

Development of the U.S. Digital Economy: Problems and Countermeasures

Yanbin Zhuang^{1,*}

¹Business College, University of
Connecticut, Storrs, U.S.

*Corresponding author: rci24001@
uconn.edu

Abstract:

This article examines the growth of the digital economy in the United States rigorously. It discusses some of the current problems and suggests concrete solutions. The present work discovers slow digital transformation in traditional industries, an expanding digital divide in firms and territories, and continuing challenges in data security and privacy protection. The rising international rivalry's intensification, or the challenge posed by China's state-backed technological strategies and meanwhile the extraterritorial repercussions of EU regulations, further convoluting United States policy, is described by this article. The research recommends improving data governance, enabling access to digital infrastructure, fostering greater industrial integration, and collaborating internationally on rulemaking to safeguard competitiveness. In addition to producing usable findings for policymakers and industry leaders, the work also provides insight into the significance of timely, flexible strategies in a period of rapid technological change. This research helps both theoretical study and practical policymaking in the digital economy.

Keywords: Digital economy; industrial transformation; data security; global competition.

1. Introduction

The digital economy in the US has evolved rapidly, driven by technological progress in internet, mobile, and cloud computing. The advancement of the digital economy in the US has evolved with successive waves of technological innovation, starting with the widespread deployment of the internet in the 1990s. The widespread adoption of mobile devices and cloud computing in the 2000s spurred rapid digital integration, facilitating new business models and altering consumer behavior. The internet extends our

reach in communication, learning, and participation in the economy. The current wave of AI augmentation has further expanded digital capabilities, propelling innovative new business models in finance, healthcare, manufacturing, and other fields. But this has occurred unevenly, and conventional sectors frequently lack the capacity to effectively adopt and scale digital, creating a digital divide. Regrettably, this gap threatens to worsen, leading to more inequitable access to opportunities and resources. It calls for an inclusive digital policy that balances innovation with inclusion in our digital transformation [1].

The US currently confronts three major, synergistic concerns related to the digital economy due to unbalanced progression and global interdependence: sluggish digital transformation in conventional sectors, persistent data security and privacy risks, and developing global regulatory and competitive tensions. Many manufacturing and service firms still struggle with more extensive digital transformation, which strains company performance and widens the digital divide, especially for small and medium-sized businesses (SMEs) with insufficient digital resources and talents [2]. Increased data breaches have exposed regulatory gaps and eroded consumer confidence, while conflicting US and foreign regulations have made information privacy requirements more complicated. Chinese and EU international benchmark initiatives are escalating competitive and regulatory responses for US corporations, increasing the intricacy of digital governance globally.

The digital economy is critically important to the US economy by catalyzing innovation, boosting productivity, and enhancing the quality and variety of goods and services. However, the digital divide significantly exacerbates social and economic inequalities and limits opportunities for inclusive growth directly. The digital economy has accelerated information flows and technologies, making resources and opportunities more accessible worldwide. But “digital” is not universally accessible, and regional disparities in the deployment of digital resources and training perpetuate, if not aggravate, existing inequities [3-4]. Any strategic plan must be cognizant of growing disparities to guarantee the broadest possible dissemination of digital transformation’s rewards; policymakers cannot afford to neglect these important disparities.

2. Problem

Slow digital transformation in traditional sectors, persistent data security and privacy issues, and increasing international competitive and regulatory pressures define the connected challenges the US digital economy confronts. In many conventional service sectors, including manufacturing, adoption of digital technology is sluggish, preventing productivity growth and widening the digital divide for SMEs that lack digital resources and talent. High-profile data breaches like the Equifax hack reveal regulatory loopholes and reputational risks. State-backed Chinese technology firms and the extraterritorial effects of EU legislation imperil US market dominance and regulatory authority [5-6]. In this rapidly evolving environment, the US needs to improve data governance, increase digital infrastructure and competitiveness, and work internationally to preserve competitiveness and authoritativeness.

2.1 Industrial Transformation and the Digital

Divide

In the US digital economy, slow adoption of commercial technology in conventional manufacturing and service sectors, as well as continuing disparities in access to digital infrastructure, are impediments to industrial transformation. Their ability to innovate and adjust is harmed by the unwillingness of many industrial and service sectors to develop their systems [7]. According to comparative studies, improved company performance is a direct result of digital innovation and transformation [8]. Many businesses, however, lack change strategies. Cost issues, a lack of technological infrastructure, and a lack of digital expertise all constrain adoption. These constraints are worsened for SMEs by limited access to government programmes and cooperation. Because of their lack of infrastructure and digital expertise, rural and poor participants also encounter barriers that aggravate regional disparities. A targeted strategy is needed to successfully address these concerns. This method might entail better access to technology and training in digital abilities and the addition of legal structures to digital infrastructure growth.

Traditional steel and car production are offered as examples of the difficulties associated with industrial change. Robotics, AI-driven predictive maintenance systems, and industrial internet platforms are only to some extent implemented by the industry [9]. The majority of businesses still use obsolete equipment and manufacturing processes. As a result, productivity increases have not grown as quickly as they have in sectors with a high level of technical innovation, leaving US heavy industry vulnerable to foreign competitors with greater digital integration. The digital divide is highlighted by infrastructure inequities between Europe and the US [10-12]. According to Federal Communications Commission statistics, urban consumers receive high-speed internet at a rate of approximately 97%, whereas only around 65% of rural households do. This disparity exacerbates levels of social and income inequality. It inherently limits rural households’ and SMEs’ ability to use cutting-edge digital technologies in addition to the fundamental issue of infrastructure access.

2.2 Data Security and Privacy

Persistent data protection and privacy problems remain the most significant issues with the digital economy in the US. Any insufficiencies or poor implementation of regulatory frameworks are demonstrated to have dire results for businesses and millions of people whose important or private information was exposed thanks to high-profile data breaches like the Equifax leak or the SolarWinds intrusion [13]. For consumers, varying degrees of protection materialise depending on whether they reside in a state with privacy rules as opposed to the federal level, whereas, for businesses, diverse levels of protection elsewhere account

for varying degrees of responsibility and cost. The framework of the European Union's General Data Protection Regulation has a completely different unity (GDPR). According to multiple academics, the statistics processing regulations in the GDPR are much more successful because of the harder implementation. New technologies, including cloud computing and the Internet of Things (IoT), raise issues for data integrity since they form large-scale heterogeneous data repositories that traditional security mechanisms are unable to safeguard. As a result, contemporary and cutting-edge methods like complex encryption algorithms, access control, and privacy-by-design must be implemented. The US stands the chance of dropping behind its competitors' measures for electronic safeguarding and failing to maintain public faith without a complete and flexible regulatory framework [13].

2.3 Global Competition and Regulatory Leadership

The competition for the global digital economy between China, the EU, and the US is becoming increasingly fierce, with each enacting their own technological and regulatory paradigm. The state-endorsed, top-down industrial technique, which involves large investments in significant technologies like telecommunications and artificial intelligence, allows Chinese enterprises to challenge US digital supremacy in key sectors and push for global standards alignment. The US government had to display a more interventionist impulse to preserve market supremacy. The US reaction emphasised support for standards development and assumption of the role of innovation [14]. Contrarily, the extraterritorial reach of the GDPR adds to the price of compliance for US businesses. The US government needs to take on a larger role in international standard-setting in order to counteract current and future competitive and regulatory pressures. It needs to leverage its technological prominence and promote open digital ecosystems through participating in multilateral initiatives and setting standards and rules for emerging technologies [15].

In reality, US governmental actions targeting specific technology and companies reflect this rising competition. The limits imposed on Huawei's participation in 5G infrastructure contracts or the examination of TikTok over data security issues reflect national security concerns that impact digital governance. Such a US stance indicates a willingness to utilize regulatory control over market access as a defense against what it deems as risky technologies, a behavior changes from earlier laissez-faire positions. Due to the strategic AI rivalry between China and the US, this intense AI investment divide underscores the underpinning technologies, with China committing more than \$70 billion of state-backed money for AI development, where-

as US financing is spread out across federal research programs and private industry ventures. The disparities highlight the distinct governance structures and market-driven versus state-led techniques used by both powerful nations.

3. Countermeasure

The US digital economy's problems need a multi-pronged strategy. Because of this, there is a pressing need for multi-stakeholder and inclusive strategy development. The introduction of emerging digital technologies by SMEs may be sped up with the use of public-private partnerships and focused workforce training initiatives. Moreover, a unified US federal data governance approach is required [16]. To facilitate a particularly easy adherence, international regulatory cooperation will counterbalance competing frameworks such as those of the EU and China. These methods have to be combined to ensure long-term economic resilience and competitiveness.

3.1 Promoting Industrial Integration and Bridging the Digital Divide

The strategy for powering industrial integration and bridging the digital divide requires a multi-pronged approach. Legislative and regulatory frameworks are important policy instruments to facilitate digital infrastructure construction and resource distribution in order to close the digital divide. An equitable digital human resource distribution is improved in the US by the Rural Digital Opportunity Fund (RDOF), which the Federal Communications Commission recently introduced. It allocates over \$20 billion to significantly raise high-speed broadband access in rural communities with low service levels.

The RDOF programme might provide grants to finish infrastructure construction in essential rural regions in accordance with precise speed and location commitments. In theory, this will reduce regional disparities. Distributing digital resources contributes to digital supply-side resilience, which promotes sustainable industrial growth, so the digital divide must be eliminated. In fact, a digital divide in connection to mobile business websites and digital media marketing reduces SME efficiency. Building a digital economy is facilitated by developing a digital infrastructure that integrates humans and data. Human capital is continually refreshed by the development of local economies dependent on SMEs because they are flexible. Stimulating entrepreneurial dynamism may enhance a country's comparative advantage and boost industry competitiveness [17].

3.2 Strengthening Data Governance and Privacy Regulations

New, coordinated US data legislation that balances inno-

vation, security, and privacy goals is a government emphasis. The Digital Economy Act created the Digital Markets Unit for market fairness and consumer protection in the broad technology sector. A market-driven regulatory environment is essential to the digital economy and non-digital sectors. The legislation's central provisions would ensure data security, set guidelines for promoting interoperability and data portability to let consumers decide how their data is processed by the digital ecosystem, and allow for the smooth sharing of data inside organisations while upholding privacy rights. The European Union's agency, the European Center for Cybersecurity, was established by the EU's Cybersecurity Act. This legislation also aims to fortify the Connected Digital Single Market and advance the EU's global mission to withstand cyber-attacks. It emphasizes a unified approach to data security and cybercrime and introduces the Binding Corporate Rules procedure. It transforms industry self-regulation into a binding strategy to handle consumer data, offering certain companies a set of maximum regulatory rules.

3.3 Enhancing International Cooperation and Regulatory Strategy

The U.S. can bolster international cooperation and regulatory strategies to secure its digital economy and augment national resilience by prioritizing the establishment of bilateral and multilateral partnerships to offer transparent and standards-based alternatives to authoritarian models while consolidating internal regulations to foster a participatory and trustworthy digital ecosystem. A multi-level collaboration among democratic partners to facilitate cooperation on international standards and best practices will be essential in countering the EU's regulatory dominance and China's centralized approach in driving global digital agendas and establishing global digital norms dedicated to safeguarding democratic values. Strengthening existing alliances through forums like the Quad, AUKUS, and Five Eyes, and engaging or even expanding these partnerships to developing nations or regional powers, can further support the promotion of an open, interoperable digital trade framework. In this regard, leveraging the existing WTO, G20, and OECD platforms can offer new economic alternatives to confront China's state-led economic model. Moreover, the prioritization of innovation, intellectual property protection, and resilient trade systems that avoid dependency on global supply chains should become key elements of U.S. domestic policies. Following these combined international and domestic strategies, the U.S. is capable of remaining atop the digital economy while gaining international traction in molding an open and interoperable digital space that prioritizes democratic values.

4. Conclusion

The digital economy in the U.S. serves as a cornerstone of economic growth, social progress, and national competitiveness. The gaps it faces, such as the underprivileged digital divide between vast segments of the population, the stagnated digitalization of traditional industries, the persistent data security and privacy concerns, competition in the global market, and the extraterritorial ramifications of foreign regulations, demanding significant and flexible policy responses. Accordingly, strong data governance should be a prerequisite for privacy protection and public trust. U.S. policymakers should advocate establishing a single federal framework for advanced data regulation. This would help reduce inconsistent regulations and strengthen law enforcement in the existing international standards and best practices. Drawing lessons from international experiences, such as in the E.U. or the Asia-Pacific region, establishing a clear legal framework and transparent data governance will be vital for global digital exchange in both home and international activities. Finally, to safeguard regulatory dominance and set new digital standards, cooperation in international forums will be necessary as global competition, particularly with China and the E.U., intensifies.

References

- [1] Kuteesa K N, Akpuokwe C U, Udeh C A. Theoretical perspectives on digital divide and ICT access: Comparative study of rural communities in Africa and the United States. *Computer Science & IT Research Journal*, 2024, 5(4): 1045.
- [2] Sayem A, Biswas P K, Khan M M A, et al. Critical barriers to Industry 4.0 adoption in manufacturing organizations and their mitigation strategies. *Journal of Manufacturing and Materials Processing*, 2022, 6(6): 136.
- [3] Cetin M B. Evaluating the effects of digital privacy regulations on user trust. *arXiv*, 2024.
- [4] Chukwurah E G. Proactive privacy: Advanced risk management strategies for product development in the U.S. *Computer Science & IT Research Journal*, 2024, 5(4): Article 1047.
- [5] Chen P, Yan Z, Wang P. How can the digital economy boost the performance of entrepreneurs? A large sample of evidence from China's business incubators. *Sustainability*, 2023, 15(7): 789.
- [6] Adelakun B O, Nembe J K, Oguejiofor B B, et al. Legal frameworks and tax compliance in the digital economy: A finance perspective. *International Journal of Advanced Economics*, 2024, 6(3): 900.
- [7] Krismajayanti N P A, Darma G, Mahyuni L P, et al. Drivers, barriers and key success of digital transformation on SMEs: A systematic literature review. *Journal of Accounting and Strategic*

Finance, 2024.

[8] Lokuge S, Duan S X. Towards understanding enablers of digital transformation in small and medium-sized enterprises. arXiv, 2021.

[9] Takyi K N, Gavurová B. Unveiling the mediating nexus of digital transformation on digital leadership and enterprise performance in manufacturing firms. European Conference on Management Leadership and Governance, 2023.

[10] Pham T T H, Ngoc T T B, Cuong D M, et al. Digital skills of human resources: Exploratory research of innovations in enterprises. HighTech and Innovation Journal, 2024.

[11] Hokmabadi H, Rezvani S M, De Matos C A. Business resilience for small and medium enterprises and startups by digital transformation and the role of marketing capabilities: A systematic review. Systems, 2024, 12(6): 220.

[12] Mahida A. A comprehensive review on ethical considerations in cloud computing: Privacy, data sovereignty and compliance. Journal of Artificial Intelligence & Cloud Computing, 2022.

[13] Pearce H. Big data and the reform of the European data protection framework: An overview of potential concerns associated with proposals for risk management-based approaches to the concept of personal data. Information & Communications Technology Law, 2017, 26: 312–335.

[14] Wu X. Technology, power, and uncontrolled great power strategic competition between China and the United States. China International Strategy Review, 2020, 2: 99–119.

[15] Zúñiga N, Datta Burton S, Blancato F, et al. The geopolitics of technology standards: Historical context for US, EU and Chinese approaches. International Affairs. Advance online publication, 2024.

[16] Chun J, Schröder de Witt C, Elkins K. Comparative global AI regulation: Policy perspectives from the EU, China, and the US.

[17] Weritz P. Hey leaders, it's time to train the workforce: Critical skills in the digital workplace. Administrative Sciences, 2022, 12(3): 94.