CHAPMAN LAW REVIEW

Citation: Paul M. Schwartz, *Data Privacy Federalism 3.0*, 29 CHAP. L. REV. 465 (2026).

Data Privacy Federalism 3.0

Paul M. Schwartz

CONTENTS

Data Privacy Federalism 3.0

*Paul M. Schwartz**

Federalism is a bedrock concept in the political organization of the United States. It is also a topic of intensive scholarly attention. Yet, compared to other areas of federalism, questions concerning personal data have received little notice. This Article's analysis of data privacy federalism is organized around two topics: preemption (Data Privacy Federalism 1.0) and anti-commandeering (Data Privacy Federalism 2.0). It argues that recent developments have dramatically changed the landscape for preemption and federal-state data sharing, resulting in Data Federalism 3.0.

In Data Federalism 3.0, a number of developments have dramatically altered the past landscape for preemption. First, there has been an explosion of omnibus state privacy statutes. Second, there is a continuing lack of a federal omnibus privacy law and an almost complete absence of congressional privacy lawmaking at the sectoral level. This Article advocates for continuing state lawmaking on privacy matters and does so on federalism grounds. State lawmaking about data privacy is supported by the classic Brandeisian notion of the states as laboratories for innovative policymaking. In addition, there is the potential of states to serve as catalysts for bipartisan policy cooperation.

There have also been important recent developments concerning the sharing of personal data among different levels of government. These changes significantly implicate the anti-commandeering doctrine. Data-driven unilateral actions by the Trump administration toward the states represent "agonistic federalism," to use a term recently coined by Professors Aziz Huq and Zachary Clopton. The executive branch has engaged in a hostile attack on the states by weaponizing personal data collected through federal-state programs. In response, this Article proposes that anti-commandeering provisions should extend to personal information. The states should develop this constitutional doctrine as part of their opposition to the Trump administration's seizures of personal data. This Article's main lesson is that the future of federalism depends on the rules for personal data sharing among the federal and state governments.

---

* Jefferson E. Peyser Professor of Law. This Article was presented on February 6, 2026, as the Keynote Address at the *Chapman Law Review*'s symposium, Data Flow Frontiers. My thanks to Brianna Gerth and Jack Mays of the *Chapman Law Review* for their expert assistance and to symposium participants for their helpful remarks. Many thanks as well to my research assistants Nadia Orchid Ghaffari, Aaniyah Hicks, and Allen Park. Thanks as well to Doug Avilla and I-Wei Wang of the Berkeley Law Library. Finally, I am grateful to Professor Aziz Huq and Dean Erwin Chemerinsky for their helpful comments.

I. INTRODUCTION

Federalism is a bedrock concept in the political organization of the United States. As the Supreme Court has held, "[i]t is incontest[able] that the Constitution established a system of 'dual sovereignty.'"[1] While the states surrendered many of their powers to the federal government at the founding, they retained explicit and implicit sovereignty under the Constitution. Federalism is also a topic of intensive scholarly attention. Yet, compared to other areas of federalism, questions concerning personal data have received little notice.

An analysis of data privacy federalism can be structured around two topics. First, there is the issue of preemption. Data Privacy Federalism 1.0 considers the extent to which federal law should preempt state law in regulating the use of personal data by private companies. Should data privacy issues involving the private sector be regulated by the federal government, or by state governments? Should this power be shared and, if so, how? These questions have been present from the enactment of the first federal data privacy law in 1970.[2]

Second, there is the matter of the terms and conditions under which federal and state governments share personal data with each other. A central issue in Data Privacy Federalism 2.0 is the extent to which the Constitution limits the authority of the federal government to access state data. Under the anti-commandeering principle, neither Congress nor the executive branch can "command" state and local officials in certain ways.[3] Yet, the Supreme Court has never decided whether the core federalism principle of anti-commandeering applies to personal data. The question remains open as to whether there is an "information sharing exception" to federalism.[4]

Recent political developments have dramatically changed the landscape for preemption and federal-state data sharing. The result is Data Federalism 3.0. This Article explores the altered outlook for these aspects of federalism. It advocates for continuing

---

1 Printz v. United States, 521 U.S. 898, 918 (1997) (quoting Gregory v. Ashcroft, 501 U.S. 452, 457 (1991)).

2 For an introduction to preemption issues present in data privacy law, see generally Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009).

3 For an introduction, see *Amdt10.4.2 Anti-Commandeering Doctrine*, CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/amdt10-4-2/ALDE_00013627/ [https://perma.cc/59BC-ZNYS] (last visited Mar. 25, 2026).

4 Bridget A. Fahey, *Data Federalism*, 135 HARV. L. REV. 1007, 1026 (2022).

state enactment of data privacy legislation and calls for development of anti-commandeering principles to guard against the ongoing data grabs of the executive branch. These actions by the federal government have changed the past terms of data sharing for a variety of vitally important federal-state programs, including Medicaid and the Supplemental Nutrition Assistance Program (SNAP).[5]

Before this Article turns to data privacy federalism, an introduction to the basics of data privacy law and federalism would be helpful. Data privacy law defines rules for personal data processing by organizations and individuals.[6] As a normative matter, data privacy serves an essential role in promoting individual autonomy and democracy.[7] Yet, the collection, processing, and transfer of personal data are also essential. These activities can promote economic development, assist law enforcement, safeguard national security, and further other important policy goals.

As for federalism, it distributes power among a central government and subdivisional governments. Federalism considers which powers should belong to the national authority, which to the states and localities, and which are to be shared.[8] Like data privacy, which seeks to establish appropriate tradeoffs among different policy goals, federalism does not seek to maximize the authority of a single level of government but instead seeks to assign governmental authority among dual sovereigns. This Article's main lesson is that the future of federalism depends on the rules for personal data sharing among the federal and state governments.

II. DATA PRIVACY FEDERALISM 1.0: PREEMPTION

Data Privacy Federalism 1.0 is about the division of power among different levels of government when regulating private sector data use. The first federal data privacy law in the United

---

5 *See, e.g.*, Jude Joffe-Block, *At Least 27 States Turned Over Sensitive Data About Food Stamp Recipients to USDA*, NPR (Oct. 16, 2025, at 12:55 ET), https://www.npr.org/2025/10/16/nx-s1-5533045/snap-privacy-usda-lawsuit [https://perma.cc/4N6N-J6KX].

6 DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 2 (8th ed. 2024).

7 *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613–14 (1999); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 709–10 (1987).

8 For an overview of federalism scholarship, see Jessica Bulman-Pozen, *From Sovereignty and Process to Administration and Politics: The Afterlife of American Federalism*, 123 YALE L.J. 1920, 1924–27 (2014).

States, the Fair Credit Reporting Act (FCRA) (1970), contains a strong preemption clause. From the start, the FCRA preempted state laws "to the extent that those laws are inconsistent with any provision of [it]."[9] Congress has also modified the contours of the FCRA preemption several times in the more than half-century since its enactment.[10] In 1996, for example, Congress expanded the FCRA's preemption of state laws inconsistent with any provision of the FCRA. The 1996 amendment to the statute explicitly references "any State regulation related to specifically enumerated subjects already regulated by the FCRA."[11] Enumerated subjects in this law include the prescreening of consumer reports, the duties of a person who takes adverse action in respect to a consumer, and the information available to victims of identity theft.[12]

As this example demonstrates, preemption has long been a moving target for data privacy federalism. It is also a vitally important doctrine because of how the United States regulates this area. Unlike the rest of the world, the United States lacks a so-called omnibus or general national data protection law.[13] Almost all other countries have enacted such a national law, and the European Union itself has taken this approach at a supranational level.[14] Its General Data Protection Regulation is one of the most influential privacy regulations in the world.[15] In the United States, in contrast, Congress has traditionally proceeded through the enactment of sectoral laws, that is, laws that regulate only a specific area of personal data use.[16]

The number of federal sectoral laws is extensive, but there are also notable gaps remaining. Federal data privacy statutes include the FCRA (1970), the Family Educational Rights and Privacy Act (1974), the Driver's Privacy Protection Act (DPPA) (1994), the Electronic Communications Privacy Act

---

9 15 U.S.C. § 1681t(a).

10 As the Consumer Financial Protection Bureau summarizes regarding the FCRA in a 2025 interpretative rule, "the scope of that preemption has changed over time." Fair Credit Reporting Act; Preemption of State Laws, 90 Fed. Reg. No. 48710, 48710–11 (Oct. 28, 2025) (to be codified at 12 C.F.R. pt. 1022).

11 For a discussion, see *id.* at 48711–12.

12 *See id.*

13 SOLOVE & SCHWARTZ, *supra* note 6, at 1056–57.

14 *See id.* at 1056.

15 *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 772 (2019).

16 STEPHEN P. MULLIGAN, WILSON C. FREEMAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., DATA PROTECTION LAW: AN OVERVIEW 7 n.60 (2019).

(1986), the Video Privacy Protection Act (VPPA) (1988), the Health Insurance Portability and Accountability Act (HIPAA) (1996), the Children's Online Privacy Protection Act (COPPA) (1998), and the Gramm-Leach-Bliley Act (1999). The jurisdictional reach of these laws rests on the congressional vision at the time of enactment, including its understanding of the critical technology of that day. To illustrate, the FCRA's reach rests on the concept of a "consumer reporting agency," a settled idea in 1970, but an area of commerce with more fluid borders today.[17] The nearly forty-year-old VPPA's meaning in the twenty-first century turns on judicial interpretations of several key statutory terms, including "video tape service provider."[18]

In addressing the extent to which federal and state data privacy laws should or should not co-exist, Congress has developed a variety of solutions. These approaches to data preemption are important because many state sectoral laws occupy the same or similar terrain as federal statutes. For example, the leading federal health care privacy regulation is HIPAA's Privacy Rule, which explicitly permits stricter state laws.[19] HIPAA sets a floor for protection of individuals. But to complicate matters, HIPAA also preempts any state law that is "contrary" to it.[20] A contrary state law is one that makes it impossible to comply with both HIPAA and state law. There is ample case law analyzing whether a state health privacy law is more protective of patients, or is, in fact, contrary to the federal regulation.[21]

Another set of issues is raised when state sectoral privacy laws are enacted *before* a federal law aimed at a similar area of personal data use. For example, there are no federal biometric statutes, but states, including Colorado, Texas, Illinois, and Ore-

---

17 *See* Fair Credit Reporting Act, 15 U.S.C. § 1681a(f). To illustrate, Spokeo, the operator of a "people search engine" and not a traditional "credit reporting agency," was engaging in activities that fell under the FCRA's scope. Spokeo, Inc. v. Robins, 578 U.S. 330, 333–36 (2016).

18 18 U.S.C. § 2710(a)(4); *see, e.g.*, Osheske v. Silver Cinemas Acquisition Co., 132 F.4th 1110, 1111 (9th Cir. 2025) (noting that "a classic in-theater movie-going experience is [not] subject to the Video Privacy Protection Act," even if its website shows trailers for films).

19 45 C.F.R. § 160.203(b) (2026).

20 *Id.* § 160.202.

21 *See, e.g.*, Ledford v. UofL Health-Louisville, Inc., 720 S.W.3d 594, 601 (Ky. Ct. App. 2025) ("State laws that are not contrary to HIPAA are not preempted. If, and only if, a state law is contrary to HIPAA must a court then consider whether the state law is more stringent."); Washington v. Alderwood Surgical Ctr., LLC, No. C22-1835-RSM, 2023 WL 6461145, at *3 (W.D. Wash. Oct. 4, 2023) (noting that "since Washington state law is more stringent than HIPAA, the [Uniform Healthcare Information Act] preempts the federal procedure").

gon, have passed such laws.[22] The Illinois Biometric Information Privacy Act (BIPA) (2008) is the most important of these statutes, at least judging from the amount of litigation and high monetary settlements that it has generated.[23] Should the federal government express interest in enacting a federal biometric statute, these states, as first-movers, will likely oppose any congressional enactment that would water down their own laws.

Fortunately, preemption under Data Privacy Federalism 1.0 has never been an all-or-nothing matter. As noted above, Congress has an impressive toolkit for setting the terms of the interplay between federal and state laws. These include subject matter preemption; the creation of ceilings and floors in federal legislation; the limitation of a ceiling or floor only to "conduct" regulated; sunset provisions (which re-open federal-state negotiations after a set period); and the sharing of enforcement authority.[24] As we have seen, the FCRA demonstrates that federal preemption choices can change over time through congressional amendment of laws. The FCRA has made use of a sunset provision, which permitted a re-opening of federal-state negotiations in 2003.[25] With the enactment that year of the Fair and Accurate Credit Transactions Act, an amendment to the FCRA, Congress removed any sunsets from the FCRA.[26]

The results of Data Federalism 1.0 have also sometimes been uncomplicated. As an example, COPPA permits enforcement of its requirements both by the Federal Trade Commission (FTC), the leading federal consumer protection agency, and by state Attorneys General. Shared prosecutorial powers have led to many successful enforcements to protect children's interests. To illustrate, the FTC and New York carried out a joint enforcement ac-

---

22 Bobby Allyn, *With No Federal Facial Recognition Law, States Rush To Fill Void*, NPR (Aug. 28, 2025, at 13:23 ET), https://www.npr.org/2025/08/28/nx-s1-5519756/biometrics-facial-recognition-laws-privacy [https://perma.cc/XMR8-ZHWC]; *Global Biometrics Regulation Chart*, BAKER DONELSON (May 2025), https://www.bakerdonelson.com/webfiles/Publications/Global-Biometrics-Laws-Chart.pdf [https://perma.cc/XL59-7MYL].

23 Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10 (2024); *see* Ryan Kenney, *What Is BIPA and Why Does It Matter?*, EDGEWORTH ECON. (Sep. 7, 2023), https://www.edgeworthеconomics.com/insight-what-is-BIPA-why-does-matter [https://perma.cc/5ZDK-ADWQ]. For a discussion on the significance and impact of BIPA, see SOLOVE & SCHWARTZ, *supra* note 6, at 854–62.

24 Schwartz, *supra* note 2, at 919–21, 943, 945.

25 *See* Fair Credit Reporting Act; Preemption of State Laws, 90 Fed. Reg. 48710, 48714 (Oct. 28, 2025) (to be codified at 12 C.F.R. pt. 1022).

26 *See id.*

tion against Google that settled for $170 million in 2019.[27] The split saw $136 million collected by the FTC and $34 million by New York.[28]

Similarly, HIPAA permits enforcement of its provisions by both the Department of Health and Human Services (HHS) and state Attorneys General.[29] This division of authority has led to high settlements by both entities following investigations of violations of federal health care law.[30] States also sometimes pool resources and engage in multistate actions. One such action by New York, New Jersey, and Connecticut in 2024 led to a $4.5 million settlement with Enzo Biochem.[31]

III. DATA PRIVACY FEDERALISM 2.0: ANTI-COMMANDEERING

We turn now to Data Federalism 2.0, which concerns the sharing of data among different levels of government. As a distinct field of law, data privacy first emerged in the late 1960s and early 1970s.[32] A key concern of that time was the threat posed by the increasing amount of personal data in control of the government. In his account of the rise of first-generation data privacy statutes, Viktor Mayer-Schönberger summarizes, "Without computers a modern welfare state could not operate."[33] In particular, the Great Society of President Lyndon B. Johnson sought the creation of domestic programs to expand social welfare, eliminate racial injustice, and improve access to education and healthcare.

---

27 Press Release, Fed. Trade Comm'n, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sep. 4, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law [https://perma.cc/7VSU-TY4U].

28 *Id.*

29 *See State Attorneys General*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Dec. 21, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/index.html [https://perma.cc/85PE-LGBJ] (noting that a 2009 amendment to HIPAA added this authority for state Attorneys General).

30 The largest HIPAA fine collected to date by the federal government was the 2018 penalty assessed against Anthem Inc. for a data breach. *See Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest Health Data Breach in History*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Oct. 15, 2018), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/anthem/index.html [https://perma.cc/F3Z6-Y9DD].

31 Steve Alder, *HIPAA Enforcement by State Attorneys General*, THE HIPAA J. (Jan. 25, 2026), https://www.hipaajournal.com/hipaa-enforcement-by-state-attorneys-general/ [https://perma.cc/99ZP-56T5].

32 For a comparative study examining the rise of data privacy law, see COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 2–3 (1992).

33 Viktor Mayer-Schönberger, *Generational Development of Data Protection in Europe*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 219, 222 (Phillip E. Agre & Marc Rotenberg eds., 1997).

This agenda also called for enhanced governmental collection of digitalized personal data.[34]

The rational provision of governmental services meant not only the computerization of personal data, but the linkage of information held by different levels of government. Many social welfare programs in the United States involve joint federal and state administration. Medicaid provides a good example of Data Federalism 2.0. Created in 1965, Medicaid is a joint federal-state program that provides free or low-cost health coverage to millions of low-income individuals.[35] It is also a data-driven partnership in which the federal government sets guidelines, oversees compliance, and approves state plans. As for the states, they operate the program and determine eligibility within federal rules.

Until recently, the sharing of data among different levels of government received scant scholarly attention. That changed in 2022 with the publication of Professor Bridget Fahey's path-breaking article, *Data Federalism*.[36] In it, Professor Fahey develops an insightful account of federal-state "data pools."[37] Her article identifies four essential elements present in the "intergovernmental data market."[38] First, personal data should be seen as a form of governmental power.[39] Second, federalism now does more than divide governing authority; it concerns the terms of access to personal data.[40] Third, rather than traditional cooperative federalism, which is established through detailed federal statutes, data federalism operates in an "interstitial space" where different levels of government collaboratively fill in gaps in statutory formal law through negotiated agreements about sharing data.[41]

As for Professor Fahey's fourth point, it links data federalism to an important constitutional limitation on the federal government, namely, the anti-commandeering principle.[42] *Printz v. United States* is the leading Supreme Court case about

---

34 *See* BENNETT, *supra* note 32, at 46, 68–70.

35 *Medicaid 101*, MEDICAID & CHIP PAYMENT & ACCESS COMM'N, https://www.macpac.gov/medicaid-101/ [http://perma.cc/AM7J-65R9] (last visited Mar. 18, 2026).

36 *See* Fahey, *supra* note 4, at 1009.

37 *Id.* at 1012.

38 *Id.* at 1016–29.

39 *Id.* at 1017.

40 *Id.* at 1029.

41 *Id.* at 1014.

42 *Id.* at 1054–55.

this doctrine.[43] In it, the Court observed that "the Federal Government . . . may not compel the States to enact or administer a federal regulatory program."[44] As Justice Antonin Scalia stated for the *Printz* Court, the Federal Government cannot issue orders requiring that the states address particular problems.[45] It also cannot command state officers "to administer or enforce a federal regulatory program."[46] In the view of the *Printz* Court, "[S]uch commands are fundamentally incompatible with our constitutional system of dual sovereignty."[47]

How does anti-commandeering relate to data privacy federalism? According to Professor Fahey, data takings by the federal government should be seen as a form of "commandeering." When the federal government engages in "snatching up and carting away" state data assets, it is engaging in "commandeering" that is contrary to the Constitution.[48] We turn now to Data Privacy Federalism 3.0. How have recent developments changed the terms of the debate around preemption and anti-commandeering?

IV. DATA PRIVACY FEDERALISM 3.0

The foundation for federalism policy considerations has shifted considerably. These developments more than justify viewing the new era as one of Data Privacy Federalism 3.0.

A. Preemption Today

Regarding preemption, two important changes have occurred in the privacy landscape. The first is the explosion of omnibus state privacy statutes. The second is the continuing lack of a federal omnibus privacy law, as well as an almost complete absence of congressional privacy lawmaking at the sectoral level.[49]

---

43 *See* 521 U.S. 898, 925 (1997).

44 *Id.* at 926 (quoting New York v. United States, 505 U.S. 144, 188 (1992)).

45 *Id.* at 935.

46 *Id.*

47 *Id.*

48 *Id.*

49 In 2025, Congress enacted the TAKE IT DOWN Act, Pub. L. No. 119-12, 139 Stat. 55. This statute criminalizes the non-consensual publication of intimate imagery and gives enforcement power to the FTC. David Leibert, *Congress's Attempt to Criminalize Nonconsensual Intimate Imagery: The Benefits and Potential Shortcomings of the TAKE IT DOWN Act*, NAT'L ASS'N OF ATT'YS GEN. (Aug. 26, 2025), https://www.naag.org/attorney-general-journal/congresss-attempt-to-criminalize-nonconsensual-intimate-imagery-the-benefits-and-potential-shortcomings-of-the-take-it-down-act/ [https://perma.cc/UUV7-FND6].

Already in 2013, a headline in the *New York Times* noted, *No U.S. Action, so States Move on Privacy Law*.[50] The article observed that over two dozen sectoral privacy laws had been enacted that year in more than ten states, and "in places as different as Oklahoma and California."[51] Some of the most important state legislation at the time concerned data breach notification and data disposal requirements. All fifty states and the District of Columbia have now enacted data breach notification statutes.[52] The only federal requirement in this area is found in an amendment to HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) Act (2009), which requires HIPAA-covered entities and their business associates to notify affected individuals and the Secretary of HHS within sixty days of discovery of a breach of certain kinds of personal data.[53] Like HIPAA, the HITECH Act only preempts state breach notification laws that are less protective than it or that conflict with federal requirements.[54]

The next important development at the state-level dates back to 2018 and the enactment of the California Consumer Privacy Act (CCPA).[55] This law is an EU-style general data privacy law. As Professor Graham Greenleaf observed in 2020, "[f]ifty years after the 1970 enactment of the first data privacy Act by the German state of Hesse, the US private sector finally has a broadly applicable data privacy Act."[56] In recent years, other states have followed California's example and enacted omnibus-style privacy laws. There are now twenty states with such general laws.

An area of cutting-edge sectoral state legislation concerns geolocational data. In 2025, Maryland and Oregon banned the sale of precise geolocational data.[57] At least four other states

---

50 Somini Sengupta, *No U.S. Action, so States Move on Privacy Law*, N.Y. TIMES (Oct. 30, 2013), https://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html [https://perma.cc/32LN-G6G8].

51 *Id.*

52 SOLOVE & SCHWARTZ, *supra* note 6, at 901–05.

53 45 C.F.R. §§ 164.400–.414 (2026).

54 The obligations of state laws that are stricter than HIPAA must be followed. State breach notification laws, however, generally sweep more broadly than HITECH by covering leaks of all personal data law, including non-health data. In contrast, HITECH reaches only "Protected Health Information." 45 C.F.R. § 160.102; *see also* SOLOVE & SCHWARTZ, *supra* note 6, at 453.

55 The law is codified at Title 1.81.5. CAL. CIV. CODE §§ 1798.100–.199.100 (2023).

56 Graham Greenleaf, *California's CCPA 2.0: Does the US Finally Have a Data Privacy Act?*, 168 PRIV. L. & BUS. INT'L REP., Dec. 2020, at 16–17, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3793435 [https://perma.cc/S3QT-6DHT].

57 *See* Tonya Riley, *Protecting Geolocation Data Emerges as State Privacy Priority*, BLOOMBERG L. (Feb. 13, 2026, at 02:00 PT), https://news.bloomberglaw.com/privacy-and-data-

have now introduced bills that ban the sale of geolocational data.[58] Another frontier of state sectoral regulation is surveillance pricing. New York has now enacted a law requiring disclosure to consumers when companies use algorithms to set prices.[59] In contrast to dynamic pricing, which changes prices based on overall market demand, surveillance pricing leverages an individual's personal data to set a tailored cost for a product or service.[60] Violations of the New York law can result in civil penalties of up to $1,000 per violation.[61]

Finally, state enactment of sectoral privacy laws includes a wave of laws regulating AI. While AI is not exclusively a data privacy issue, it raises significant issues about this area. In the assessment of Professor Daniel Solove, "AI remixes existing privacy problems in complex and unique ways."[62] For example, it encourages collection of more personal data to improve predictive AI's accuracy.[63] AI also raises privacy concerns around the scraping of data online without consent and the leakage from large language models that can release personal information drawn on in training models.[64] At present, four states have broadly applicable AI laws: California, Colorado, Texas, and Utah.[65] Beyond these general AI statutes, and somewhat surprisingly, almost every state has enacted regulations affecting one or another aspect of AI.[66]

In contrast to this intense state activity, Congress has been mired in gridlock around privacy legislation, including an absence of federal laws regarding geolocational data, surveillance pricing, or AI. The standstill reflects an overall lack of congres-

---

security/protecting-geolocation-data-emerges-as-state-privacy-priority [https://perma.cc/R9M4-2EUS].

58 *Id.*

59 *Consumer Alert: Attorney General James Warns New Yorkers About Algorithmic Pricing as New Law Takes Effect*, N.Y. STATE ATT'Y GEN. (Nov. 5, 2025), https://ag.ny.gov/press-release/2025/attorney-general-james-warns-new-yorkers-about-algorithmic-pricing-new-law-takes [https://perma.cc/X2GE-YKQ8].

60 Darrell M. West, *What Is Dynamic Pricing and Why Do Consumers Need Better Protections?*, BROOKINGS INST. (Mar. 18, 2026), https://www.brookings.edu/articles/what-is-dynamic-pricing-and-why-do-consumers-need-better-protections/ [https://perma.cc/ZDU6-4MWP].

61 *Consumer Alert*, *supra* note 59.

62 Daniel J. Solove, *Artificial Intelligence and Privacy*, 77 FLA. L. REV. 1, 5 (2025).

63 *See id.* at 9–11.

64 *See id.* at 5–6, 9–11.

65 *Artificial Intelligence Update - August 2025*, QUINN EMANUEL (Aug. 18, 2025), https://www.quinnemanuel.com/the-firm/publications/artificial-intelligence-update-august-2025/ [https://perma.cc/VC4M-7F5R].

66 *See U.S. AI Law Tracker*, ORRICK (Mar. 27, 2026), https://ai-law-center.orrick.com/wp-content/uploads/Orrick-US-AI-Law-Tracker.pdf [https://perma.cc/3XFB-AHQ7].

sional activity; beyond data privacy, the current Congress has "a growing reputation as the least productive in modern history."[67] The most recent significant federal attempt to enact a national privacy law concerned the proposed 2022 American Data Privacy and Protection Act.[68] One of the most important hurdles to enactment of this bill and subsequent omnibus privacy bills has been whether the national law would override stricter state laws, such as California's CCPA.[69] Congressional enactment of new sectoral privacy laws is also at a virtual standstill.

With each new general state privacy law enacted, the task of passing a federal law has become more difficult. Yet, this result is not inevitable. Indeed, as scholars have demonstrated, state legislative efforts in a variety of areas (such as environmental law) led to a "flight to Washington" by regulated industries to seek a federal legislative solution. J.R. DeShazo and Jody Freeman have termed this phenomenon "defensive preemption."[70] As DeShazo and Freeman observe, state-level regulations can motivate regulated industries and prompt their demand for federal preemptive lawmaking.[71] In writing about preemption and privacy in 2009, I devoted much of my analysis to "life under defensive preemption" for privacy law.[72] At the time, it seemed likely to me that the future of privacy law would be, if not a federal omnibus law, a federal consolidation of state sectoral laws. Yet, even federal sectoral lawmaking has not occurred with any frequency.

It is an open question as to why Congress has been inactive in the privacy landscape. One factor may be a lack of pressure in D.C. by tech companies in favor of a federal privacy law. It is possible that the tech industry now has a general distrust of federal legislative solutions and is willing to live with the (state) devils that it knows. Something like that may explain why there are now fifty state breach notification laws and no sectoral

---

67 Barbara Sprunt, *'Congress is in a Coma.' Former Lawmakers Sound Alarm on Health of the House*, NPR (Dec. 21, 2025, at 05:00 ET), https://www.npr.org/2025/12/21/g-s1-101741/congress-is-in-a-coma-former-lawmakers-sound-alarm-on-health-of-the-house [https://perma.cc/ST89-CZ2W].

68 American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

69 Emily Catron & Gary Kibel, *Federal Data Privacy Legislation: Differences with State Laws Raise Preemption Issues*, REUTERS (Aug. 10, 2022), https://www.reuters.com/legal/legalindustry/federal-data-privacy-legislation-differences-with-state-laws-raise-preemption-2022-08-10/ [https://perma.cc/ZUP2-6XCW].

70 J.R. DeShazo & Jody Freeman, *Timing and Form of Federal Regulation: The Case of Climate Change*, 155 U. PA. L. REV. 1499, 1500 (2007).

71 *Id.* at 1530.

72 Schwartz, *supra* note 2, at 931–40.

federal data breach notification statute that would consolidate the sometimes vastly different obligations under the state statutes. Another possibility is that the many chokepoints in Congress mean that only legislation with overwhelming bipartisan support can be enacted.[73]

Beyond gridlock, another development has been the attempt of the Trump administration to prohibit or limit state regulation in emerging technological areas. To be sure, there has not yet been a federal attempt to stop states from enacting omnibus data privacy statutes. Rather, this federal effort has centered around AI, which, as already noted, is a matter that raises privacy concerns and has led to considerable state legislative activity. Revoking the Biden administration's Executive Order 14067, President Donald Trump's Executive Order 14365 has sought to federalize the issue of AI regulation. Issued on December 11, 2025, this Executive Order mandates a "minimally burdensome national policy framework for AI."[74] The order observes, "State-by-State regulation by definition creates a patchwork of 50 different regulatory regimes that makes compliance more challenging, particularly for start-ups."[75] It calls for congressional action "to ensure that there is a minimally burdensome national standard—not 50 discordant State ones."[76]

Trump's Executive Order would permit state activity concerning AI only in limited areas, including child safety and infrastructure development.[77] Pursuant to it, Congress is to block other state AI laws.[78] The Executive Order also raises specific objections to state AI regulation that is considered to be ideologically-driven or violative of the First Amendment.[79] In anticipation of the enactment of a minimally burdensome federal law, the order also creates an AI Litigation Task Force at the Department of Justice. Its task is to challenge state AI laws that are "inconsistent with the policy set forth" in the order.[80]

---

73 Abraham Newman points to the presence in the United States of extensive institutional veto points on the enactment of new legislation, "including the bicameral nature of the U.S. Congress and the presidential system," as a historic factor limiting the scope of U.S. federal privacy law. ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 59–60 (2008).

74 Exec. Order No. 14365, 90 Fed. Reg. 58499, 58499 (Dec. 16, 2025).

75 *Id.*

76 *Id.*

77 *Id.*

78 *Id.*

79 *Id.* at 58500.

80 *Id.* at 58499.

In parallel to the issuance of the Executive Order, the House of Representatives introduced a ten-year ban on states and municipalities enacting laws and regulations related to AI.[81] Ultimately, the Senate rejected this bill and did so overwhelmingly.[82] A second congressional attempt to block state AI laws involved placing the ban in the National Defense Authorization Act.[83] Ultimately, this provision was stripped from the defense bill.[84] At that time, Republican House leadership promised that AI preemption language would show up in future legislation.[85]

The latest salvo in this federal-state conflict is represented by the Trump administration's National Policy Framework for Artificial Intelligence, released on March 20, 2026.[86] The framework emphasizes the need for congressional action regulating AI.[87] Among its goals, it calls for enactment of a federal AI law to protect children, to respect intellectual property rights, to safeguard residential ratepayers from increased electricity costs due to new AI data centers, and prevent the use of AI in banning "content based on partisan or ideological agendas."[88]

Finally, this document calls for a federal AI policy framework that will preempt cumbersome state AI laws. Much is unclear, however, about the precise boundaries of this future

---

81 Danielle Ochs & Zachary V. Zagger, *U.S. Senate Strikes Proposed 10-Year Ban on State and Local AI Regulation from Spending Bill*, OGLETREE DEAKINS (July 2, 2025), https://ogletree.com/insights-resources/blog-posts/u-s-senate-strikes-proposed-10-year-ban-on-state-and-local-ai-regulation-from-spending-bill/ [https://perma.cc/7TM6-XXZM].

82 Press Release, U.S. Senate Comm. on Com., Sci., & Transp., Senate Strikes AI Moratorium from Budget Reconciliation Bill in Overwhelming 99-1 Vote (July 1, 2025), https://www.commerce.senate.gov/press/dem/release/senate-strikes-ai-moratorium-from-budget-reconciliation-bill-in-overwhelming-99-1-vote-2025-7/ [https://perma.cc/TB8Z-EED9].

83 *See* Press Release, Cong. Progressive Caucus, Congressional Progressive Caucus Announces Official Position Opposing Preemption of State AI Regulations in Annual Pentagon Policy Bill (Nov. 26, 2025), https://progressives.house.gov/2025/11/congressional-progressive-caucus-announces-official-position-opposing-preemption-of-state-ai-regulations-in-annual-pentagon-policy-bill [https://perma.cc/K7JB-KFWL].

84 *See* Joshua A. Geltzer et al., *What the NDAA Means for AI and Cybersecurity*, WILMERHALE (Dec. 19, 2025), https://www.wilmerhale.com/en/insights/client-alerts/20251219-what-the-ndaa-means-for-ai-and-cybersecurity [https://perma.cc/AWF9-K33M].

85 Press Release, Steve Scalise, House Majority Leader, Scalise, Johnson, Guthrie, Jordan, Babin: House Will Work to Implement National AI Framework (Mar. 20, 2026), https://scalise.house.gov/press-releases/Scalise-Johnson-Guthrie-Jordan-Babin-House-Will-Work-to-Implement-National-AI-Framework [https://perma.cc/PDU8-AGFW].

86 *A National Policy Framework for Artificial Intelligence*, THE WHITE HOUSE (March 20, 2026), https://www.whitehouse.gov/wp-content/uploads/2026/03/03.20.26-National-Policy-Framework-for-Artificial-Intelligence-Legislative-Recommendations.pdf [https://perma.cc/L3RH-UJM7].

87 *Id.*

88 *Id.*

preemption. On one hand, "Preemption must ensure that State laws do not govern areas better suited to the Federal Government or act contrary to the United States' national strategy to achieve global AI dominance."[89] On the other hand, the resulting national standard is not to preempt "traditional police powers retained by the states to enforce laws of general applicability against AI developers . . . , including particular laws to protect children, prevent fraud, and protect consumers."[90] In sum, the threat remains of federal blocking legislation that stops state AI laws.

With or without federal blockage of state data lawmaking, continuing state enactment of laws in this area might also lead to significant challenges resting on the Dormant Commerce Clause.[91] The current crop of state data privacy laws are drafted well, however, to survive such challenges. In *National Pork Producers Council v. Ross*, the Supreme Court rejected an expansive view of the Dormant Commerce Clause.[92] California had acted to forbid the in-state sale of whole pork meat that came from breeding pigs that were "confined in a cruel manner."[93] The Court upheld the contested state law largely because the statute imposed the same burden on in-state and out-of-state pork producers. The California statute was not designed to protect local economic interest and penalize out-of-state competitors. Consequently, there was no violation of the "antidiscrimination principle" that rests at the "very core" of Dormant Commerce Clause jurisprudence.[94]

Along the same lines as the California statute in *National Pork Producers Council*, state omnibus privacy laws and emerging state sectoral laws are nondiscriminatory. These laws apply to local and out-of-state industries alike. For example, the CCPA extends its protection to "consumers," defined as California residents, and regulates businesses, whether in-state or out-of-state in the same fashion based on their activities as pertaining to "a

---

89 *Id.*

90 *Id.*

91 For a discussion of the scope of the Dormant Commerce Clause in the age of the Internet, see generally Jack Goldsmith & Eugene Volokh, *State Regulation of Online Behavior: The Dormant Commerce Clause and Geolocation*, 101 TEX. L. REV. 1083 (2023).

92 598 U.S. 356, 364 (2023).

93 *Id.* at 365–66 (quoting CAL. HEALTH & SAFETY CODE § 25990(b)(2) (West 2026)).

94 *Id.* at 369 (citation omitted). For an analysis of this case that finds its core concern in how the Dormant Commerce Clause prevents purposeful discrimination against out-of-state economic interests, see generally Jack Goldsmith & Eugene Volokh, *The Relevance of* Ross *to Geolocation and the Dormant Commerce Clause*, 102 TEX. L. REV. ONLINE 30 (2023).

consumer's personal information."[95] As a further example, the Colorado AI law extends its protections to a "consumer," defined as "an individual who is a Colorado resident."[96] Its obligations apply to a "developer," which means "a person doing business in this state that develops or intentionally and substantially modifies an artificial intelligence system."[97] There is no distinction made between in-state and out-of-state developers. Thus, at least under current caselaw, Dormant Commerce Clause attacks on state data regulations will represent a constitutional challenge that favors the states.

On its own merits, moreover, state lawmaking around emerging privacy issues should be welcome on federalism grounds. An important distinction is first to be made. Concerning privacy lawmaking, I already observed in 2009, "Whether one is a privacy advocate or skeptic, history teaches that the federal government and the states may switch back and forth in their concern for and level of attention to this issue."[98] Moreover, privacy advocates and skeptics alike should exercise realism about the data-driven preferences of the states. For example, regarding data about reproductive choices post-*Dobbs*, states can be expected to exercise the ideological preferences of the majority party. As a consequence, some states will oppose privacy protections for personal data that reveal reproductive decisionmaking. To illustrate, the Texas Attorney General sued the federal government in fall 2024 to stop federal medical privacy rules that would prevent state authorities "from viewing the medical records of women who travel out of state to seek abortions where the procedure is legal."[99]

Independent of one's prior normative commitments, however, a federalism perspective offers at least two insights about potentially positive state contributions to regulating data privacy. The first is the classic Brandeisian notion of the states as laboratories for innovative policymaking. The second is the potential of states as catalysts for bipartisanship policy cooperation.

---

95 CAL. CIV. CODE § 1798.100 (West 2023).

96 S.B. 24-205, 2024 Gen. Assemb., Reg. Sess. (Colo. 2024).

97 *Id.* § 6-1-1701(7).

98 Schwartz, *supra* note 2, at 938.

99 *See* Michael Wines, *Texas Sues for Access to Records of Women Seeking Out-of-State Abortions*, N.Y. TIMES (Sept. 6, 2024), https://www.nytimes.com/2024/09/06/us/texas-abortion-medical-records.html [https://perma.cc/TMX3-XSDY].

We begin with the Brandeisian argument for state lawmaking. Justice Louis Brandeis famously pointed to this benefit of state regulation and identified the ability of these "novel social and economic experiments" to take place, at least some of the time, "without risk to the rest of the country."[100] As regards data privacy law, states have often preceded the federal government in identifying areas of regulatory significance and in taking action. The states have also provided innovative approaches to regulation of privacy. Indeed, the states have created opportunities for simultaneous experiments with different policies.[101]

As for the states as a force for bipartisan policy consensus, some scholars have already explored how federalism can assist different levels of government and various political entities in the United States in negotiating differences. Professor Judith Resnick has identified among the "core challenges of federalism" the production of "shared commitments while respecting differences."[102] In a similar approach, Dean Cristina Rodríguez sees federalism as allowing the creation of a framework for "negotiation of disagreements large and small."[103] In my view, these approaches are especially appealing today because of the fractured times in which we live.[104]

Federalism has tremendous promise as a framework for negotiating national differences concerning the regulation of personal information. This Article has already mentioned joint federal-state enforcement activities under COPPA, a federal law. At the state level as well, there have been shared enforcement actions. For example, a bipartisan coalition of twenty-eight states

---

100 New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

101 See Paul M. Schwartz, *The Value of Privacy Federalism*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 334 (Beate Roessler & Dorota Mokrosinska eds. 2015) (arguing that the "social value of privacy federalism" is to ensure "diversity and competition" in the response to "new kinds of technologies and social forms").

102 Judith Resnick, *Federalism(s)' Forms and Norms: Contesting Rights, Deessentializing Jurisdictional Divides, and Temporizing Accommodations*, *in* FEDERALISM AND SUBSIDIARITY: NOMOS LV 363, 368 (James E. Fleming & Jacob T. Levy eds., 2014).

103 Christina M. Rodríguez, *Negotiating Conflict Through Federalism: Institutional and Popular Perspectives*, 123 YALE L.J. 2094, 2097 (2014).

104 For a prescient analysis of polarized disputes in constitutional adjudication and the development of an "equality principle" for polarized disputes, see generally ROBERT A. BURT, THE CONSTITUTION IN CONFLICT (1992).

has objected to the sale of personal genetic information.[105] The states involved ranged on the political spectrum from Florida, Kansas, and Oklahoma to Colorado, Minnesota, and New York.[106] In addition, both Texas and California are now investigating the personal data practices of car manufacturers, an important topic in today's age of connected cars.[107] Finally, California, joined by several other states, has created the bipartisan Consortium of Privacy Regulators. Ten states are now part of this organization, including one red state, Indiana.[108]

In the age of D.C. gridlock, it is important that the states continue to regulate digital data issues. As Professor Spiros Simitis, a European pioneer of data privacy, stated in 1987, all data privacy regulations "remain provisional measures because of the incessant advances in technology."[109] In Professor Simitis' judgment, "The regulation of personal data collection and retrieval should be regarded as a constant learning process based on continual observation of both the changes in information techniques and the conflicts generated by systematic data use."[110] In the face of the never-ending tidal wave of changes in cyberspace, policy inaction should not be an alternative. The states should continue to seize the day. Moreover, the hope should be for a consolidation of lessons learned, whether through federal law or states amending their statutes.[111]

At the same time, however, the power of the states to regulate data privacy and cybersecurity is not boundless. One possible issue for the future will be whether state privacy enforcement actions interfere with the Constitution's assignment of power

---

105 Press Release, William Tong, Att'y Gen., Connecticut Enters Multistate Legal Fight to Protect Genetic Information in 23andMe (June 11, 2025), https://portal.ct.gov/ag/press-releases/2025-press-releases/connecticut-enters-multistate-legal-fight-to-protect-genetic-information [https://perma.cc/C89P-QGGT].

106 *Id.*

107 Press Release, Cal. Priv. Prot. Agency, Ford to Change Practices, Pay Fine for Adding Unnecessary Friction to Opt-Out Process (Mar. 5, 2026), https://privacy.ca.gov/2026/03/ford-to-change-practices-pay-fine-for-adding-unnecessary-friction-to-opt-out-process/ [https://perma.cc/8KUW-45UP]; Press Release, Ken Paxton, Att'y Gen. of Tex., Attorney General Ken Paxton Opens Investigation into Car Manufacturers' Collection and Sale of Drivers' Data (June 6, 2024), http://texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-opens-investigation-car-manufacturers-collection-and-sale-drivers-data [https://perma.cc/SH5R-TSAX].

108 *Minnesota and New Hampshire Join Bipartisan Consortium as Privacy Collaboration Continues Growing Nationwide*, CAL. PRIV. PROT. AGENCY (Oct. 8, 2025), https://cppa.ca.gov/announcements/2025/20251008.html [https://perma.cc/4NTE-2EVH].

109 Simitis, *supra* note 7, at 742.

110 *Id.* at 741.

111 *See* Schwartz, *supra* note 2, at 939–41.

over foreign relations to the President and Congress. As an example of a state role that touches on foreign affairs, the Texas Attorney General is currently enforcing its general consumer protection law against "China-Aligned Companies."[112] In a series of lawsuits, Ken Paxton, Texas' Attorney General, is arguing that Chinese law requires these companies to divulge Americans' personal data to Chinese intelligence agencies.[113] Texas is also alleging that devices from these entities raise security risks with their products being used to "launch multiple cyber-attack operations against the United States."[114]

To be sure, states are traditionally permitted wide discretion to protect their citizens. A classic example of this protection with a global dimension would be civil or administrative actions against foreign manufacturers of products that cause in-state harm. At the same time, the dormant foreign affairs doctrine restricts the ability of states to intrude into the "field of foreign affairs" reserved for the federal government.[115] In 2003, the Supreme Court drew on this concept in a data privacy case. In *American Insurance Ass'n v. Garamendi*, it invalidated a California law that required insurers licensed in that state to disclose Holocaust-era insurance policies to the California Insurance Commissioner.[116] This information was to be used in a state-run registry of unclaimed Holocaust-era life insurance policies; the hope was that this step would allow descendants of the victims of the Shoah to learn about and collect on these policies.[117] The Supreme Court invalidated the California Holocaust Victim Insurance Relief Act on grounds that "the Executive's responsibility for foreign affairs" blocked this state action.[118]

---

112 *See, e.g.*, Press Release, Att'y Gen. of Tex., Attorney General Paxton Sues TP Link for Allowing the CCP to Access Americans' Devices in First of Several Lawsuits Being Filed this Week Against China-Aligned Companies (Feb. 17, 2026), https://www.texasattorneygeneral.gov/news/releases/attorney-general-paxton-sues-tp-link-allowing-ccp-access-americans-devices-first-several-lawsuits [https://perma.cc/2GYA-QSB6].

113 *Id.*

114 *Id.*

115 Zschernig v. Miller, 389 U.S. 429, 432, 436 (1968). For a discussion, see ERWIN CHEMERINSKY, CONSTITUTIONAL LAW 459–65 (7th ed. 2023).

116 539 U.S. 396, 401 (2003).

117 *See id.* at 410–11.

118 *Id.* at 420. In this case, I had provided an expert opinion regarding German data protection law in the proceedings before the lower courts. Gerling Glob. Reinsurance Corp. of Am. v. Quackenbush, No. S-00-0506WBSJFM, 2000 WL 777978, at *10 (E.D. Cal. 2000), *rev'd sub nom.*, Am. Ins. Ass'n v. Garamendi, 539 U.S. 396 (2003).

There are scant Supreme Court decisions regarding the dormant foreign affairs doctrine. Most likely, state enforcement activities pursuant to general state legislation, as currently pursued by the Texas Attorney General, are constitutionally unproblematic under this doctrine.[119] In contrast, a state statute that singled out a specific foreign nation would likely raise constitutional problems. Such a law might name one or more "countries of concern" and seek to regulate personal data transfers to these foreign adversaries.[120] Thus far, however, the states do not appear interested in enacting such legislation. In my judgment, a greater source of constitutional friction with state data privacy laws will be the First Amendment and its protections for flows of information, including personal data.[121]

B. Anti-Commandeering Today

Professor Fahey has wisely alerted us to the extent that governmental data pools raise federalism issues. And, in this context, there is another notable Trump administration executive order to consider. Trump Executive Order 14243 would radically alter the established process for sharing personal data among different levels of government.[122] In place of past negotiations at the federal and state level around the creation of data pools, the executive branch is now acting by fiat. The Executive Order states, "Immediately upon execution of this order, Agency Heads shall take all necessary steps, to the maximum extent consistent with law, to ensure the Federal Government has unfettered access to comprehensive data from all State programs that receive Federal funding . . . ."[123] The import of this sentence is clear: the Trump administration wishes to command full federal access to data collected through the countless state programs that rely on federal

---

119 As another example, under general state authority, Florida has started a CHINA Prevention Unit within the Office of the Attorney General to address "threats posed by the Chinese Communist Party (CCP) and other foreign adversaries to Florida consumers, data privacy, and economic security." Press Release, Off. of Att'y Gen. State of Fla., Attorney General James Uthmeier Launches China Prevention Unit to Counter Foreign Adversaries and Protect Floridians' Data (Feb. 5, 2026), https://www.myfloridalegal.com/newsrelease/attorney-general-james-uthmeier-launches-china-prevention-unit-counter-foreign [https://perma.cc/WK88-ELUS].

120 *See* Crosby v. Nat'l Foreign Trade Council, 530 U.S. 363, 366 (2000) (invalidating a Massachusetts statute that "bars state entities from buying goods or services" from any company doing business with Burma in a unanimous decision).

121 *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 557 (2011) (invalidating a Vermont prescription privacy law because it singled out pharmaceutical marketers and data miners).

122 Exec. Order No. 14243, 90 Fed. Reg. 13681, 13681–82 (Mar. 20, 2025).

123 *Id.* at 13681.

money. The Executive Order also reaches private-sector data to the extent that a private entity is acting as a vendor managing state information.

Prior to this Executive Order, the Trump administration's new approach to federal-state data relations began through actions by the Department of Government Efficiency (DOGE).[124] One of the aims of this short-lived federal entity was to collect and consolidate personal information from as many federal governmental sources as possible. According to one tally, DOGE tried to gain access to more than eighty data systems across at least ten federal agencies.[125] Its goal was total information sharing and the destruction of any "information silos" within the government regarding personal data.[126] DOGE engaged in an unprecedented data grab to begin construction of a totalizing federal database. As part of its activities, it also seized state-supplied data that was in the control of federal agencies for limited use in administering federal-state programs.

DOGE has now been disbanded, but many of its employees have gone to other federal agencies.[127] While DOGE has vanished as a formal entity, it forged a path that is being followed by other federal agencies, including the Department of Homeland Security (DHS) and the Department of Agriculture (USDA). Twenty states are now suing HHS for sharing state health data with DHS.[128] The

---

124 Exec. Order No. 14158, 90 Fed. Reg. 8441, 8441 (Jan. 29, 2025); *see* Sarah Cahalan et al., *The People Carrying Out Musk's Plan at DOGE*, N.Y. TIMES (June 16, 2025), https://www.nytimes.com/interactive/2025/02/27/us/politics/doge-staff-list.html [https://perma.cc/6CAB-VCTP].

125 Jonathan Swan et al., *A Subdued Musk Backs Away from Washington, but His Project Remains*, N.Y. TIMES (Apr. 24, 2025), https://www.nytimes.com/2025/04/23/us/politics/elon-musk-doge-trump.html [https://perma.cc/GM43-YFLQ].

126 *See* Stephanie K. Pell, Josie Stewart & Brooke Tanner, *Privacy Under Siege: DOGE's One Big, Beautiful Database*, BROOKINGS INST. (June 25, 2025), https://www.brookings.edu/articles/privacy-under-siege-doges-one-big-beautiful-database/ [https://perma.cc/V9CG-NJ3B].

127 Press Release, Elizabeth Warren, Senator, Warren, Blumenthal, Garcia Launch Investigation into DOGE Employees Embedding into Top Government Roles (Aug. 7, 2025), https://www.warren.senate.gov/newsroom/press-releases/warren-blumenthal-garcia-launch-investigation-into-doge-employees-embedding-into-top-government-roles [https://perma.cc/EQN2-WKZP]. For a post-mortem examination of DOGE, see Makena Kelly & Vittoria Elliott, *DOGE Isn't Dead. Here's What Its Operatives Are Doing Now*, WIRED (Dec. 2, 2025, at 06:00 PT), https://www.wired.com/story/what-is-doge-doing-now/ [https://perma.cc/KWT9-C549].

128 Amanda Seitz & Kimberly Kindy, *20 States Sue After the Trump Administration Releases Private Medicaid Data to Deportation Officials*, AP NEWS (July 1, 2025, at 20:07 PT), https://apnews.com/article/trump-medicaid-immigrant-california-161f7e1b9087512d674258f32f822878 [https://perma.cc/456M-Z5J3].

states gave this personal information to HHS for administration of the Medicaid program.[129] Early in the second Trump administration, HHS turned this information over to DHS for immigration enforcement.[130] This action affected millions of individuals.

As for the USDA, it is the federal entity responsible for SNAP, which helps approximately forty-two million Americans, or about one in eight, purchase groceries.[131] The USDA and the states jointly administer this program. In late 2025, the USDA announced that it would stop paying SNAP funds to states that did not turn over extensive personal information about program recipients, including home addresses, Social Security Numbers, recent locations, and immigration status.[132] The federal goal was to use this data for immigration enforcement. Twenty-two states have sued to prevent the Trump administration from demanding that they turn over this data.[133]

In early stages of the ensuing litigation in both matters, state litigants have largely been successful. In December 2025, Judge Vince Chhabria issued a preliminary injunction against the data sharing between HHS and DHS.[134] His injunction does allow basic biographical contact and locational information to be shared by the HHS with the DHS.[135] But Judge Chhabria found that the federal government had offered no justification for its sharing of additional personal data, such as "sensitive medical information about Medicaid patients."[136] In issuing an earlier preliminary injunction, Judge Chhabria pointed to the long-standing HHS policy of not sharing certain personal data of Med-

129 *Id.*

130 *Id.*

131 *See Supplemental Nutrition Assistance Program Participation and Costs*, USDA FOOD & NUTRITION SERV. (Feb. 13, 2026), https://fns-prod.azureedge.us/sites/default/files/resource-files/snap-annualsummary-4.pdf [https://perma.cc/5JNY-Y2U9].

132 Linda Qiu, *Agriculture Dept. Threatens to Withhold Food Stamps from Democratic States*, N.Y. TIMES (Dec. 2, 2025), https://www.nytimes.com/2025/12/02/us/politics/food-stamps-democratic-states.html [https://perma.cc/K7HA-M372].

133 Nate Raymond, *Trump Administration Cannot Force States to Supply Food Stamp Data, US Judge Rules*, REUTERS (Feb. 26, 2026, at 13:48 PT), https://www.reuters.com/legal/government/trump-administration-cannot-force-states-supply-food-stamp-data-us-judge-rules-2026-02-26/ [https://perma.cc/7Z73-ZA2X].

134 Order Granting in Part and Denying in Part Motion for Preliminary Injunction at *1, California v. U.S. Dep't of Health & Hum. Servs., No. 25-cv-05536-VC, 2025 WL 3751931 (N.D. Cal. Dec. 29, 2025).

135 *Id.* at *2–3.

136 *Id.* at *3.

icaid patients and added that various federal and state actors in the Medicaid system had relied on this approach.[137]

In the SNAP litigation, state litigants have also enjoyed victories in federal courts. In September 2025, a district court in the Northern District of California issued a temporary restraining order that prevented the contested data collection and blocked the USDA from withholding administrative funding from states.[138] More recently, on February 26, 2026, this court issued a preliminary injunction that continued the block on the federal withholding of SNAP funding from the states that had refused to share recipient data.[139]

How do these recent data-driven actions by the federal government fit into a federalism framework? The actions of the Trump administration toward the states go far beyond the range of behavior that scholars have termed "uncooperative federalism." To illustrate, we can consider the argument in favor of "uncooperative federalism" by Jessica Bulman-Pozen and Heather Gerken in 2009.[140] As part of their approach, and perhaps unexpectedly, these scholars took a stance in favor of commandeering. In their view, uncooperative federalism can play a positive role in "a well-functioning federal system."[141] Bulman-Pozen and Gerken argue, "[t]he state's leverage over the federal government only increases after the federal government has devolved regulatory powers to the state."[142] Involvement of state officials through commandeering would lead to a range of positive results, including "greater federal-state integration," states with "greater agenda-setting power," and the enabling of state bureaucrats to serve "as 'connected critics' within the federal system."[143] This analysis does not fit the current moment.

When it comes to data privacy federalism at present, there is an absence of federal-state integration, state agenda setting, or

---

137 *See id.*

138 Order Granting Temporary Restraining Order as to All Plaintiff States Other than State of Nevada at 25, California v. U.S. Dep't of Agric., 800 F. Supp. 3d 1015 (N.D. Cal. 2025) (No. 25-cv-06310-MMC).

139 Order Granting in Part Plaintiff States' Motion to Enforce or Expand Preliminary Injunction at *13, California v. U.S. Dep't of Agric., No. 25-cv-06310-MMC, 2026 WL 534417 (N.D. Cal. Feb. 26, 2026).

140 Jessica Bulman-Pozen & Heather K. Gerken, *Uncooperative Federalism*, 118 YALE L.J. 1256, 1258–60 (2009).

141 *Id.* at 1260.

142 *Id.* at 1268.

143 *Id.* at 1297.

connected state critics within the federal system. While we still live in an era of federalism, it is one marked by extreme hostility on the part of the federal government to state policies contrary to the administration's goals. Professors Aziz Huq and Zachary Clopton term this new approach, "agonistic federalism."[144] Federalism under the Trump administration is not an extension of uncooperative federalism. It represents not continuity, but "a rupture of integrated federalism instigated by the federal government."[145] As one of its primary elements, the current administration is engaged in "the weaponization of states' entanglement in cooperative federalism programs."[146] Huq and Clopton argue that "something new is afoot" and point to the volume and scope of the federal actions to terminate state funding upon noncooperation.[147] With considerable understatement, they also note the Trump administration's "disinterest for statutory requirements and settled conventions."[148]

The Huq-Clopton model is extremely helpful in mapping the contours of the second Trump administration's approach to data privacy federalism. The Trump administration is now seizing and consolidating data from within federal-state data pools (as in the Medicaid example) and threatening to defund federal-state social programs if states do not share personal information (as in the SNAP example). As a result of the breakdown of integrated federalism, the anti-commandeering concept is more important than ever. There is also an urgent need to develop it for the information age in which we live.

In particular, the Supreme Court has never ruled that its anti-commandeering jurisprudence applies to personal data. In *Printz*, Justice Scalia for the majority explicitly declined to answer this question. *Printz* conceded the existence of "a number of federal statutes enacted within the past few decades that require the participation of state or local officials in implementing federal regulatory schemes."[149] The majority opinion added that some of these regulatory programs "require only the provision of infor-

144 Aziz Z. Huq & Zachary D. Clopton, *Agonistic Federalism*, 104 TEX. L. REV. (forthcoming 2026) (manuscript at 14) (available at https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2420&context=public_law_and_legal_theory) [https://perma.cc/JP28-3LDS].

145 *Id.* at 15.

146 *Id.* at 21.

147 *Id.* at 22–24.

148 *Id.* at 24.

149 Printz v. United States, 521 U.S. 898, 917 (1997).

mation to the Federal Government."[150] These programs also did not "involve the precise issue before" the *Printz* Court, which was "the forced participation of the States' executive in the actual administration of a federal program."[151] Thus, *Printz* explicitly reserved for another day the question of whether anti-commandeering protections extended to personal information.[152]

Subsequent to *Printz,* the Supreme Court rejected a state challenge to a federal data privacy statute. In *Reno v. Condon*, the unanimous Court upheld the DPPA as a proper exercise of Congress' authority to regulate interstate commerce under the Commerce Clause.[153] The *Reno* Court noted the DPPA's wide reach. It declared, "[t]he DPPA regulates the universe of entities that participate as suppliers to the market for motor vehicle information—the States as initial suppliers of the information in interstate commerce and private resellers or redisclosers of that information in commerce."[154] In an opinion by Chief Justice William Rehnquist, the *Reno* Court concluded, "Because drivers' information is, in this context, an article of commerce, its sale or release into the interstate stream of business is sufficient to support congressional regulation."[155]

As for the idea of anti-commandeering, the *Reno* Court dismissed any similarities with *Printz* or its earlier federalism decision in *New York v. United States*. In these opinions, the Court was concerned with Congress taking over the state legislative process, or "conscripting the States' officers directly."[156] The *Reno* Court conceded that "the DPPA's provisions will require time and effort on the part of state employees."[157] But this federal law did not require "the States in their sovereign capacity to regulate their own citizens."[158] It also did not require the enactment of any

150 *Id.* at 918.

151 *Id.*

152 Two other Justices in *Printz* addressed the relationship between personal data and federalism. In her concurrence, Justice Sandra Day O'Connor approved of the Court's choice to refrain from deciding whether "purely ministerial reporting requirements imposed by Congress on state and local authorities" were invalid. *Id.* at 936 (O'Connor, J., concurring). In contrast, Justice John Paul Stevens in dissent argued that the anti-commandeering principle did not apply to personal data. He stated, "The enactment of statutes that merely involve the gathering of information . . . do not raise even arguable separation-of-powers concerns." *Id.* at 960 n.22 (Stevens, J., dissenting).

153 528 U.S. 141, 143 (2000); U.S. CONST., art. I, § 8, cl. 3.

154 *Reno*, 528 U.S. at 151.

155 *Id.* at 148.

156 *Id.* at 149 (quoting *Printz*, 521 U.S. at 935).

157 *Id.* at 150.

158 *Id.* at 151.

state laws or draw on "state officials to assist in the enforcement of federal statutes regulating private individuals."[159]

Data Privacy Federalism 3.0 is concerned with a different policy issue than *Reno*. The policy issue in *Reno* concerned a federal legislative approach where the states maintained the personal information in question. Records from the Department of Motor Vehicles were and are the province of state agencies that license motor vehicles.[160] The policy controversy in Data Federalism 3.0 involves federal use of state data for new purposes and without legislative authority or state agreement. In German, the pithy term for this general kind of action is "*Zweckentfremdung*," or "purpose alienation," and it is the source of much scholarly analysis in that country's data protection treatises.[161]

In the United States, a new debate has just started on this concept in the context of actions taken by the Trump administration over federal-state data resources. This federal behavior is not, however, without precedent. The Center for Democracy & Technology identifies federal efforts to access sensitive data as beginning "[u]nder the George W. Bush administration and continuing through much of the Obama administration."[162] This think tank notes that such behavior has "accelerated over the last decade" and faced "significant legal pushback from a bipartisan group of states and fierce opposition from the civil rights and pro-democracy communities."[163]

Considering the renewed attempts during the second Trump administration to pressure states to surrender personal data to it, we are fortunate that Professor Fahey has begun the process of analyzing how anti-commandeering should apply to personal data. Already in 2022, she provided a ringing endorsement for its application to data privacy federalism. She writes, "As data moves

---

159 *Id.*

160 Like HIPAA, moreover, the DPPA permits state laws that are more protective and do not conflict with it. The DPPA only sets out "permissible uses," 18 U.S.C. § 2721(b), but does not prohibit states from enacting stronger disclosure requirements.

161 *See* Alexander Roßnagel, DATENSCHUTZRECHT: DSGVO MIT BDSG [DATA PROTECTION LAW: GDPR WITH BDSG] art. 6, ¶ 4 (1st ed. 2019) (Ger.); Tobias Herbst, *Zweckbindung* [*Purpose Limitation*], *in* DATENSCHUTZ-GRUNDVERORDNUNG/BDSG KOMMENTAR [GENERAL DATA PROTECTION REGULATION/BDSG COMMENTARY] 274–86 (Jürgen Kühling & Benedikt Buchner eds. 2024) (Ger.).

162 CTR. FOR DEMOCRACY & TECH., FEDERAL EFFORTS TO EXPAND ACCESS TO DATA FROM STATE-RUN PROGRAMS AND INDIVIDUAL PRIVACY 3 (July 23, 2025), https://cdt.org/wp-content/uploads/2025/07/Federal-Efforts-to-Expand-Access-to-Data-from-State-Run-Programs-and-Individual-Privacy-FINAL.pdf [https://perma.cc/8EAQ-V7ZQ].

163 *Id.*

across governmental boundaries, it remains connected to the individual who originated it and the government that collected it."[164] Fahey argues that governments "retain an interest in safeguarding their data as it is put to use by their sister governments."[165]

Like Fahey, I believe that anti-commandeering principles apply to personal data. As Huq and Clopton warn, "the national government is engaging in a form of asymmetrical assault on the states through a no-holds-bar reneging on what had seemed an enduring and enabling intergovernmental bargain."[166] Federalism offers a vitally important constitutional bulwark for resistance to these actions. Professor Jennifer Urban, my colleague at Berkeley Law and Chairperson of the California Privacy Protection Agency, has pointed in this regard to two important tasks for the states.[167] Their first role is to "buttress their privacy laws to protect their people's data and vigorously enforce those laws."[168] In addition, Professor Urban calls for the states to "vigorously oppose any attempts by Congress to preempt their protections."[169] The result will be to create a "privacy immune system" for the United States.[170] At this juncture, Federalism 2.0 (anti-commandeering) meets Federalism 1.0 (preemption).

There is also a complication here. As noted above, privacy advocates should not view ever-increasing deference to state privacy regulation as invariably serving their policy preferences. Professor Bulman-Pozen wisely reminds us that the meaning of federalism has long been a historically contingent matter.[171] Independent of prior normative commitments, one should be skeptical of any theory of federalism as a "one-way ratchet" that will always favor the states. In their approaches to data privacy issues, the states will not invariably reflect a narrow Democratic or Republican perspective. Hence, there is also potential here for bipartisan cooperation among blue and red states. At the same time, however, some state activity simply will "flesh out nationwide controversies" at the state level.[172]

---

164 Fahey, *supra* note 4, at 1073.

165 *Id.*

166 Huq & Clopton, *supra* note 144, at 27.

167 Jennifer M. Urban, *Governing Data: The Role of State Privacy Law*, 28 YALE J.L. & TECH. 1, 35–36 (2026).

168 *Id.* at 36.

169 *Id.*

170 *Id.* (emphasis removed).

171 *See* Jessica Bulman-Pozen, *Partisan Federalism*, 127 HARV. L. REV. 1077, 1098–1100 (2014).

172 Bulman-Pozen, *supra* note 8, at 1946.

Where does anti-commandeering fit in as part of this evolving landscape? As *Printz* emphasizes, the states are independent, sovereign entities in the US.[173] Professor Fahey has demonstrated how much federal-state data sharing occurs through "intergovernmental agreements" rather than formal legislation.[174] These agreements exist in a "kind of interstitial space between and across governments."[175] Current behavior by the Trump administration unilaterally changes the terms of past bargaining and eviscerates their democratic legitimacy. Instead of honoring the terms of past intergovernmental agreements, the Trump administration has been adopting a policy of "grab-and-go" concerning personal data.

This conduct represents a problematic commandeering of resources in which the states retain an interest. As *Printz* also stresses, federalism serves an important role in protecting citizens from arbitrary or excessive government action.[176] Indeed, Judge Chhabria in his initial injunction in the Medicaid data litigation objected to the HHS action as "arbitrary and capricious" under the Administrative Procedure Act.[177] In *New York v. United States*, an anti-commandeering case that preceded *Printz*, the Court stated, "the Constitution divides authority between federal and state governments for the protection of individuals."[178] Anti-commandeering principles should be used as part of the opposition by the states to the Trump administration's seizures of personal data.

Finally, there are actions that the states can take regarding the federal data grab. Consider the executive order that Governor Jay Pritzker of Illinois issued in May 2025, to protect the privacy of Illinois residents with autism.[179] The order prohibits state agencies from disclosing autism-related data to the federal government unless there is individual consent or it is legally re-

173 *See* Printz v. United States, 521 U.S. 898, 919–20 (1997).

174 Fahey, *supra* note 4, at 1014.

175 *Id.*

176 *Printz*, 521 U.S. at 921.

177 Order Granting in Part and Denying in Part Motion for Preliminary Injunction at *3, California v. U.S. Dep't of Health & Hum. Servs., No. 25-cv-05536-VC, 2025 WL 3751931 (N.D. Cal. Dec. 29, 2025).

178 505 U.S. 144, 181 (1992).

179 GOVERNOR OF ILL., EXECUTIVE ORDER 2025-02: EXECUTIVE ORDER TO PROTECT THE CIVIL RIGHTS, HUMAN RIGHTS, AND PRIVACY OF AUTISTIC PEOPLE IN ILLINOIS (2025), https://www.illinois.gov/government/executive-orders/executive-order.executive-order-number-02.2025.html [https://perma.cc/CQH2-H8TJ].

quired.[180] Moreover, disclosures are to be limited to the minimum amount of information and anonymized where allowed and practicable. This action was taken in response to the stated plan of HHS Secretary Robert F. Kennedy, Jr. to create a national autism database. As this example indicates, the states are not without tools to protect their residents within the intergovernmental data market.

V. CONCLUSION

A new federalism era for information has begun, that of Data Privacy Federalism 3.0. This epoch is marked by a combination of federal legislative inactivity and an avalanche of state privacy legislation. These developments make the topic of preemption more important than ever. In response, this Article has advocated for continuing state lawmaking.

From a federalism perspective, the first benefit of this activity will be the states having an opportunity to act as laboratories for policy innovation. Beyond this classic argument for federalism, a second advantage will be to create opportunities for bipartisan policymaking at the state level. Due to today's polarized environment, these avenues for cooperation are especially important. At the same time, there are limits to the state role for data privacy. On the horizon may be the question of whether potential state attempts to regulate the data activities of international companies interfere with a more appropriate exclusively federal role in this area.

A further aspect of the new federalism age for information is the importance of the anti-commandeering doctrine for data privacy. It is long established that neither Congress nor the executive branch can command the states in certain ways. Whether this anti-commandeering applies to personal information is an open question. An aspect of data federalism making headlines today concerns federal agencies making unilateral decisions about personal information collected as part of joint federal-state programs. An anti-commandeering principle should apply to these actions and form an essential part of data privacy federalism today.

---

180 *Id.*; *see* Press Release, JB Pritzker, Off. of Governor, Gov. Pritzker Issues Executive Order to Safeguard Rights of Autistic Illinoisans (May 7, 2025), https://gov-pritzker-newsroom.prezly.com/gov-pritzker-issues-executive-order-to-safeguard-rights-of-autistic-illinoisans [https://perma.cc/3N6K-6FPZ].