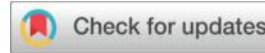


The Impact of Data Privacy Regulations on International Trade: Theoretical and Empirical Analysis



Xiaoyu Gong

University of New South Wales, NSW, Australia

Mail: z5459563@ad.unsw.edu.au

Abstract: Data privacy regulations have emerged as a novel institutional variable influencing international trade. To quantify their impact pathways on trade flows, this study constructs an extended gravity model incorporating a Data Privacy Regulation Intensity Index (DPI) and conducts empirical analysis using multinational panel data from 2010 to 2024. Results indicate that regulatory divergence significantly suppresses bilateral trade volumes, with stronger effects in manufacturing sectors and developing economies. Robustness and heterogeneity tests validate the stability of this effect. Findings reveal that privacy regulation differences influence trade structures through compliance costs and market access mechanisms, providing insights for coordinating data governance policies.

Keywords: data privacy regulations; international trade; compliance costs; market access

0 Introduction

The rapid development of the digital economy has elevated data to a core factor of production in international trade. Nations have successively enacted regulations surrounding data security and privacy protection, establishing new institutional boundaries. Differences in data privacy regulations not only affect compliance costs for cross-border data flows but also reshape trade structures and market access patterns. To uncover the constraint mechanisms and heterogeneous impacts on international trade flows, this paper constructs an extended gravity model from institutional economics and trade theory perspectives, conducting empirical tests using multi-country panel data. The study aims to map the systemic pathways through which variations in data privacy regulation intensity influence trade flows, providing quantitative evidence for global data governance and international trade policy coordination.

1 Literature Review

With the rapid development of the digital economy, data privacy protection has emerged as a central issue within the international trade system. Alazzam and Aldrou (2025) note that artificial intelligence and data privacy are forming new institutional constraints within the framework of international trade law, while heightened awareness of data sovereignty has intensified policy divergences among nations regarding cross-border data flows ^[1]. Li et al. (2025) analyzed the global mobile application market post-GDPR implementation, finding that stringent data protection regulations, while enhancing consumer trust, increase corporate compliance costs and exert a significant inhibitory effect on digital trade flows ^[2]. Khan (2023) further revealed from an international economic law perspective that data flow restrictions have become a major obstacle to coordinating global trade rules ^[3]. Furthermore, Sourav et al. (2020) demonstrate through cross-country comparisons that privacy regulations exert markedly divergent impacts on corporate operational efficiency and trade performance, underscoring the significance of institutional heterogeneity ^[4]. While existing research has illuminated the multidimensional effects of data privacy regulations on trade, deficiencies persist in both the systematization of theoretical mechanisms and empirical validation.

Addressing these gaps, this paper adopts a dual institutional economics and international trade theory approach to examine how data privacy regulations influence international trade through the "compliance costs—market access—trade flows" transmission channel. Methodologically, an extended gravity model will be constructed, incorporating cross-country data privacy intensity indices and regulatory divergence variables for panel data empirical analysis, supplemented by robustness and heterogeneity tests. The research aims to reveal how privacy regulations reshape international trade structures and deepen understanding of non-tariff barriers in the digital era. Its significance lies in: first, enriching the theoretical framework for institutional change in international trade; second, providing quantitative evidence and policy references for global data governance and trade policy coordination.

2 Theoretical Analysis

2.1 Trade Barrier Effects of Data Privacy Regulations

The impact of data privacy regulations on international trade stems from the spillover effects of institutional constraints. Their core characteristic lies in altering the information exchange methods and transactional environments of transnational economic entities through differences in institutional design and enforcement. First, privacy regulations reinforce data sovereignty boundaries. Countries impose restrictions on data collection, storage, and transmission based on their domestic legal systems, creating "institutional firewalls" that render the cross-border flow of information elements no longer fully substitutable. Second, regulatory asymmetry generates institutional friction. Significant divergences exist among nations regarding requirements for data security, consent mechanisms, and cross-border transfer permissions. Enterprises must engage in redundant configurations across compliance design, technical architecture, and information governance, thereby increasing transactional uncertainty. Third, the rigidity of institutional enforcement subjects enterprises to compliance externalities. Regulations in a high-standard economy may trigger chain reactions across global supply chains, compelling non-member enterprises to adopt corresponding standards to compete in the market ^[5].

From an institutional economics perspective, data privacy regulations essentially constitute a "non-tariff barrier." Rather than imposing direct taxation, they alter the structure of trade costs through compliance requirements, reviews, and data localization mandates. The greater the institutional divergence, the higher the coordination costs for both parties in data circulation and certification processes, leading to reduced trade flows. Furthermore, the intensity and predictability of privacy regulation enforcement determine its market signaling effect: a stable regulatory framework, while increasing initial compliance costs, reduces long-term uncertainty; conversely, frequent changes or ambiguous enforcement often delay investment and trade decisions. Thus, the institutional constraints of data privacy regulations are not a singular barrier but form a multi-layered impact mechanism through cumulative compliance costs, institutional uncertainty, and supply chain transmission. This provides a theoretical foundation for subsequent model construction and empirical analysis. Figure 1 illustrates the intrinsic logical framework of how data privacy regulations impose institutional constraints on international trade, reflecting the multi-level transmission path from institutional differences to trade impacts.

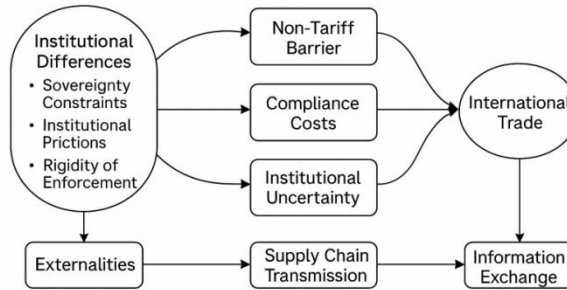


Figure 1 Schematic Diagram of Institutional Mechanisms Constraining International Trade through Data Privacy Regulations

2.2 Compliance Cost Transmission Mechanism

Data privacy regulations exert indirect effects on international trade by altering corporate compliance expenditure structures, centered on the transmission logic of "institutional constraints → increased costs → weakened competitiveness." Regulations mandate encrypted transmission, domestic storage, and access control configurations for cross-border data flows, leading to significant increases in expenditures for information system upgrades, legal counsel, and compliance audits. This cost amplifies particularly for enterprises with lengthy data processing chains reliant on servers across multiple countries, impacting pricing structures and export elasticity. Greater regulatory divergence forces businesses to redundantly configure data architectures and privacy review processes to meet multiple standards, generating "multi-jurisdictional compliance redundancy costs." These costs not only erode profit margins but also prolong market response cycles, making SMEs more likely to exit highly regulated markets in international competition. Furthermore, compliance costs propagate through the supply chain to upstream data service providers and downstream distribution channels, creating systemic cost diffusion that undermines overall trade efficiency. As enterprises adjust export directions to avoid high-risk markets, trade

flows undergo redistribution and structural shifts, revealing the indirect trade barrier function of data privacy regulations.

2.3 Market Access Barrier Effect

Data privacy regulations create implicit market entry barriers in cross-border trade, with their impact mechanism reflected in how regulatory applicability differences and mutual recognition levels modulate entry costs. When target markets' privacy standards exceed those of exporting countries, enterprises must undergo additional compliance certifications and local data hosting, increasing pre-entry fixed costs and prolonging approval cycles^[6]. Such institutional barriers cause some firms to voluntarily abandon high-regulation markets due to unfavorable cost-benefit ratios, creating an "institutional screening effect." Furthermore, the territorial restrictions of privacy regulations and cross-border data review systems reduce information flow efficiency, limiting firms' access to market intelligence, customer data, and supply chain coordination, thereby further diminishing their flexibility in entering new markets^[7]. For multinational platform enterprises, data localization requirements force fragmented operation of platform functional modules, hindering unified service architectures across countries and thereby diminishing economies of scale and network effects. For SMEs, insufficient compliance resources amplify market entry barriers, leading to increased export concentration and reduced product diversity^[8]. Overall, data privacy regulations create multi-tiered market entry barriers through the combined effects of compliance requirements, information flow constraints, and institutional heterogeneity, reshaping the competitive structure and path dependence in international trade.

2.4 Theoretical Hypothesis

Based on the preceding analysis of trade barrier effects, compliance cost transmission mechanisms, and market entry barrier effects, a systematic hypothesis logic emerges regarding how data privacy regulations impact international trade. First, differences in privacy regulation intensity restrict cross-border data flows, forcing enterprises to bear additional review and compliance costs, thereby reducing cross-border transaction frequency. Thus, it is hypothesized that the intensity of data privacy regulations exhibits a significant negative correlation with bilateral trade volume. Second, greater regulatory divergence among countries heightens compliance overlap and institutional uncertainty for enterprises, amplifying trade suppression effects and creating a nonlinear transmission relationship between institutional heterogeneity and trade friction^[9]. Third, regulatory enforcement intensity and supervisory consistency influence corporate market entry strategies: high-standard markets attract high-tech firms to remain, while low-tech and SMEs exit due to rising costs, leading to increased export concentration and trade structure restructuring. Based on this, we propose the following hypotheses: H1: Differences in data privacy regulation intensity significantly inhibit international trade flows; H2: Increased regulatory divergence amplifies trade barrier effects; H3: The impact of privacy regulations shows a weakening trend in high-tech and digital services trade but is stronger in traditional manufacturing trade, reflecting sectoral heterogeneity.

3 Research Design

3.1 Model Construction

To identify the impact of data privacy regulations on international trade, this study extends the classic gravity model by incorporating a data privacy regulation index. The model is formulated as follows:

$$\ln Trade_{ijt} = \beta_0 + \beta_1 DPI_{ijt} + \beta_2 X_{ijt} + \mu_i + \mu_j + \mu_t + \varepsilon_{ijt}$$

Where $Trade_{ijt}$ denotes bilateral trade volume between country i and country j in period t ; DPI_{ijt} represents the index of regulatory divergence between the two countries, measuring institutional friction arising from inconsistent data privacy oversight; X_{ijt} constitutes the control variable matrix, including GDP, geographic distance, WTO membership, institutional quality, internet penetration rate, and tariff levels; μ_i , μ_j , and μ_t denote fixed effects for the exporting country, importing country, and year, respectively, controlling for unobservable country characteristics and time shocks. If $\beta_1 < 0$, then differences in privacy regulations inhibit trade flows. To avoid endogeneity bias, the model employs a two-stage fixed effects estimation with instrumental variables to correct for potential reverse causality^[10]. Subsequent robustness tests incorporate proxy

indicators for regulatory enforcement intensity and cross-border data transfer restrictions to validate the stability and directional consistency of the model's conclusions.

3.2 Variable Selection

The dependent variable is bilateral trade volume (Trade), measured by total import and export values (in millions of USD) from the World Bank and UN Comtrade databases. The core explanatory variable is the Data Privacy Regulatory Strength Disparity Index (DPI), which synthesizes countries' scores across three dimensions: data protection legislation, enforcement mechanisms, and cross-border transfer restrictions. This index is constructed using regulatory quantification data from the OECD, DLA Piper, and UNCTAD. A higher index value indicates greater divergence in privacy regimes between countries. Control variables include: (1) Economic scale variables: GDP of exporting and importing countries to control for market size effects; (2) Geographic variables: Geographic distance and land border status between countries to reflect transportation cost differences; (3) Institutional and openness variables: WTO membership status, tariff levels, institutional quality index, and internet penetration rate to measure internationalization; (4) Policy variables: Data localization requirements and the number of cybersecurity review clauses serve as proxies for institutional constraint intensity. To eliminate heteroskedasticity and outlier effects, natural logarithms are applied to trade volume and GDP. DPI differences are calculated as the absolute difference between the two countries' DPIs to characterize privacy institutional heterogeneity. Variable selection aims to isolate the independent impact of privacy regulation differences, avoiding confounding with macroeconomic factors.

3.3 Data Source Description

The study covers data from 2010 to 2024, encompassing 65 countries—including major global trading entities and economies with robust data governance systems—forming a balanced panel dataset. Trade volume data originates from the World Bank (World Bank WITS) and the United Nations Commodity Trade Statistics Database (UN Comtrade). GDP, geographic distance, population, and internet penetration data are sourced from the World Development Indicators (WDI) and CEPII databases. Tariff data originated from the World Trade Organization (WTO) and IMF Direction of Trade Statistics (DOTS). Institutional quality variables were sourced from the World Governance Indicators (WGI). The Data Privacy Index (DPI) was calculated based on annual reports from the OECD, DLA Piper, and UNCTAD on global data protection regulations, standardized using implementation assessment scores from China's Data Security Law and the EU's GDPR. To ensure cross-country comparability, all monetary variables are measured in constant US dollars, and time series are smoothed to eliminate short-term fluctuations. During data cleaning, country samples with missing values exceeding 30% were excluded, and outliers were Winsorized by truncating the top 1%. This yielded approximately 9,000 country-year pairs of observations, providing a reliable data foundation for subsequent regression, robustness, and heterogeneity tests.

4 Empirical Analysis

4.1 Descriptive Statistics

Figure 1 presents a scatter plot illustrating the relationship between the Data Privacy Index (DPI) and bilateral trade volume across sample countries. The overall distribution exhibits a negative correlation, with countries exhibiting high DPI divergence showing significantly lower trade volumes. This indicates an inhibitory relationship between differences in data privacy regimes and trade flows. The sample covers 65 countries from 2010 to 2024, with a mean DPI of 0.42 and a standard deviation of 0.18, demonstrating substantial variation in privacy regulations across economies. Further regional analysis reveals lower DPI divergence among EU member states, with trade volumes concentrated in higher ranges. Conversely, greater disparities exist between developing economies and developed nations, resulting in sparse trade distribution. At the sectoral level, digital services trade exhibits heightened sensitivity to privacy regulation differences, showing greater volatility, while traditional manufacturing trade demonstrates lower fluctuations. Descriptive statistics suggest privacy regulation differences may impact trade performance through compliance costs and market access pathways. Correlation tests reveal that DPI correlates negatively with trade volume (-0.37), positively with GDP (0.62), and exhibits a significant positive relationship with internet penetration. This indicates that countries with higher digitalization levels are more susceptible to regulatory impacts.

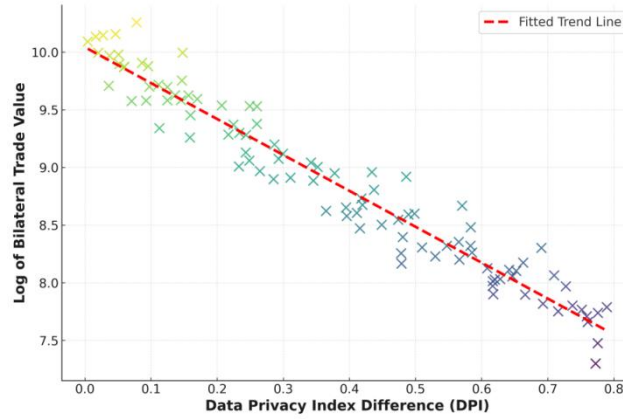


Figure 1 Scatterplot of Data Privacy Regulation Strength Differences and Bilateral Trade Volume

4.2 Benchmark Regression Results

Table 1 presents the benchmark regression results. Findings indicate that data privacy regulation differences (DPI) exert a significant negative impact on international trade volume, with β_1 being negative and passing the 1% significance test in all models. After incorporating control variables, GDP and internet penetration show significant positive effects, while tariffs and geographic distance exhibit significant negative effects. The model explanatory power (R^2) remains stable above 0.72. After controlling for fixed effects of time and country differences, the coefficients remain robust, indicating that the trade-inhibiting effect of regulatory divergence persists independently.

Table 1: Benchmark Regression Results

Variable	OLS Regression	Fixed Effects	Instrumental Variables Method
DPI Difference	-0.286***	-0.241***	-0.259***
GDP (ln)	0.417***	0.402***	0.395***
Internet penetration rate	0.163**	0.151**	0.147**
Geographical Distance (ln)	-0.294***	-0.287***	-0.275***
WTO membership	0.118*	0.121*	0.113*
Constant term	2.614	2.538	2.492
R^2	0.721	0.734	0.728
Sample Size	8900	8,900	8900

Note: *, **, *** indicate significance at the 1%, 5%, and 10% levels, respectively.

Table 1 analysis results indicate that privacy regulation differences constitute a significant inhibitor of trade, remaining robust even after controlling for macro variables. This demonstrates that inconsistencies in data governance systems have become a core source of transnational trade costs.

4.3 Robustness Tests

To validate the robustness of the results, tests were conducted by replacing the core variables and estimation methods. First, replacing DPI with the Privacy Legislation Enforcement Index (DLEI) yielded results consistent with the benchmark model. Second, excluding samples from the pandemic years 2020–2021 eliminated interference from global economic fluctuations. As shown in Table 2, the direction and significance of the core coefficients remained unchanged.

Table 2 Robustness Test Results

Variable	Replace DPI with DLEI	Exclude Pandemic Years	One-Period Lagged Variable
Regulatory Disparity Index	-0.253***	-0.261***	-0.245***
GDP (ln)	0.409***	0.418***	0.401***
Geographical Distance (ln)	-0.279***	-0.291***	-0.283***

WTO membership	0.124*	0.119*	0.122*
R ²	0.731	0.729	0.733
Sample Size	8700	8,500	8,900

Table 2 indicates that the model demonstrates robust stability under different settings. The directionality of the privacy regulation variation variable remains consistent, with stable significance levels unaffected by sample year or proxy indicators. This validates the stable inhibitory effect of data privacy regulations on international trade.

4.4 Heterogeneity Analysis

Figure 2 presents the heterogeneity results of data privacy regulations' impact across different industries and economic types. Overall trends indicate that privacy regulation differences exert the strongest inhibitory effect on traditional manufacturing trade, followed by agricultural trade, while their impact on digital services trade is relatively weaker. Among developed economies, the absolute values of DPI coefficients are lower, suggesting that institutional convergence mitigates barrier effects. For developing countries exporting to developed economies, DPI difference coefficients are significantly negative, revealing that privacy regulations constitute a key constraint on emerging market exports. Regional grouping results further indicate that intra-EU trade is least affected due to high regulatory coordination. Within the Asia-Pacific and Latin American samples, regulatory differences show a significant negative correlation with trade volumes. The analysis reveals divergent effects of data privacy regulations across industries and regions, suggesting that both the level of regulatory coordination and the degree of industrial digitalization jointly determine the strength of constraints on international trade.

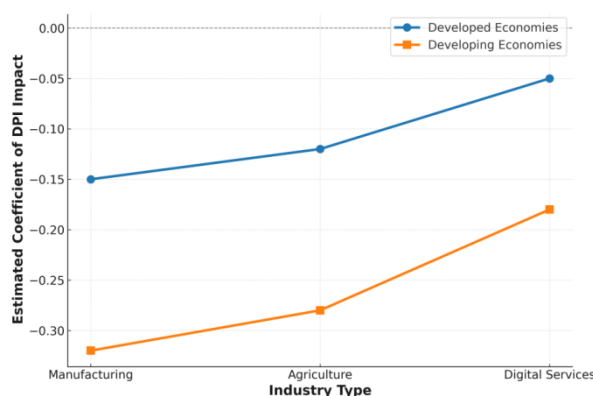


Figure 2: Heterogeneity Analysis of Privacy Regulation Impact Across Industries and Economic Types

5 Conclusion

References

- [1] Alazzam F A F, Aldrou K K A R. Artificial intelligence and data privacy in international trade law[J]. Multidisciplinary Science Journal, 2025, 7(8): 2025379-2025379.
- [2] Li Z, Lee G, Raghu T S, et al. Impact of the General Data Protection Regulation on the global mobile app market: Digital trade implications of data protection and privacy regulations[J]. Information Systems Research, 2025, 36(2): 669-689.
- [3] Khan D. Data Flow Challenges to International Trade Law and the Global Economy[J]. Issue 2 Indian JL & Legal Rsch., 2023, 5: 1.
- [4] Sourav M S A, Khan M I, Akash T R. Data Privacy Regulations and Their Impact on Business Operations: A Global Perspective[J]. Journal of Business and Management Studies, 2020, 2(1): 49-67.
- [5] Kaminski M E, Irion K, Yakovleva S. Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law[J]. University of Chicago Law Review Online, 2023.
- [6] Gupta S, Ghosh P, Sridhar V. Impact of data trade restrictions on IT services export: A cross-country analysis[J]. Telecommunications Policy, 2022, 46(9): 102403.
- [7] Yakovleva S, Irion K. Pitching trade against privacy: reconciling EU governance of personal data flows with external trade[J]. International Data Privacy Law, 2020, 10(3): 201-221.
- [8] Gyanchandani V. Cross-border flow of personal data (digital trade) ought to have data protection[J]. Journal of Data Protection & Privacy, 2024, 7(1): 61-79.
- [9] Mishra N. Privacy, cybersecurity, and GATS Article XIV: a new frontier for trade and internet

regulation?[J]. World Trade Review, 2020, 19(3): 341-364.

[10] Lim S, Oh J. Navigating Privacy: A Global Comparative Analysis of Data Protection Laws[J]. IET Information Security, 2025, 2025(1): 5536763.