RESEARCH PAPER: FEDERALISM AND THE REGULATION OF EMERGING TECHNOLOGY

SUBMITTED BY

FARHEENA NAWAB

COURSE: L.L.M(IP)

YEAR: 2025-2026

ENROLLMENT NO: A03104425012

INSTITUTION: AMITY LAW SCHOOL, NOIDA

COURSE CODE: LAW(646)

UNDER THE SUPERVISION OF

MS. BHAVNA BATRA

ASSISTANT PROFRSSOR

FEDERALISM AND THE REGULATION OF EMERGING TECHNOLOGY

Abstract

Traditional methods of governance are facing significant difficulties as a result of the rapid development of emerging technologies including artificial intelligence (AI), autonomous vehicles (AVs), digital platforms, and advanced data analytics. Because of the constitutional federalism that separates the powers of the federal and state governments in the United States, regulating technology has become a challenging task that requires striking a balance between safety, innovation, and democratic accountability. This article uses case studies of data privacy, artificial intelligence, autonomous vehicles, and broadband infrastructure to explore how the federal structure simultaneously facilitates and limits effective technological regulation.

Federalism offers a special dual style of government that permits experimentation through state initiatives while maintaining the federal ability to maintain national uniformity when needed. In the absence of comprehensive federal regulations, states have arisen as "laboratories of democracy," spearheading early initiatives to govern AI and digital privacy. State-level AI governance frameworks, such as California's Consumer Privacy Act (CCPA), serve as examples of proactive local policymaking that has impacted national discourse. But the spread of disparate state laws has also resulted in a patchwork of requirements for businesses that operate across state lines, raising the expense of compliance and stifling innovation.

Through sector-specific guidance, rulemaking, and the pre-emption of conflicting state laws, federal agencies like the Federal Communications Commission (FCC), National Highway Traffic Safety Administration (NHTSA), and Federal Trade Commission (FTC) have tried to close regulatory gaps. However, these initiatives frequently run into limited statutory authority, political deadlock, and jurisdictional issues. The interaction between federal inertia and state dynamism highlights the advantages and disadvantages of the US federal

government in managing quickly changing technologies.

The study makes the case for a fair and reasonable approach to "cooperative federalism" in technology policy, one that permits states to innovate outside of clearly defined federal baseline criteria for fundamental public values like safety, openness, and privacy. Interstate regulatory compacts, adaptive rulemaking, and explicit pre-emption provisions can reduce fragmentation without impeding state innovation. The study comes to the conclusion that, with the right coordination, federalism can be an asset rather than a liability for efficient technology governance. In the era of developing technologies, the United States may establish a regulatory environment that fosters innovation and the defence of fundamental rights by striking a balance between national coherence and localized responsiveness.

KEYWORD- Federalism, Technology Governance, Artificial Intelligence Regulation, Data Privacy, Cooperative Federalism, Emerging Technologies, United States.

Introduction

Innovation in technology has emerged as the 21st century's distinguishing characteristic. At a rate never seen in earlier industrial revolutions, emerging technologies like blockchain, biotechnology, autonomous vehicles (AVs), artificial intelligence (AI), and powerful data analytics are revolutionizing economies, governance, and daily life. These advancements present enormous potential for advancement, but they also bring up difficult issues of accountability, ethics, privacy, and security.[1] Since the federal and state governments in the United States are legally separated, federalism has a particular influence on how such rapidly changing technology are regulated. At the core of the contemporary governance dilemma is deciding which level of government should regulate a particular technology and to what degree.

Federalism is intended to promote policy experimentation and prevent dictatorship by distributing power. States are frequently referred to as "laboratories of democracy," able to test novel policies that could eventually influence national norms and customize solutions to

[1] Knight Brian R., *Federalism and Federalization on the Fintech Frontier*, 20 *Vanderbilt Journal of Entertainment & Technology Law* 129 (2020).

meet local demands. Contrarily, the federal government offers consistency, coherence, and the power to control issues that cut across state lines, such national security and interstate trade. Although this framework encourages flexibility and pluralism, it also creates conflict when technology function flawlessly across national boundaries. Purely local legislation is useless since data gathered in one state may be processed in another and kept in a third. Similar to this, digital platforms and driverless cars operate within national networks that transcend conventional jurisdictional borders.[2]

States have increasingly filled the regulatory gap in the absence of comprehensive federal legislation. New standards for data privacy and consumer rights have been set by state legislation such as *Virginia's Consumer Data Protection Act (CDPA)*[3], *California's Consumer Privacy Act (CCPA)*[4], and others. Similarly, a number of jurisdictions have launched pilot programs for testing autonomous vehicles, legislation requiring accountability for AI, and prohibitions on face recognition. These programs highlight the need of state innovation while also highlighting the dangers of a disjointed legal system. Businesses that operate in several states must deal with varying responsibilities, and residents are subject to different protections based on where they reside.

On the other hand, the federal government frequently faces charges of industry capture or regulatory overreach when it tries to exercise preemptive authority through organizations like the *National Highway Traffic Safety Administration (NHTSA)*[5], the *Federal Communications Commission (FCC)*[6], or the *Federal Trade Commission (FTC)*[7]. Thus, the argument over centralizing or decentralizing technology regulation raises more fundamental issues regarding democratic legitimacy, effectiveness, and flexibility in a world that is changing quickly.

This study examines these tensions by examining the disputes that emerge between federal and state actors, the distribution of regulatory authority over developing technologies within the U.S. federal government, and possible frameworks for striking a balance.[8] The study demonstrates the dynamic interaction between innovation and regulation in a federal setting

[2] Bowles Rice LLP (Roger Hanshaw), *Pre-emption, Federalism, and the Regulation of Emerging Technologies*, American Bar Association – Section of Environment, Energy, and Resources (2025).
[3] Va. Code tit. 59.1, ch. 53, §§ 59.1-575 - 59.1-585 (2021) (eff. Jan. 1, 2023).
[4] Cal. Civ. Code § 1798.100 et seq. (West 2018 & Supp. 2025).
[5] 49 U.S.C. § 105 (Pub. L. 97-449, Jan. 12, 1983) (codifying establishment of NHTSA within the Department of Transportation).
[6] 47 U.S.C. § 154 (establishing the Federal Communications Commission under the Communications Act of 1934, as amended).
[7] 15 U.S.C. § 41 (establishing the Federal Trade Commission).
[8] Narechania Tejas N. & Stallman Erik, *Internet Federalism*, 34 *Harv. J.L. & Tech.* 548 (2021).

using case studies of data privacy, AI governance, autonomous cars, and broadband regulation.[9] In the end, it makes the case for a cooperative governance approach that maintains state autonomy to innovate while establishing federal baseline protections. Such an approach can ensure that the United States remains both technologically progressive and grounded in its constitutional commitment to shared power and accountability.

I. Federalism and Technology Regulation: Concepts and Doctrinal Tools

1. Federalism's normative and functional trade-offs

Federalism supplies benefits policy experimentation, localization to fit differing preferences, competition that can check centralized power but also costs: uneven protection of rights, regulatory complexity for national markets, and legal conflicts (preemption). Because technology is both national/international (data flows, interstate commerce, platform marketplaces) and local (zoning for telecom towers, municipal facial recognition prohibitions), regulation of technology exacerbates these trade-offs.[10] Utilizing federalism's experimental advantage while preventing detrimental fragmentation is the governance dilemma.

2. Doctrinal tools: pre-emption, delegation, and agency authority

Federal-state relations are governed by three legal mechanisms: (1) cooperative federalism federal frameworks that establish baselines while allowing for state variation; (2) delegation and agency rulemaking federal agencies (FCC, NHTSA, FTC, EPA, etc.) can develop sectorial rules that may pre-empt conflicting state rules; and (3) pre-emption under express, implied, or field pre-emption doctrines, federal law can prohibit state regulation. Federal pre-emption of state regulations is more common in cases where agencies have explicit statutory power; in cases where federal law is lacking, states frequently fill in the blanks.[11] Therefore, a combination of statutes, agency posture, and case outcomes determine the regulatory competence division in tech sectors.

[9] *Sarah E. Light*, "Federalism and the Regulation of Emerging Technology" (2023) 45 *Harvard Journal on Legislation* 201.
[10] *Carnegie Endowment for International Peace*, *Federalism and the Regulation of Emerging Technology* (Carnegie Endowment, 2023).
[11] Brian Knight, *Federalism and Federalization on the Fintech Frontier*, 20 *Vanderbilt Journal of Entertainment & Technology Law* 129 (2020).

II. Background of Literature and Policy (Selected Scholarship & Trackers)

Researchers and policy groups note that states are actively involved in a variety of tech-related areas, including local prohibitions on surveillance technology, AI governance legislation, privacy laws (such as those in California, Virginia, and Colorado), and AV statutes. According to data, in situations where Congress or federal agencies have been hesitant to act, states have acted as "regulators of first resort."[12] The FCC's attempts to pre-empt internet, the NHTSA's AV safety guidelines, and federal agency pronouncements on AI and data policies have all been active at the same time. Through 2024–2025, state legislative activity in privacy and AI is expected to accelerate, according to trackers kept up to date by IAPP, NCSL, Carnegie, and legal analytics firms. Both state policy innovation and the legal conflicts with federal actors are highlighted in these convergent literatures.[13]

III. Case Studies

1. Data privacy: state law proliferation vs. federal baseline need

States have passed a variety of data-protection and privacy laws during the past ten years (such as California's CCPA/CPRA, Virginia's CDPA, Colorado's CPA, and many more), resulting in a patchwork of regulations for companies doing business throughout the country. Around 20 states have comprehensive privacy laws in existence or soon to be implemented, according to trackers, while many more have sectorial or more specific rules as of the end of 2025. Although state laws offer valuable experimental opportunities, such as customized consent regimes, rights of access and deletion, and enforcement structures, they can result in uncertainty for interstate data flows and compliance costs for businesses. Calls for a nationwide baseline privacy law that harmonizes rights while preserving some state innovations have been sparked by this patchwork.[14]

Implications: A hybrid outcome is exemplified by the data privacy case: states take the lead and exert pressure on the federal government, but the lack of federal baseline requirements results in gaps (such as those pertaining to minors and employment data) and differing

[12] Carlos Ignacio Gutierrez Gaviria, *The Role of Artificial Intelligence in Pushing the Boundaries of U.S. Regulation: A Systematic Review*, 38 *Santa Clara High Tech. L.J.* 123 (2022).
[13] Tatevik Davtyan, *The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained*, 16 *Case W. Res. J.L. Tech. & Internet* 223 (2025).
[14] "The Future of AI Is in the States: The Case of Autonomous Vehicle Policies", Daniel J. Mallinson et al., *Business and Politics*, Vol. 26, Iss. 2, pp. 180-199 (2024).

protections among states. Concerns about litigation and interstate commerce also support some degree of federal harmonization.

2. Artificial Intelligence: state experiments and federal fragmentation

Federalism is finding a new front in the fight over AI control. From operational use limits in judicial systems to more comprehensive private-sector AI accountability regulations, states and state institutions (courts, agencies) have started implementing AI-related rules. For instance, courts and administrative bodies in New York, California, and other states have put in place temporary regulations on the use of generative AI in official roles, and numerous states have passed or are considering legislation and guidelines specifically related to AI. The U.S. trend toward decentralized, sector-specific regulation rather than a single harmonized statute is described by academic studies, and federal agencies and Congress have suggested sectorial alternatives. Both innovation and differing standards for AI system developers and users result from this interaction.[15]

Implications. AI serves as an example of the potential for detrimental divergence, such as disparate interpretations of "high-risk" uses, reporting requirements, or procurement regulations, which could obstruct interstate markets and make developer compliance more difficult. However, state experimentation can also reveal workable regulatory frameworks that guide federal policy.

3. Autonomous vehicles (AVs): safety, pre-emption, and certification authority

The interaction between state motor vehicle codes and the federal safety authority (NHTSA) is demonstrated by autonomous vehicle governance. With a patchwork of AV laws covering operation, insurance, licensing, and testing, states have taken the lead. Courts have acknowledged that state rules may be superseded when they clash with federal safety standards, and NHTSA creates guidance and safety policy at the federal level. Both local inventiveness and legal ambiguity about liability and performance criteria have resulted from the lack of a unified federal AV statute.[16]

[15] Srinivas Parinandi, Jesse Crosson, Kai Peterson & Sinan Nadarevic, *Investigating the Politics and Content of US State Artificial Intelligence Legislation*, *Business and Politics* (Mar. 2024).
[16] Bilyana Petkova, *The Safeguards of Privacy Federalism*, 20 *Lewis & Clark Law Review* 595 (2016).

Implications: Federal standards have a stronger pre-emption argument for technologies that prioritize physical safety and interstate movement; nonetheless, states continue to play significant roles in road construction, automobile registration, and tort law, necessitating cooperative federalism and explicit authority allocation.

4. Telecommunications, broadband, and 5G: FCC authority vs. state/municipal control

Broadband deployment and wireless infrastructure sit in a contested federal–state space. The FCC asserts authority over interstate communications and has litigated to preempt state laws that limit municipal broadband or restrict wireless siting. States regulate land use and municipal franchises, creating friction where federal broadband policy aims to promote deployment. The preemption doctrine here has been uneven in courts, and congressional clarity remains partial.[17]

Implications. Infrastructure-heavy technologies require coordination: land-use remains local, but spectrum and interstate service models are federal. Mismatches produce deployment delays or policy conflict.[18]

IV. Analysis: Patterns of Conflict and Complementarity

When federalism and technology innovation are combined, a complex web of rivalry, collaboration, and conflict across regulatory entities is revealed. Digital infrastructure, autonomous systems, data analytics, and artificial intelligence are examples of emerging technologies that transcend national and regional borders. However, power is purposefully divided between the national and subnational levels in the US constitutional framework. Tension and constructive dynamism are both results of this authority dispersal. State initiative, federal necessity, legal unpredictability, and political economy are four interconnected characteristics that shed light on the systemic logic by which American federalism mediates technological development and help us comprehend the evolving equilibrium.

1. Why States Move First

[17] Bridget Fahey, *Data Federalism*, *Public Law & Legal Theory Working Paper* (2022).
[18] Ani B. Satz, *The Federalism Challenges of Protecting Medical Privacy in Workers' Compensation*, Emory University School of Law (2019).

State governments have been the first to respond in many developing technology fields. This phenomena is driven by three factors: policy experimentation, regulatory gap-filling, and political responsiveness. When combined, they provide an explanation for why subnational governments frequently take action before federal institutions create all-encompassing frameworks.[19]

Political responsiveness remains a defining feature of state initiative. State governments are closer to their constituencies, making them more sensitive to immediate public concerns about privacy, safety, or fairness. For instance, when facial-recognition technologies began proliferating across law-enforcement agencies without clear oversight, several cities and states such as San Francisco, Massachusetts, and Maine imposed moratoria or outright bans on their use (Carnegie Endowment for International Peace, 2024).[20] Similarly, state courts and bar associations have adopted their own rules governing the use of AI in judicial filings, ensuring transparency and accountability in the administration of justice. These actions reflected not merely legal necessity but democratic responsiveness; local publics demanded restraint and protection in the face of opaque technologies. The decentralized nature of federalism thus ensures that regulation can emerge even when national consensus lags.

A second driver is **regulatory gap-filling**. Where Congress or federal agencies act slowly, states step in to address perceived governance voids. Due to politics and procedural inertia, the federal legislative process frequently finds it difficult to keep up with technological advancements. Therefore, without comprehensive federal legislation, states have stepped up to enforce cyber security, privacy, and AI accountability standards. One landmark example is the 2018 California Consumer Privacy Act (CCPA), which effectively established a de facto nationwide standard and filled the void left by congressional inactivity. Similar laws were then passed by other states, such as Virginia, Colorado, and Connecticut, illustrating the domino impact of subnational leadership. In this way, state regulation frequently serves as a trigger as well as a remedy, pressing Congress to take action while temporarily replacing the lack of federal control.

Third, states experiment with their policies. States are "laboratories of democracy," as Justice Louis Brandeis memorably noted. This experimental characteristic is especially useful in

[19] "Why States and Localities Are Acting on AI", Nicol Turner Lee & Obioha Chijioke, Brookings Institution (Dec. 15, 2023).
[20] U.S. Artificial Intelligence Regulation During the Biden Administration, Christopher S. Yoo & Alexander Mueller, 17 *J. L. Econ. Regul.* 7 (2024).

fields that are known for their quick innovation and uncertainty. States produce empirical evidence regarding the effectiveness of regulations by evaluating different strategies, such as algorithmic auditing standards, AI procurement criteria, or autonomous-vehicle safety protocols. For example, Arizona and California took different approaches to testing autonomous vehicles: California mandated strict safety reporting, whereas Arizona focused on deregulation to draw in business investment. These studies' comparative results guide later federal discussions, enabling national politicians to adjust uniform regulations based on observed successes and failures. The ability of American federalism to adapt through subnational experimentation is highlighted by this dynamic.[21]

These three forces work together to explain why nations frequently move first. Institutional plurality permits experimentation to come before harmonization; structural gaps force them to act in the absence of national policy; and political proximity enables them to react quickly. However, state leadership cannot take the place of federal action. Certain structural aspects of the contemporary technological economy necessitate standardization and coordination, which can only be supplied by federal institutions, as the next section demonstrates.

2. Where Federal Action Is Necessary or Preferable

There are areas where federal assistance is essential, even while state initiative produces valuable innovation. In issues pertaining to international affairs, national security, and interstate commerce, the Constitution itself establishes federal priority. By their very nature, emerging technologies include transnational externalities and network effects that make strictly local control insufficient.[22]

Network interconnection and interstate commerce provide a major justification for federal leadership. Because AI models, data brokers, and digital platforms operate beyond state lines, fragmented state regulations are ineffective and expensive. The burden of complying with various privacy laws or algorithmic-accountability frameworks increases exponentially as the number of jurisdictions increases. Without knowing which rules apply in cross-border transactions, businesses must negotiate a maze of responsibilities, from notification requirements in California to opt-out options in Virginia. In addition to impeding innovation,

[21] Adaptive Legal Frameworks and Economic Dynamics in Emerging Technologies: Navigating the Intersection for Responsible Innovation, Lescrauwaet, Wagner, Yoon & Shukla, *Law & Economics*, Vol. 16, No. 3 (2022).
[22] Global AI Governance Law and Policy: US, Antony Hilton, C. Kibby & Richard Sentinella, IAPP Resource Center (Sept. 2025).

this regulatory fragmentation compromises consumer protection by resulting in inconsistent enforcement. By offering consistent guidelines and permitting states to strengthen national safeguards without compromising them, a federal baseline can ease these conflicts. The allocation of essential resources and national security constitute a second justification. Defence, intelligence, and economic competitiveness all depend on technologies like 5G, cloud computing, and artificial intelligence.[23] Their governance touches on areas that are constitutionally within the purview of the federal government, such as supply chain security, cyber resilience, and foreign policy. Radio frequencies, for instance, are essentially interstate and global in character, making it impossible for fifty different state regimes to effectively regulate spectrum allotment. To protect national interests, centralized supervision is also needed for export restrictions on sophisticated semiconductors and cross-border data flows. Federal primacy is not just desirable in these situations, but required by the constitution. Lastly, federal coordination is supported by consistent consumer protection. Federal legislation can provide certainty and public confidence when uneven state standards cause market distortion or consumer confusion. Organizations with the institutional capacity and technical know-how to create complex, evidence-based laws include the Federal Communications Commission (FCC), the Federal Trade Commission (FTC), and the National Highway Traffic Safety Administration (NHTSA). Smaller governmental entities would be unable to respond coherently to complex technological risks due to their centralization of specialized knowledge. In fact, Congress's acknowledgment that national uniformity is occasionally necessary for good government is reflected in its delegation of authority to these entities.[24]

Therefore, the size, interconnection, and security implications of the technological economy warrant federal leadership in important areas, even though federalism values decentralization. The question is not whether the federal government should take action, but rather how to make sure that its involvement enhances rather than replaces the beneficial roles that state experimentation and responsiveness play.

3. Legal Friction Points and Unpredictability

[23] Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US, Jon Chun, Christian Schroeder de Witt & Katherine Elkins, arXiv preprint (Oct. 2024).
[24] Local US Officials' Views on the Impacts and Governance of AI: Evidence from 2022 and 2023 Survey Waves, Sophia Hatz, Noemi Dreksler, Kevin Wei & Baobao Zhang, arXiv (2025).

There will always be legal conflict where multiple authority coexist. One of the defining characteristics of technology governance is pre-emption litigation, which involves disagreements over whether federal law supersedes state regulation. Courts are frequently asked to decide whether a federal act "occupies the field," contradicts state goals, or only establishes a minimal requirement. However, judicial results are often unpredictable due to the fragmented character of federal legislation in emerging-technology fields.[25]

Pre-emption jurisprudence is intricate and situation-specific. For instance, the lack of a comprehensive federal statute in the area of data privacy raises the question of whether sector-specific rules, such as the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act, implicitly supersede more general state restrictions. Inconsistent precedents result from courts' differing interpretations of congressional purpose. Similar to this, state testing and licensing requirements for autonomous vehicles may conflict with NHTSA safety rules, leading industry participants to argue that state restrictions impede interstate commerce.

The costs of this legal ambiguity are high. Legal duties that differ or overlap present a compliance challenge for businesses that operate in several states. By 2025, there will be over 20 different state privacy regulations, forcing businesses to implement disjointed compliance architectures that raise administrative costs and the possibility of unintentional violation. Uncertain about potential legal action or changes to regulations, innovators may postpone product introductions or completely leave some areas. Paradoxically, the uncertainty that results might stifle the very innovation that flexible federalism is supposed to promote.

Pre-emption litigation also reveals underlying institutional problems, such as the judiciary's difficulty establishing boundaries in fields that are undergoing rapid technological change. Courts, frequently lacking technical competence, must interpret statutes that date back decades through the prism of new technologies. The ensuing patchwork of decisions increases ambiguity and points to the necessity of interagency cooperation and congressional clarification to lessen interpretation discrepancy.[26]

[25] One Bad NOFO? AI Governance in Federal Grantmaking, Dan Bateyko & Karen Levy, arXiv (2025).
[26] Shawn Marie Boyne, *Data Protection in the United States*, (2018) 66 *Am. J. Comp. L.* Suppl. 1, 299-343 — sectoral federal + state privacy frameworks.

4. Political Economy and Capture Risks

Another aspect of federalism's conflict and complementarity is brought about by the political economy of technology regulation: interest-group dynamics and regulatory capture. Both centralization and decentralization have unique weaknesses and opposing benefits.[27]

Concentrating power in a small number of federal agencies can make it easier for large national corporations to seize control. Giants in the technology industry have the means, connections, and lobbying power to sway rulemaking through advisory panels, revolving-door employment, and consultations. Thus, centralized policymaking may put incumbents' interests ahead of those of customers or smaller rivals. Federal preemption opponents frequently caution that standardized national norms may become stale due to corporate influence, impeding the development of more robust state-level safeguards.[28]

On the other hand, local capture may also affect state-level regulation. Regional businesses may have a disproportionate impact on state legislators looking to entice investment, such as Californian tech companies or Arizona's concentration of autonomous car manufacturers. This risk is lessened, though, by the competitive federalism dynamic, which allows states to implement stronger regulations in response to industry pressure, thereby fostering economic or reputational incentives for balance. A self-correcting component that is lacking in centralized regimes is introduced by this inter jurisdictional competition.

Additionally, policy pluralism is strengthened by political diversity among states. Different political cultures libertarian in Texas, pragmatic in Illinois, and progressive in California produce a range of viewpoints that, when combined, enhance national discourse. Successful state models have the potential to influence federal law over time. Thus, the iterative relationship between the federal and state levels prevents any one actor from controlling the regulatory agenda, acting as a safeguard against capture.[29]

All things considered, the political economics of federalism in the governance of developing technologies is conflicted: centralization encourages uniformity but runs the risk of capturing ideas, while decentralization fosters diversity and experimentation but runs the risk of

[27] Denise DiPersio, "Data Protection, Privacy and US Regulation", *Proc. ACL Anthology* (2022) — examines ongoing bills and multi-level regulation.
[28] Amol Khanna, Adam McCormick, Andre Nguyen, Chris Aguirre & Edward Raff, *Position: Challenges and Opportunities for Differential Privacy in the U.S. Federal Government*, *arXiv* (2024) — federal capability vs privacy framework tensions.
[29] "Layered, Overlapping, and Inconsistent: A Large-Scale Analysis of the Multiple Privacy Policies and Controls of U.S. Banks", Lu Xian et al., *arXiv preprint* (2025) — shows inconsistencies due to state & federal regulation overlap.

incoherence. The best balance is achieved through organized complementarity, in which states are free to innovate and challenge federal organizations that establish standards and coordinate enforcement.

V. Governance Options: A Framework for Coordinated Federalism in Tech

1. Federal minimum baselines , room for state augmentation

Congress should adopt technology-neutral baseline statutes for core public interests (privacy baseline, safety norms, transparency obligations for AI in critical contexts) that set minimum protections while allowing states to strengthen protections so long as they do not unduly burden interstate commerce or conflict with federal safety standards.

Rationale: Baselines reduce fragmentation costs while preserving state laboratories for higher protections or localized responses.[30]

2. Explicit pre-emption rules and narrow field pre-emption

When Congress delegates authority, statutes should clarify pre-emption scope—expressly foreclosing or permitting state rules in specified domains. Narrow field pre-emption should be used sparingly and only where national uniformity is indispensable (e.g., motor vehicle safety performance standards where federal tests apply).

3. Regulatory sandboxes and interstate compacts

Federal support for state-led sandboxes (regulatory test beds) and encouragement of interstate compacts can scale promising state innovations and reduce duplicative compliance burdens. The federal government can fund and coordinate multi-state regulatory experiments to assess trade-offs and outcomes.[31]

4. Agency–state coordination mechanisms

Federal agencies should institutionalize regular coordination with state regulators (memoranda of understanding, joint guidance, technical assistance). This reduces regulatory

[30] Zihao Li, *Regulating Online Algorithmic Pricing: A Comparative Study of Privacy and Data Protection Laws in the EU and US*, *arXiv preprint* (2025) — comparative perspective that highlights fragmentation in US regulation.
[31] Marcelo Corrales Compagnucci, *The EU-US Data Privacy Framework: Is the Dragon Eating its Own Tail?*, *arXiv preprint* (2024) — international transfers + how US state / federal roles matter.

surprises and fosters common data standards. Where agencies have technical role (e.g., FCC spectrum), they should provide model rules for state-level implementation.

5. Procedural safeguards and transparency for fast-moving tech

Because technologies evolve rapidly, rulemaking should prioritize adaptive, evidence-driven mechanisms: sunset provisions, periodic review, requirement for impact assessments, and mandated data sharing (with privacy protections) so policymakers can learn quickly about consequences.[32]

VI. Applying the Framework: Policy Recommendations by Domain

A. Data Privacy and AI-Related Data Practices

The rapid diffusion of digital platforms, artificial intelligence, and data-driven services has magnified the inadequacies of the United States' fragmented data-protection regime. In the absence of a comprehensive federal privacy statute, states have stepped in to fill the vacuum. California's Consumer Privacy Act (CCPA) and its later amendment, the California Privacy Rights Act (CPRA), introduced a model of consumer rights—including access, deletion, and opt-out mechanisms that several states such as Virginia, Colorado, and Utah have emulated (International Association of Privacy Professionals [IAPP], 2025). While this proliferation demonstrates the experimental virtue of federalism, it has simultaneously created a "patchwork problem" for national and multinational firms that must tailor compliance programs to multiple, often inconsistent, state laws. Consumers are likewise disadvantaged by the variability of rights across jurisdictions.[33]

A federal baseline privacy statute is therefore imperative. Such legislation should articulate minimum national standards for personal-data collection, processing, and protection while explicitly preserving states' ability to legislate stronger safeguards. By setting a uniform floor, Congress would reduce administrative complexity and ensure that every citizen enjoys a core level of privacy protection regardless of residence. The federal baseline should codify key consumer rights access, correction, deletion, and portability and mandate timely breach

[32] Robert D. Williams, "To enhance data security, federal privacy legislation is just a start", *Brookings Instit. Commentary* (Dec. 1, 2020) — arguing for federal baseline protections alongside state innovations.
[33] "The Future of AI Is in the States: The Case of Autonomous Vehicle Policies", Daniel J. Mallinson et al., *Business & Politics*, Vol. 26, No. 2, 2024, pp. 180-199 — state experiments with autonomous vehicle policy under federalism.

notifications and transparency regarding automated decision-making in high-risk contexts such as credit scoring and employment. Scholars have noted that "preemption by floor" rather than "pre-emption by ceiling" maintains the constitutional balance envisioned by cooperative federalism (Solve & Schwartz, 2023).[34]

Equally critical is the modernization of the Federal Trade Commission (FTC). The FTC has long served as the de facto national privacy regulator through its Section 5 authority over unfair or deceptive practices, yet its capacity to address algorithmic harms and systemic data misuse remains limited. Congress should expand the FTC's rulemaking powers, allocate technical expertise in artificial-intelligence auditing, and authorize civil-penalty authority for first-time violations. A technically equipped FTC could issue sector-specific guidance and coordinate with state attorneys general to ensure consistent enforcement. In this hybrid model, federal institutions provide coherence and resources, while states preserve the ability to innovate beyond the federal floor, thereby achieving both uniformity and dynamism in data-governance regimes.

B. Artificial Intelligence

Artificial intelligence regulation epitomizes the need for a multi-level, risk-based governance strategy. AI systems differ dramatically in function and potential harm from innocuous recommendation engines to predictive-policing algorithms that affect constitutional rights. Because a single, monolithic framework risks over- or under-regulating heterogeneous technologies, Congress should authorize federal agencies to develop sector-specific AI rules grounded in shared principles such as transparency, accountability, and human oversight (Reuters, 2025). For example, the Department of Housing and Urban Development could focus on algorithmic bias in housing eligibility, the Equal Employment Opportunity Commission on AI in hiring, and the Food and Drug Administration on medical-diagnostic algorithms.[35]

This sectorial follow-up model would mirror existing U.S. regulatory traditions while establishing consistency through cross-cutting principles. Federal coordination can occur via an inter-agency AI Council that issues overarching guidance, ensuring that terms like "high-risk AI" or "automated decision system" have consistent definitions across sectors. The

[34] "Legal Issues in Autonomous Vehicle Regulations", Michael Harris, *Frontiers of Law & Policy Research* (FLPR), Vol. 4, Issue 1 (2022) — identifies conflicts of jurisdictions, safety, ethics, etc.
[35] Sütfeld, L. R., Bronson, J. & Kirchmair, L., *Automated Vehicle Regulation Needs to Speak to Code, not to Humans: Keeping Safety and Ethics in the Public Domain*, *Philosophy & Technology* 38 (2025) Article 15 — focusing on how automated vehicle regulations must align ethical code and law.

absence of definitional clarity currently impedes compliance and enforcement, as states employ varying thresholds for risk classification.

States should nevertheless retain authority over public-sector AI applications and procurement. Several jurisdictions, including New York and California, have adopted rules requiring human oversight in judicial or administrative use of generative AI. Such localized regulation reflects democratic responsiveness to community concerns about fairness and accountability. Federal guidance can complement these measures by setting baseline disclosure and record-keeping obligations, while states can impose additional procedural safeguards.[36]

In implementing AI governance, the United States must also prioritize algorithmic transparency and impact assessment. Federal law should require organizations deploying high-risk AI to conduct algorithmic-impact assessments and publish summaries detailing data sources, model objectives, and mitigation strategies. The FTC, equipped with expanded expertise, could oversee compliance and issue penalties for deceptive representations of AI capabilities. This multi-layered system, in which federal agencies establish standards and states operationalize enforcement, would reconcile innovation incentives with constitutional commitments to equality and due process.

C. Autonomous Vehicles

Autonomous-vehicle (AV) technology illustrates the intersection of federal safety authority and state regulatory prerogatives. The National Highway Traffic Safety Administration (NHTSA) has jurisdiction over vehicle-performance standards, while states control licensing, registration, and road safety. Yet the rapid introduction of self-driving cars blurs these boundaries, generating uncertainty over liability, insurance, and operational standards. According to the U.S. Department of Transportation (2024), over twenty states have enacted AV testing or deployment statutes, most of which vary in safety-certification requirements and data-reporting obligations.[37]

A coherent approach requires the federal government to adopt performance-based safety standards for autonomous systems that emphasize measurable outcomes—such as collision-

[36] Cason Schmit, Theodoros Giannouchos, Mahin Ramezani, Qi Zheng, Michael A. Morrisey & Hye-Chung Kum, "US Privacy Laws Go Against Public Preferences and Impede Public Health and Research: Survey Study", *J. Med. Internet Res.* (2021) — shows mismatch between public expectation and regulatory structure.
[37] *The State of Data Privacy in the U.S.*, FORC Journal, Fall 2023, Vol. 34, Ed. 3 — summarizing how state laws fill gaps left by lack of comprehensive federal law.

avoidance effectiveness and sensor redundancy—rather than prescriptive design mandates. Such flexibility encourages technological innovation while maintaining consistent public-safety benchmarks nationwide. Where federal performance standards exist, Congress should include narrow, express pre-emption clauses to prevent conflicting state safety rules that might hinder interstate deployment, while explicitly preserving state authority over licensing, insurance, and tort law.

States, in turn, should integrate AV oversight into their broader transportation-safety frameworks by establishing certification programs, collecting operational-safety data, and coordinating with NHTSA on incident reporting. This layered governance structure promotes accountability without duplicative regulation. Moreover, NHTSA should collaborate with states to create shared data repositories for AV incident statistics and testing outcomes, thereby enhancing transparency and public trust. A cooperative approach balances national uniformity with local control over infrastructure and law-enforcement interaction, reflecting federalism's original spirit of shared competence.[38]

D. Broadband and 5G Deployment

Telecommunications infrastructure—particularly broadband and fifth-generation (5G) networks poses another arena of intense federal-state tension. The Federal Communications Commission (FCC) exercises broad authority over interstate communications, including spectrum allocation and broadband funding, while states and municipalities retain jurisdiction over land-use planning and rights-of-way. Litigation over the FCC's pre-emption of state restrictions on municipal broadband underscores the difficulty of reconciling national connectivity goals with local autonomy (Congress.gov, 2025).[39]

A sustainable strategy involves cooperative federal–local planning. The FCC should lead in setting nationwide spectrum policies, network-security standards, and interoperability requirements but must coordinate closely with state infrastructure agencies and municipal authorities regarding deployment logistics. Congress should clarify the statutory limits of federal preemption to avoid uncertainty that deters investment. Explicit legislative guidance

[38] Benjamin T. Seymour, *The New Fintech Federalism*, 24 *Yale J.L. & Tech.* 1 (2022) — experiments in fintech regulation by states vs federal preemption issues.
[39] Jeffrey J. Rachlinski & Andrew J. Wistrich, "Judging Autonomous Vehicles", 24 *Yale J.L. & Tech.* 706 (2022) — legal liability and how courts interpret state / federal roles when novel technologies are involved.

can distinguish between matters of interstate concern where federal uniformity is essential—and those of purely local impact, such as zoning for cell-tower placement.

Furthermore, Congress should expand federal funding mechanisms under programs like the Broadband Equity, Access, and Deployment (BEAD) initiative while granting states discretion to design context-specific implementation strategies. Federal oversight should ensure accountability and equitable access without micromanaging local planning. In effect, broadband policy must blend top-down coordination with bottom-up innovation, reflecting the mutual dependence of federal and state governments in building inclusive digital infrastructure.

Together, these domain-specific recommendations translate the theoretical framework of cooperative federalism into operational mechanisms that harmonize innovation with accountability. They demonstrate that technology governance, when informed by clear jurisdictional design and adaptive collaboration, can simultaneously advance economic growth, consumer protection, and democratic legitimacy.[40]

VII. Institutional Innovations and Democratic Legitimacy

Regulatory frameworks alone cannot sustain legitimacy in the face of rapid technological evolution; institutions must evolve as well. Federalism's vitality depends on continuous dialogue and mutual learning between federal and state actors. The following institutional innovations technical advisory councils, mandated impact-evaluation systems, and balanced enforcement architectures are essential to operationalizing cooperative federalism in emerging-technology governance.

1. Technical Advisory Councils with State Representation

Technological change often outpaces the capacity of existing bureaucracies to understand or regulate it. Establishing permanent technical advisory councils within key federal agencies can bridge this gap by embedding multidisciplinary expertise and ensuring state participation in national decision-making.[41] Each council should include representatives from state regulatory agencies, industry experts, civil-society organizations, and academic researchers.

[40] Brain Knight, *Federalism and Federalization on the Fintech Frontier*, 20 *Vanderbilt J. Ent. & Tech. L.* 129 (2020) — federal-state tensions, preemption in fintech.
[41] Tatevik Davtyan, *The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained*, 16 *Case W. Res. J.L. Tech. & Internet* 223 (2025).

Their role would be to advise Congress and federal regulators on the social, economic, and ethical implications of emerging technologies.

For instance, an AI and Algorithmic Accountability Council within the FTC could evaluate algorithmic-risk assessment methodologies and recommend standardized transparency metrics, while a Transportation Innovation Council within the Department of Transportation could review data from state AV pilots. Including state members institutionalizes federalism within the advisory process, ensuring that regional perspectives inform federal policy. Such councils would enhance epistemic legitimacy the perception that regulators possess adequate expertise—and foster iterative learning between levels of government.[42]

To avoid capture, councils should be subject to transparency obligations, public meeting requirements, and term limits for members. Funding should be partly shared between federal and state budgets, reinforcing mutual ownership. Over time, these councils could evolve into an intergovernmental epistemic network that sustains adaptive governance across multiple technological domains.

2. Mandated Impact Evaluations and Public Data

Effective governance of emerging technologies requires evidence, not conjecture. Both ex ante (before implementation) and ex post (after implementation) impact evaluations should be mandatory for major federal and state technology regulations. Such assessments would quantify expected social benefits, economic costs, and equity implications, while post-hoc reviews would measure real-world outcomes and unintended consequences.

For example, before adopting a nationwide AI-risk framework, agencies should conduct algorithmic-impact assessments to evaluate potential discrimination or data-bias risks. Similarly, privacy legislation should undergo cost-benefit analysis that considers compliance burdens relative to consumer-protection gains. Once policies are enacted, agencies must publish evaluation reports and underlying datasets, enabling scholars, journalists, and the public to scrutinize outcomes. Transparency of this kind builds democratic legitimacy and supports continuous improvement through empirical feedback.[43]

[42] Srinivas Parinandi, Jesse Crosson, Kai Peterson & Sinan Nadarevic, *Investigating the Politics and Content of US State Artificial Intelligence Legislation*, 26 *Business & Politics* 240 (2024).
[43] Jon Chun, Christian Schroeder de Witt & Katherine Elkins, *Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US* (arXiv preprint, Oct. 2024).

State governments play a crucial role in generating the data necessary for these evaluations. By requiring standardized reporting such as state-level AV incident data or AI-procurement outcomes—Congress can facilitate cross-jurisdictional learning.[44] An open, interoperable federal–state data platform would enable comparative analysis of regulatory effectiveness and highlight best practices. The iterative exchange of data and evaluation results turns federalism into a living learning system rather than a static allocation of authority.

3. Access to Justice and Enforcement Balance

Institutional legitimacy ultimately depends on the public's ability to seek remedies when technology-related harms occur. A balanced enforcement ecosystem must therefore allocate powers clearly among federal agencies, state attorneys general, and private litigants. Federal agencies should retain primary jurisdiction over interstate or systemic violations—such as national data breaches—while states handle localized enforcement and consumer-protection cases. Joint investigations between the FTC and state attorneys general could mirror existing environmental-law partnerships under the Clean Air Act's cooperative-federalism model.

Private rights of action present another delicate issue. Allowing individuals to sue for privacy or algorithmic violations enhances accountability but may produce excessive litigation that burdens innovation. A calibrated approach would permit private suits for willful or reckless misconduct while channelling ordinary disputes through administrative enforcement. Federal courts should retain jurisdiction over class actions involving multi-state harms to ensure consistency.[45]

Additionally, enforcement agencies must be equipped with adequate resources and technical expertise. Federal grants could support state enforcement offices in training and technology acquisition, ensuring parity of capacity. An independent Inspector for Technological Accountability, jointly appointed by Congress and the states, could audit enforcement practices and publish annual compliance reports. Such measures would strengthen procedural legitimacy, ensuring that citizens perceive the system as fair, accessible, and responsive.

Collectively, these institutional reforms embody a shift from hierarchical to networked governance. Rather than relying on unilateral federal action or fragmented state initiatives, the system would operate as a collaborative ecosystem of knowledge exchange, joint

[44] Dan Bateyko & Karen Levy, *One Bad NOFO? AI Governance in Federal Grantmaking* (arXiv preprint, 2025).
[45] Sophia Hatz, Noemi Dreksler, Kevin Wei & Baobao Zhang, *Local US Officials' Views on the Impacts and Governance of AI: Evidence from 2022 and 2023 Survey Waves* (arXiv preprint, 2025).

oversight, and shared accountability. Democratic legitimacy in technology regulation arises not merely from constitutional form but from procedural inclusivity, transparency, and continuous learning.[46]

VIII. Potential Objections and Responses

Objection 1: Federal baselines stifle state innovation.

Response: Baselines can be narrowly tailored to minimum protections; states can still innovate above that floor. Additionally, federal law can include sandbox mechanisms that elevate successful state policies.

Objection 2: Federal agencies are captured or too slow.

Response: Build transparency, stakeholder diversity, and procedural deadlines into delegation statutes; mandate regular review and anti-capture safeguards (e.g., revolving-door restrictions, disclosure requirements).[47]

Objection 3: Industry compliance costs will still be high under multiple regimes.

Response: The proposed model minimizes duplication by setting national floors, encouraging uniform reporting standards, and supporting interstate compacts—steps that reduce multi-state compliance burdens.

IX. Conclusion

The emergence of transformative technologies such as artificial intelligence (AI), autonomous vehicles (AVs), block chain, and data-driven platforms has redefined the boundaries of governance, law, and accountability. Within the United States' constitutional framework, federalism the division of authority between the national and state governments has become both an opportunity and a challenge for effective regulation.[48] This paper has demonstrated that while the federal system encourages innovation and responsiveness, it also produces jurisdictional conflicts, legal uncertainty, and regulatory fragmentation that

[46] Myrisha S. Lewis, *Innovating Federalism in the Life Sciences* (William & Mary Law School, 2023/24).
[47] Daniel A. Lyons, "Technology Convergence and Federalism: The Case of VoIP Regulation", 45 *U. Mich. J. L. Reform Caveat* 56 (2012).
[48] Jean Joseph, *Should the United States Adopt Federal Artificial Intelligence Regulation Similar to the European Union*, 20 *Loy. U. Chi. Int'l L. Rev.* 105 (2024).

complicate coherent policymaking. The key question is not whether the federal or state governments should regulate technology, but how they can do so together in a coordinated and balanced manner.

Federalism remains a double-edged sword in the digital era. On one hand, it empowers states to serve as "laboratories of democracy," enabling experimentation and swift responses to emerging technological risks. State initiatives in data privacy, algorithmic accountability, and digital safety have filled crucial policy gaps left by federal inaction. On the other hand, this decentralized approach can produce a patchwork of inconsistent rules that impede interstate commerce and create compliance burdens for businesses. The absence of harmonized standards for AI, data protection, or autonomous vehicle safety undermines both consumer protection and industrial growth.[49]

At the federal level, agencies such as the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), and the National Highway Traffic Safety Administration (NHTSA) have attempted to establish nationwide frameworks. Yet, their authority is often limited by out dated statutory mandates and political gridlock. The challenge lies in designing a governance structure that preserves the benefits of local flexibility while ensuring the predictability and coherence required for technologies that operate across state and national boundaries.[50]

The solution proposed in this paper a cooperative federalism model—offers a pragmatic middle path. Under this model, the federal government should establish baseline standards that protect fundamental rights and provide a uniform floor for consumer and data protection. States should retain the freedom to enact stricter or more innovative measures, provided these do not contradict federal objectives or unduly restrict interstate activities. Clear statutory preemption clauses, regulatory sandboxes, and interstate compacts can further minimize conflicts and promote shared learning across jurisdictions.

Moreover, adaptive governance mechanisms—such as mandatory periodic reviews, impact assessments, and joint advisory councils between federal and state regulators—can ensure that regulation keeps pace with technological change. In this sense, federalism should not be

[49] Brian Knight, *Federalism and Federalization on the Fintech Frontier*, 20 *Vanderbilt J. Entertainment & Technology Law* 129 (2020).
[50] Satoshi Narihara, Toshiya Jitsuzumi & Miki Oguma, *AI Policy and Law in the United States: The Development at the Federal and State Levels*, 16 *J. Law & Information System* 34 (2024).

viewed as a rigid constitutional constraint but as a living framework capable of evolving with societal needs and technological realities.

Ultimately, the successful regulation of emerging technologies depends on the ability of federal and state governments to collaborate rather than compete. Federalism, when properly coordinated, can become a source of strength—combining the uniformity of federal oversight with the creativity of state innovation. In an age where technology transcends borders and disrupts conventional governance, the United States must embrace a federal model that is flexible, cooperative, and forward-looking. Only through such balance can the nation safeguard public values while sustaining technological progress and democratic legitimacy in the digital age.

References

1. Brian R. Knight, Federalism and Federalization on the Fetch Frontier, 20 VAND. J. ENT. & TECH. L. 129 (2020)
2. Tejas N. Narechania & Erik Stallman, Internet Federalism, 34 HARV. J.L. & TECH. 548 (2021).
3. Sarah E. Light, Federalism and the Regulation of Emerging Technology, 45 HARV. J. ON LEGIS. 201 (2023).
4. Roger Handsaw, Pre-emption, Federalism, and the Regulation of Emerging Technologies, AM. BAR ASS'N, SEC. OF ENV'T, ENERGY & RES. (2025).
5. Carnegie Endowment for Int'l Peace, Federalism and the Regulation of Emerging Technology (2023).
6. Tatevik Davtyan, The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained, 16 CASE W. RES. J.L. TECH. & INTERNET 223 (2025).
7. Bilyana Petkova, The Safeguards of Privacy Federalism, 20 LEWIS & CLARK L. REV. 595 (2016).
8. Daniel J. Mallinson et al., The Future of AI Is in the States: The Case of Autonomous Vehicle Policies, 26 BUS. & POL. 180 (2024).
9. Srinivas Parinandi, Jesse Crosson, Kai Peterson & Sinan Nadarevic, Investigating the Politics and Content of U.S. State Artificial Intelligence Legislation, BUS. & POL. (Mar. 2024).
10. Jon Chun, Christian Schroeder de Witt & Katherine Elkins, Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the U.S., arXiv preprint (Oct. 2024).
11. U.S. DEP'T OF TRANSP. (NHTSA), Federal Automated Vehicles Policy Guidance (2024).
12. 47 U.S.C. § 154 (2018) (establishing the Federal Communications Commission under the Communications Act of 1934, as amended).
13. 15 U.S.C. § 41 (2018) (establishing the Federal Trade Commission).
14. VA. CODE ANN. §§ 59.1-575–585 (2021) (Virginia Consumer Data Protection Act).
15. CAL. CIV. CODE § 1798.100 et seq. (West 2018 & Supp. 2025) (California Consumer Privacy Act).
16. Christopher S. Yoo & Alexander Mueller, U.S. Artificial Intelligence Regulation During the Biden Administration, 17 J.L. ECON. & REG. 7 (2024).
17. Daniel A. Lyons, Technology Convergence and Federalism: The Case of VoIP Regulation, 45 U. MICH. J.L. REFORM 56 (2012).
18. Yiyang Mei & Michael J. Broyde, Reclaiming Constitutional Authority of Algorithmic Power, arXiv preprint (Aug. 2025).

Bibliography

• Carnegie Endowment for Int'l Peace, Technology Federalism: U.S. States at the Vanguard of AI Governance (2023).
• Cong. Research Serv., Stepping In: The FCC's Authority to Pre-empt State Laws, CONGRESS.GOV (2025).
• Int'l Ass'n of Privacy Prof'ls (IAPP), U.S. State Privacy Legislation Tracker (2025).
• Nat'l Conf. of State Legislatures (NCSL), Artificial Intelligence & Autonomous Vehicle Legislation Trackers (2025).
• New York Judiciary Issues Interim Policy on Generative AI Use in Courts, REUTERS (2025).
• Nicol Turner Lee & Obioha Chijioke, Why States and Localities Are Acting on AI, BROOKINGS INST. (Dec. 15, 2023).
• Robert D. Williams, To Enhance Data Security, Federal Privacy Legislation Is Just a Start, BROOKINGS INST. COMMENTARY (Dec. 1, 2020).
• U.S. DEP'T OF TRANSP., Broadband Equity, Access, and Deployment (BEAD) Initiative (2024).