. 1349 (2001).

to be, function on an ongoing basis, and are made (or not) into legitimate forms of public governance.

1. Program Creation Outside Congress. — Consistent with the contemporary focus on Congress, scholars have developed a basic theory about how most joint governance programs come to be. Congress passes a statute, and then *delegates* — in ways that resemble administrative delegations — powers to state and local governments to implement programs within certain parameters.[306] Sometimes federal agencies, too, delegate administrative powers to states through the rulemaking powers accorded them by Congress.[307]

The initiatives I describe here — the NCIC, the fusion centers, the range of ad hoc immigration-related information sharing initiatives, the CDC's disease surveillance system, and more — are not programs dreamed up by Congress and then offered to states like contracts of adhesion or take-it-or-leave-it proposals to delegate authority on specified terms. They have come to life (for good or for ill) through flattened models of *collaboration* between governments outside Congress rather than a hierarchical model of *delegation* from Congress. The states' possession of policing data predated the NCIC. The surveillance of disease by local health departments likewise started from below. And the terms of those programs continue to be negotiated by the cities and states who hold the data that powers them.

That, in turn, yields another important feature of this federalism outside Congress: It confounds our expectation about the power differential between the bargaining governments. Cooperative federalism scholarship tends to assume that the federal government is the dominant party in negotiations and the entity that really sets the terms. In the most significant data programs, however, the states hold substantial power. Studying these expectation-undermining programs and institutions yields new lines of inquiry. We can ask, for instance, whether the states can ever coerce the federal government, or whether the federal government can be the recipient of powers delegated from the states, rather than the other way around. And we can observe differences in programmatic structure when the states take the lead, as I discuss next.

2. Program Governance Outside Congress. — The fact that Congress has taken a back seat in these areas does not mean that they are without legal structure. The agreements that structure these arrangements are jointly authored by federal and state governments, and they function as joint lawmaking instruments. Although they are used even in areas where Congress plays a significant role — where they are used to fill

---

[306] *See generally* Abbe R. Gluck, Feature, *Our [National] Federalism*, 123 YALE L.J. 1996, 2025–26 (2014) (describing these "delegations" and asking whether administrative doctrines like *Chevron* deference should apply to them); Jessica Bulman-Pozen, *Administrative States: Beyond Presidential Administration*, 98 TEX. L. REV. 265 (2019) (describing states' roles in administering federal programs alongside federal agencies).

[307] *See* sources cited *supra* note 306.

statutory gaps and to memorialize states' voluntary consent to join programs — they play an outsized role in spaces characterized by the absence of clear statutory mandates. They do for data programs, in other words, what Congress did for health care in the Affordable Care Act — provide a structure, a source of authority, and a mechanism to bind the parties. But they gain their authority from the consent of each party, and, like any private-sector contract, must be understood as a product of both parties equally.

But these agreements are only the first layer of interstitial governance. As I explain in Part II, intergovernmental agreements can establish institutions like fusion centers, which are chartered by state and federal officials and use customized models of decisionmaking and information sharing. And they can enable elaborate governance processes, like the NCIC's advisory regime and its linked organizations, the National Crime Prevention and Privacy Compact Council and the Nlets organization. These negotiated institutions do not follow existing blueprints or models within the federal government or the states, but represent real institutional innovation — innovation that requires significantly more attention than this Article can provide.

The existence of institutions like the NCIC and fusion centers, moreover, should influence the growing body of federalism scholarship that addresses broadscale structural questions — that asks how our federalism has evolved and how it functions today by looking across policy areas to identify patterns and practices.[308] With some exceptions, the standard sources for answering those questions are big "cooperative federalism" statutes and the state agencies that implement them. Data pooling programs like the NCIC have, to my knowledge, never been part of those broad federalism conversations, but given that the NCIC serves as the infrastructure between every federal, state, and local law enforcement agency in the United States, it deserves its place alongside more traditional cooperative federalism programs. Including data pooling programs in conversations about joint governance will enrich the conclusions that scholarship can draw.

C. Federalism's Interstitial Space

The existence of this unorthodox form of joint governance holds promise for American law, but it also raises serious questions of legitimacy and legality. At a very basic level, these institutions and processes plainly look nothing like standard policy creation — and that gap draws

---

[308] For examples of this growing and important literature, see generally, for example, Jessica Bulman-Pozen, Feature, *From Sovereignty and Process to Administration and Politics: The Afterlife of American Federalism*, 123 YALE L.J. 1920 (2014); Gerken, *supra* note 298; Cristina Rodríguez, *Negotiating Conflict Through Federalism: Institutional and Popular Perspectives*, 123 YALE L.J. 2094 (2014); Gluck, *supra* note 16; Erin Ryan, *Negotiating Federalism*, 52 B.C. L. REV. 1, 28–36 (2011); Huq, *supra* note 26; and Judith Resnik, *Law's Migration: American Exceptionalism, Silent Dialogues, and Federalism's Multiple Ports of Entry*, 115 YALE L.J. 1564 (2006).

into question the legitimacy of the rules that do govern data exchange and pooling. Federal or state statutes can impose meaningful restraints on cooperative federalism efforts. Without those constraints, though, the normative judgments that must be made around data aggregation — related to privacy, security, accuracy, and use — are rarely being made by an accountable political body, if they are being made at all. These decisions are instead made in the shadows and are not generally reported publicly. Information about them must be obtained through FOIA and state sunshine laws, and even then (I can report) the officials addressing the request often seem unable to locate the relevant information on first try. That may be because there is little standardization and only murky lines of authority dictating which officials at which levels of government can release what information publicly.[309]

In these areas, we also see an unusual degree of influence by mid- and line-level officials — immigration agents, for instance, have built cross-governmental alliances to exchange data assets that might not be possible if Congress or state legislatures had to authorize data transfer in the first instance.[310] Indeed, whereas governments jealously safeguard the ability of their agents to spend money without legislative oversight, the same is not true for data.[311] Scholars have documented so-called "picket-fence federalism," in which federal bureaucrats work directly with their state counterparts to advance joint ends.[312] But the influence of street-level bureaucrats on intergovernmental data exchange runs far deeper than even these accounts suggest. When not just the head of a state DMV but the frontline employees who receive discrete data requests from similarly low- and mid-level ICE agents are empowered to approve those requests, we can observe several effects.

One is that data exchanges can be negotiated by the very governmental agents that stand to benefit from expanded access to private data — by the entities that are using that data, in many instances to surveil and track the people who originally gave it to the state, without input from the constituents who stand to be harmed. By pressing data sharing decisions deeper into administrative agencies, we draw them further from the policymaking institutions that have a responsibility to balance the need for data against other important values. We should worry that many of these exchanges are conducted without meaningful public oversight — as the example of the facial recognition database

---

309 The agreement initiating Virginia's fusion center, for instance, entered into between Virginia and the FBI, purports to contract around the state's sunshine act, providing that any requests for information would be "referred" to the FBI for further action, rather than fulfilled according to state law. *See* Memorandum of Understanding Between the Fed. Bureau of Investigation and the Va. Fusion Ctr. § VI.A (Feb. 28, 2008) (on file with the Harvard Law School Library).

310 *See supra* section II.C.3, pp. 1050–53.

311 This is the basis, for example, of the rule against apparent authority in government contracting. Government agents must have *actual* authority to bind the government to financial transactions.

312 *E.g.*, Hills, *supra* note 204, at 1236.

makes clear. There are thus scarce opportunities for the individuals whose private data is shared between governments to decide whether access to that data should be expanded or contracted, and on what terms.

More broadly, this means that the institutions that govern data exchange follow a "legal process" for making consequential governmental decisions that is characterized by a highly attenuated relationship to traditional sources of legal authority — thus calling into question not only the democratic legitimacy of the rules that are enacted, but in some cases, the basic procedural legitimacy of those rules themselves. Federalism scholarship and doctrine presume that the lawmaking mechanisms established by the federal government and the states are procedurally and democratically legitimate in a basic sense — that when the states and federal government negotiate over the terms of joint programs, they represent their respective constituencies. The legal process of data exchange at least raises questions about that assumption.

To be sure, we can also see opportunity and possibility in the institutional arrangements that characterize data federalism. Federal and state legislatures are not always best positioned to adapt statutory enabling authority to the needs of modern technologies. Having more flexible ways of allowing the federal government and states to join forces in the use of innovative technologies may help draw the social benefits of those technologies out. Indeed, having more flexible ways to structure *any* form of policy program could expand our chance of adapting that program to socially beneficial ends. This interstitial federalism creates an entirely new set of institutional possibilities. It allows us to envision new forms of institutions that draw the relevant parties to a common table in a much wider variety of ways.

Those who worry about the overweening power of the federal government may also appreciate the ways that these institutions empower states to be more significant bargaining parties. Why, if the Tenth Amendment reserves to the states all powers not granted to the federal government, should the states not initiate intergovernmental efforts more collaboratively, instead of simply being the beneficiaries of Congress's largesse?

CONCLUSION: BEYOND DATA

My aim in this Article is not to offer the last word on intergovernmental data exchange, but only an early one — to open avenues of future research and analysis. Data is not going away, and the ways it changes governance will only multiply. As data continues to occupy a place at the core of our social, economic, and political lives, it is appropriate that our system of government — our federalism — both shapes and is shaped by it.

But data is not the only new form of power that our governments use, trade, negotiate, and structure institutions around. There are other

forms of governmental power that have yet to enter our conversations about federalism but that, like data, could alter how we see our governments interacting. Before the twentieth century, for instance, it should not be surprising that the dominant power our governments bargained over was not money or administrative capacity, but land, a form of power with unique attributes of its own.[313] And today, our governments are experimenting with ways to alienate powers we have not traditionally viewed as transferable, like the capacity to exercise legitimate coercive force against their constituents. Our governments have a robust trade in that power as they cross-deputize police and immigration officers and house federal inmates in state prisons and state inmates in federal ones.

And although the unorthodox forms of governance I have canvassed here are particularly pronounced in the data world because of Congress's light touch, there is reason to believe that they also arise in more traditional areas. Intergovernmental agreements are used to fill in gaps that Congress leaves even in the most comprehensive statutes; I would hypothesize that we would find odd institutions above them even there.

Data federalism, then, is a case study in a federalism that is always evolving: in the powers it distributes, in the ways it facilitates cooperation and incites conflict, and in the tools it provides our governments to jointly address common problems.

---

[313] *See generally* Gregory Ablavsky, *The Rise of Federal Title*, 106 CALIF. L. REV. 631 (2018); ROBERT JAY DILGER & MICHAEL H. CECIRE, CONG. RSCH. SERV., R40638, FEDERAL GRANTS TO STATE AND LOCAL GOVERNMENTS: A HISTORICAL PERSPECTIVE ON CONTEMPORARY ISSUES 14 (2019), https://fas.org/sgp/crs/misc/R40638.pdf [https://perma.cc/5H66-MEHZ] ("[Prior to the Civil War,] Congress typically authorized federal land grants to states instead of authorizing direct cash assistance to states for internal improvements.").