Available Online: 27 January 2026 DOI: 10.54254/2753-7102/2026.31528

"Digital Leviathan" and "Digital Commons": a comparative study of digital government development paths in China and the United States with consideration of privacy rights

***Qian Gong*[1,2*], *Ming Ni*[1]**

[1]School of Economics, Management and Law, Changchun Normal University, Changchun, China
[2]School of Public Administration, Jilin University, Changchun, China

*Corresponding Author. Email: gongqian@ccsfu.edu.cn

Abstract. Amid the global wave of digital government transformation, China and the United States have pursued markedly different development paths. This paper investigates the fundamental differences between the two countries' approaches in terms of top-level design, technological applications, public participation, and the impact on privacy rights, as well as the underlying logic behind these differences. Through comparative case studies and policy text analysis, the research focuses on China's "Health Code" and "One-Stop Online Services," alongside the EU's GDPR and California's CCPA as core cases. The main findings are as follows: China's path is state-led and efficiency-oriented, producing highly effective governance tools but facing the risk of a "Digital Leviathan"; the U.S./EU path prioritizes rights and checks and balances, building a "Digital Commons" at the potential cost of efficiency. Both approaches must confront their respective challenges and explore avenues for dialogue and mutual learning.

Keywords: digital government, privacy rights, Digital Leviathan, Digital Commons, China-U.S. relations

1. Introduction

As digital technologies become deeply embedded in state governance, a global wave of digital government transformation has emerged. "Building a digital government is an inevitable outcome of the deep integration of technological development and state governance. It is also a key measure for countries and regions to fully enhance development momentum and improve people's well-being in the digital era" [1]. Guided by the "Digital China" strategy, China has promoted the deep integration of digital technologies with public administration and social governance. From crisis management practices such as the "Health Code" to the routine service optimization of "One-Stop Online Services," digital technologies have become a core pillar supporting the modernization of the national governance system and governance capacity. The United States, by contrast, has launched various "digital service" initiatives, leveraging a market-driven innovation ecosystem and a mature legal tradition to construct a digital governance framework centered on the protection

of privacy rights. As central actors in global digital governance, China and the U.S. have chosen markedly different paths, reflecting their respective institutional advantages while simultaneously exposing the common challenge of balancing governance and individual rights in the digital era. This transformation has profoundly reshaped government operations and the state–citizen relationship, with significant implications for the structure of civil rights.

Although both countries employ advanced digital technologies to advance government modernization, their practical implementations and public experiences differ markedly. China's digital government is characterized by high-efficiency coordination and comprehensive coverage, demonstrating strong executive capacity in pandemic control and public service optimization. The U.S. digital government, in contrast, prioritizes rights protection and checks and balances, employing a rigorous legal framework and market mechanisms to prevent the abuse of power. Are these differences merely superficial variations in technological application, or do they reflect fundamental divergences rooted in political philosophy and institutional tradition? Why do similar technological tools produce radically different governance outcomes and rights protection paradigms? And while digital technologies strengthen state governance capacity, how can they avoid excessively encroaching upon citizens' privacy? These questions form the core research agenda of this study.

This research carries both theoretical and practical significance. Theoretically, it goes beyond a purely technological determinist perspective, approaching the issue from the standpoint of the political philosophy of technology. By integrating the theoretical frameworks of the "Digital Leviathan" and the "Digital Commons," it conducts an in-depth analysis of the state–technology–society interaction, bringing together political philosophy, state–society relations, legal traditions, and the technological development environment into a unified analytical framework. This enriches research in the fields of digital governance and comparative politics, offering new perspectives for understanding state governance models in the digital era. Practically, it clearly delineates the differences between China's and the U.S.'s digital government development paths and their impacts on privacy rights. It provides a reference for optimizing and upgrading China's digital government—maintaining governance efficiency while mitigating "Digital Leviathan" risks through legal system improvement, enhanced algorithmic transparency, and strengthened oversight mechanisms. It also offers lessons for global technology governance and the protection of civil rights, promoting the development of an inclusive and pluralistic digital governance framework.

2. Theoretical framework construction

Within the field of digital government research, two core paradigms have emerged. The "efficiency paradigm" focuses on how digital technologies enhance administrative efficiency and governance effectiveness, while the "rights paradigm" emphasizes the protection and safeguarding of citizens' rights, particularly privacy. Scholarly debates have long centered on the tension between "digital authoritarianism" and "digital democracy": some argue that digital technologies may reinforce centralization of power, whereas others contend that they can empower citizen participation. Existing comparative studies of China's and the U.S.'s digital governance often examine single dimensions—such as technological applications, institutional design, or cultural traditions—lacking a systematic integration. Moreover, many studies adopt either descriptive or binary-contrast approaches, failing to incorporate technological pathways, governance logic, and rights outcomes into a unified analytical framework. To address this gap, this paper employs "Digital Leviathan" and "Digital Commons" as core theoretical lenses, refining conceptual definitions and constructing a comparative framework.

The Digital Leviathan concept derives from Hobbes' theory of absolute sovereignty. In the digital era, it specifically refers to the establishment of a centralized, unified, and highly coordinated state governance system empowered by digital technologies. Its core is a "control-enabled" governance model, which prioritizes order, security, and efficiency, with legitimacy grounded in governance performance. China's tradition of "concentrating power to accomplish major tasks" provides fertile ground for this approach.

The Digital Commons, by contrast, is rooted in Locke's social contract theory and Ostrom's theory of common-pool resources. In the digital era, it refers to the governance model in which digital resources are treated as public goods, managed collectively by multiple stakeholders. Its core is a "rights-contractual" governance model, which emphasizes freedom, innovation, transparency, and checks and balances, with legitimacy grounded in procedural justice and the protection of individual rights.

Building on these concepts, this paper constructs a four-dimensional comparative model: *value objectives – actor structure – technical architecture – rights outcomes.* Value objectives: China prioritizes governance; the U.S. and EU prioritize rights. Actor structure: China exhibits a state-centered, unitary leadership model; the U.S. and EU display multi-actor co-governance with checks and balances. Technical architecture: China favors centralized platforms and interlinked data systems; the U.S. and EU lean toward distributed, federalized systems with minimal necessary data collection. Rights outcomes: China produces "managerial privacy protection", emphasizing post-hoc remedies and process compliance; the U.S. and EU pursue "defensive privacy rights", focusing on preventive measures and individual control. Using a comparative case study approach, combined with policy text analysis and secondary data, this study selects China's "Health Code" and "One-Stop Online Services", as well as the EU's GDPR and California's CCPA, as core cases to systematically examine the practical differences between these two governance paradigms.

3. The Chinese path: "control-enabled" digital government and "managerial privacy"

China's digital government is guided by a "control-enabled" logic and has established a "managerial privacy protection" paradigm. While strengthening state governance capacity, it simultaneously balances privacy rights through both institutional and technological safeguards, forming a distinctive development trajectory.

3.1. Top-level design: coordinated institutional architecture

China's digital government development follows a "national chessboard" strategy, led by the Overall Layout Plan for the Construction of Digital China, highlighting the Party's leadership and central coordination, and positioning data as a core productive factor to promote integration and utilization. This design is rooted in collectivist values and a strong state-governance logic, establishing the government's dominant role in digital governance. Institutionally, a three-tier framework of law + policy + standards has been formed: the Personal Information Protection Law (PIPL) provides a legal foundation, specialized policies specify implementation pathways, and industry standards ensure operational feasibility. This framework both guarantees unified and efficient development and mitigates risks of data misuse. Development goals are closely tied to the modernization of national governance, with "data-driven governance" empowering macro-level regulation, public safety, and the protection of citizens' livelihoods.

3.2. Technology application: efficiency-oriented practice logic

The Health Code system centers on a centralized data platform, integrating multi-departmental data resources and applying the logic of "data integration → risk assessment → targeted control" to implement dynamic,

tiered management of individuals. During the pandemic, it demonstrated remarkable governance efficiency by rapidly breaking transmission chains, though it also raised concerns about excessive data collection, algorithmic opacity, and data security risks. Post-pandemic, the Health Code has expanded to areas such as public services and transportation, evolving into a routine governance tool that exemplifies the path of "crisis-driven innovation → normalization and scaling."

The One-Stop Online Services ("Yi Wang Tong Ban") initiative centers on user-centricity, optimizing service experience through platform integration, data sharing, and process reengineering. It employs a "single source, cross-verification" mechanism to unify frequently used administrative data, enabling "one matter, one-time processing" and fully online procedures, significantly enhancing administrative efficiency and public satisfaction. At the same time, technical measures such as data classification, access control, and permission management help prevent data leakage and misuse.

3.3. Public participation: limited responsive engagement

In China's digital government, citizens primarily function as data providers and service users, submitting personal information as required to access services or comply with governance measures; such data provision carries a degree of compulsion. Channels for participation are mainly service feedback mechanisms, such as government evaluations or the 12345 hotline, but there is a lack of institutionalized involvement in core processes such as governance rule-making or technical architecture design. This model aligns with China's state–society relationship and exhibits a "responsive participation" pattern. While some regions have expanded engagement through open data initiatives, multi-actor co-governance remains at an early stage.

3.4. Privacy impact: a balanced protection paradigm

China has developed a "managerial privacy protection" paradigm, in which privacy rights are balanced against public interest and governance efficiency. Its key features include: Instrumental positioning of privacy: privacy protection may yield to public safety in emergencies. Dual legal and technical safeguards: implementation follows the principles of legality, legitimacy, and necessity, with technical measures such as data anonymization and encrypted storage. Digital Leviathan risk: excessive data collection, leakage vulnerabilities, and limited recourse remain challenges. Progressive improvement: privacy protection is gradually evolving; the introduction of the Personal Information Protection Law marks a shift toward rule-of-law governance. Some regions are experimenting with algorithmic transparency and cross-border data management, and rising public awareness is driving regulatory refinement.

4. The U.S./EU path: "rights-contractual" digital government and "defensive privacy rights"

The digital governments of the United States and the European Union are guided by a "rights-contractual" logic, establishing a "defensive privacy rights" protection paradigm. While upholding the baseline of rights protection, this approach also considers governance effectiveness and market-driven innovation, resulting in a distinctive development path grounded in rule of law and multi-actor co-governance.

4.1. Top-level design: rights-oriented legal framework

The U.S. and EU digital government models are rooted in liberalism and the limited-government tradition, with the rule of law establishing the baseline for rights protection. The EU has constructed a unified privacy legal framework centered on the General Data Protection Regulation (GDPR), which defines the legal basis

for data processing and individual rights. Implementation is ensured through coordinated oversight by the European Commission, national supervisory authorities, and the European Data Protection Board. The United States exhibits a federal–state decentralized governance structure. At the federal level, legislation such as the Federal Trade Commission Act regulates data practices, while at the state level, laws such as California's California Consumer Privacy Act (CCPA) and Virginia's Virginia Consumer Data Protection Act (VCDPA) establish localized rules. Market forces complement legal mechanisms through industry self-regulation and competition, enhancing privacy protection. Institutional objectives in both contexts prioritize citizen rights while also considering administrative efficiency and market innovation. The GDPR emphasizes the protection of personal data rights and the free flow of data, whereas the CCPA focuses on empowering consumers with information control and maintaining market fairness. Governance mechanisms form a triadic structure of legal regulation + market constraints + public oversight: the law defines rights and obligations, the market encourages enterprises to respect privacy through consumer choice, and the public supervises compliance through litigation, complaints, and reporting.

4.2. Technology application: privacy-first practice logic

EU public digital services strictly adhere to the GDPR, applying "privacy by design and by default" principles throughout the process. Data-minimization techniques are employed to collect only necessary information, with default settings providing the highest level of privacy protection. Technical architecture is distributed, with cross-departmental data sharing subject to stringent legality and necessity requirements. Encrypted transmission ensures security during inter-agency data transfers. While this model effectively safeguards privacy, it can reduce administrative efficiency, complicate cross-departmental data sharing, increase technical development and operational costs, and potentially exacerbate the digital divide. Some U.S. municipal platforms embrace the Digital Commons concept, publicly sharing transportation, environmental, and other public data to encourage developer participation in application development. Open-source technologies are used to build government service platforms, which are iteratively optimized based on public feedback. In technological application, both rights protection and market innovation are balanced: when governments cooperate with private enterprises, clear boundaries for data use are established, and privacy features such as user-controlled data sharing and revocable consent are embedded. This approach enhances service innovation while enabling public oversight through participatory engagement.

4.3. Public participation: citizens as rights holders and supervisors

In U.S. and EU digital governments, the public enjoys extensive statutory rights and participatory channels, forming the core support for "defensive privacy rights." In terms of rights, the GDPR and CCPA grant citizens the rights to be informed, consent, deletion, data portability, and remedies, providing legal instruments to counter potential abuses of power. Regarding participatory channels, citizens can initiate litigation or file complaints to compel corrective actions against violators. Following the GDPR's implementation, EU supervisory authorities received a substantial number of complaints, resulting in fines totaling several billion euros. Citizens can also participate in rule-making through public hearings and consultations, as seen in the extensive incorporation of public opinions during the CCPA revision process. Additionally, open-source communities and volunteer projects allow citizens to contribute to the development and optimization of digital service platforms. This participatory role is rooted in the U.S./EU political philosophy and the weak-state–strong-society configuration, ensuring the legitimacy and fairness of digital governance while enhancing service quality and adaptability.

4.4. Privacy impact: core features and challenges of defensive protection

In the U.S. and EU, "defensive privacy rights" regard privacy as a fundamental human right against state and corporate encroachment, with both absolute and foundational significance. In the U.S., the Fourth Amendment prohibits unreasonable searches and seizures, and cases such as Riley v. California confirm that digital property, including mobile phone data, is protected and requires a search warrant for law enforcement [2]. In the EU, the GDPR establishes privacy as an independent fundamental right, which cannot be improperly constrained by other public policy objectives. Legislation in both contexts constructs a comprehensive data lifecycle protection system, specifying clear rules for the collection, storage, use, transmission, and deletion of data. Data collection must be explicitly communicated and consented to, and government processing must undergo privacy impact assessments with publicly disclosed rules. At the same time, reasonable regulatory mechanisms balance privacy protection with market innovation. The GDPR permits compliant data sharing and secondary use, while the CCPA incorporates exemptions for small and medium-sized enterprises to reduce compliance costs.

5. Comprehensive comparison and deep-logic analysis

5.1. Systematic comparison

Within the global spectrum of digital government development, China, the United States, and the European Union represent three highly typical yet internally divergent governance paradigms. The differences among these paths extend far beyond technological applications, being deeply rooted in their respective political philosophies, governance traditions, and social contracts, which in the digital era have evolved into distinct state–market–society configurations. Table 1 presents a systematic comparative analysis of these three paths across key dimensions—including value objectives, actor structure, technical architecture, rights outcomes, core advantages, and major risks—providing a multidimensional framework for understanding global government transformation in the digital era and its complex shaping of fundamental privacy rights.

Table 1. Multi-dimensional comparison of digital government development paths in China and the U.S./EU

Dimension	Chinese Path	U.S./EU Path
Value Objectives	Governance-first (efficiency, stability), public-interest oriented	Rights-first (freedom, privacy), individual-rights oriented
Actor Structure	State-centered, unitary leadership, coordinated "active government + effective market + organic society"	Multi-actor co-governance, checks and balances, government–market–society–citizen participation
Technical Architecture	Centralized, unified platforms, data interoperability, supported by nationwide system	Distributed, federalized, minimal necessary data collection, market-driven and open-source collaboration
Rights Outcomes	Managerial privacy protection (post-hoc remedies, process compliance), balancing privacy with public interest	Defensive privacy rights (preventive measures, individual control), privacy as a fundamental human right

Table 1. Continued

Core Advantages	High governance efficiency, rapid responsiveness, broad coverage	Strong rights protection, high transparency, robust innovation capacity
Major Risks	Digital Leviathan, over-compression of privacy, algorithmic opacity	Insufficient governance efficiency, high compliance costs, digital divide

5.2. Exploration of the roots of differences

5.2.1. Political philosophy

China is deeply influenced by collectivism and a strong tradition of state-led governance, emphasizing the state's role in guiding and managing society. Individual rights are expected to be aligned with the public interest, and digital technologies are regarded as tools for enhancing state governance capacity. This philosophical tradition draws from Confucian ideals such as "all under heaven belongs to the public" and the primacy of the collective, as well as the practical experience of nation-building in modern times, forming a strong-state governance logic.

In contrast, the U.S. and EU are rooted in liberalism and the limited-government tradition, prioritizing the limitation of public authority and the protection of individual freedom. The government's core duty is to safeguard citizens' rights, and digital technologies must not infringe upon personal privacy or liberty. This philosophical tradition derives from the Enlightenment idea of natural human rights and the principles of procedural justice in Anglo-American common law, producing a limited-government governance logic.

5.2.2. State–society relations

China exhibits a strong-state, weak-society configuration, where the state plays a leading role in resource allocation and governance implementation, and social actors primarily serve supportive or auxiliary roles. This pattern originates from the historical centralization of authority and the post-1949 integration of society by the state, enabling digital government development to proceed rapidly based on a powerful administrative system, achieving nationwide unified technical infrastructure and governance rules.

The U.S. and EU, by contrast, present a weak-state, strong-society pluralistic model, in which social forces —including market actors, civil society organizations, and individual citizens—effectively check state power. This configuration stems from Western traditions of decentralization and the development of civil society, meaning digital government development is constrained by multiple actors, with rights protection as a core priority, while social participation also provides innovation and vitality to digital governance.

5.2.3. Legal tradition

China belongs to a civil law system, in which law is highly instrumental and carries paternalistic characteristics. It emphasizes using legal norms to achieve governance objectives, prioritizing substantive justice and efficiency. Digital governance laws in China are often policy-driven, emphasizing principled yet operable rules, implemented through an administratively-led enforcement model. Privacy protection tends to manifest as process compliance and post-hoc remedies.

The U.S. and EU, by contrast, are centered on common law and procedural justice, emphasizing rights protection and power limitation, with a focus on procedural fairness and access to remedies. Digital governance laws in these contexts are rights-oriented, clearly defining individual rights and channels for recourse, and are enforced through independent judicial and supervisory institutions. Privacy protection is primarily preventive and emphasizes individual control.

5.2.4. Technological development environment

China leverages a state-led "whole-nation system", concentrating resources to advance the application of digital technologies in government governance, creating nationwide unified digital infrastructure and technical standards. The government plays a central role in technology R&D, data integration, and platform construction, with enterprises and research institutions collaborating to drive innovation. The focus of technological development is on practicality and large-scale deployment.

In the U.S. and EU, by contrast, technology development is driven by a market-oriented innovation ecosystem, where progress is largely propelled by market and social forces, and the government primarily functions as a rule-maker and regulator. As noted, "the starting point of artificial intelligence technology is led by open-source communities and tech companies, fundamentally aiming to apply innovation in economic life and promote the diffusion of welfare" [3]. Technology development emphasizes innovation and rights protection, with market competition driving rapid iteration and broad application.

5.3. Trends of mutual learning between paths

General Secretary Xi Jinping has emphasized: "We should promote civilizational exchanges that respect differences while embracing diversity. The multiplicity of human civilizations brings this world its rich colors; diversity leads to exchange, exchange nurtures integration, and integration generates progress. Civilizations must coexist with a spirit of harmony in difference. Only by respecting one another, learning from one another, and coexisting harmoniously amid diversity can the world become rich, vibrant, and flourishing [4]." Although the digital government paths of China and the U.S. show significant differences, they are not entirely opposed; instead, they are exhibiting trends of mutual observation and selective learning. China has been continuously improving its legal framework for personal information protection, strengthening privacy safeguards—the enactment of the Personal Information Protection Law (PIPL) marks the beginning of a rule-of-law approach to privacy. Some regions have started experimenting with algorithmic transparency and cross-border data management, drawing on the U.S. and EU experiences in rights protection.

The U.S. and EU are likewise exploring mechanisms for efficient data use in crisis scenarios, seeking to balance rights protection and governance effectiveness. For example, during the pandemic, the EU introduced temporary policies that relaxed data-sharing restrictions to enhance emergency response capabilities; during the CCPA revision process, California considered public-safety exceptions, balancing privacy protection with public interest. At the same time, the U.S. and EU have begun to observe China's experience in optimizing public services and integrating data; some municipal open-source platforms have adopted process-reengineering concepts inspired by China to improve service efficiency. This trend of mutual learning arises from the shared challenges of digital governance: whether it is the risk of a Digital Leviathan or the rights–efficiency dilemma, these are universal issues facing governments undergoing digital transformation. As noted, "For the United States, as a leading regional power, achieving stable hegemony in the Asia-Pacific requires not only leveraging its strong hard power but also engaging in broad cooperation with regional countries to truly enhance its comprehensive political and economic influence in the region" [5]. As core participants in digital governance, China and the U.S. can mutually learn from each other, improving their own governance capacity while providing a practical foundation for the development of global digital governance rules.

6. Conclusion

This study, through comparative case analysis and policy text examination, systematically explored the differences in digital government development paths between China and the U.S., as well as their impacts on privacy rights, using the "Digital Leviathan" and "Digital Commons" frameworks as the core theoretical lens. The findings indicate that China has developed a "control-empowerment" path, characterized by state leadership and efficiency priority. Relying on a centralized technological architecture and a managerial privacy protection paradigm, China balances governance effectiveness with privacy rights, while facing the risk of a Digital Leviathan. By contrast, the U.S. and EU have established a "rights-contractual" path, centered on multi-actor co-governance and rights prioritization. Through distributed technological architectures and a defensive privacy rights paradigm, they protect citizen rights but confront challenges such as reduced governance efficiency. The roots of these differences lie not in superficial technological choices but in deep-seated divergences in political philosophy, state–society relations, legal traditions, and technological development environments. It is noteworthy that the Chinese and U.S./EU paths are not entirely opposed; a trend of mutual learning is emerging. China has strengthened legal safeguards for privacy, while the U.S. and EU are exploring ways to improve governance efficiency. Future digital government development must seek a dynamic balance between governance effectiveness and rights protection. As core global participants in digital governance, the practices and mutual learning experiences of China and the U.S. provide an important reference for fostering an inclusive and pluralistic framework of global digital governance rules.

Funding project

Youth Fund for Humanities and Social Sciences Research, Ministry of Education: "The Impact of Artificial Intelligence on Global Security and Its Governance Obstacles" (24YJC810002)

References

[1] Wan, L. (2025). Innovative practices and insights from domestic and international advanced cities in digital government construction. *Exploration*, *3*, 113–120.

[2] Liu, Y. (2025). The evolution of the reasonable expectation of privacy: Development of U.S. privacy law theory in the digital era. *Human Rights Law*, *2*, 119–138, 167–169.

[3] Xue, L. (2025, March). How can AI governance keep up with technological advancement? *China Newsweek*.

[4] Xi, J. (2015). *Speech at the series of summits commemorating the 70th anniversary of the United Nations* (p. 18). Beijing: People's Publishing House.

[5] Ma, F. (2017). Reshaping the Asia-Pacific order and the "soft" management of U.S.-China differences. *Peace and Development*, *4*, 56–68.