Factors Influencing Data Protection on Global Trade

Dayang Nur Melyssa Aleya Aziz[1], Maizatul Saadiah Mohamad[2], Roszi Naszariah Nasni Naseri[3], Suhaida Mohd Amin[4], Noraeffa Md Taib[5], Harniyati Hussain[6], Joeaiza Juhari[7], Khaizie Sazimah Ahmad[8], Ali Murtadho[9], Nurfatoni[10]

[2,3,6,7,8]Faculty of Business and Management, UiTM Cawangan Melaka, Kampus Alor Gajah, Melaka, Malaysia

[1,4,5]Faculty of Business and Management, UiTM Cawangan Melaka, Kampus Bandaraya, Melaka, Malaysia

[9,10]Faculty of Economy and Islamic Business UIN Walisongo, Indonesia

DOI: https://dx.doi.org/10.47772/IJRISS.2025.923MIC3ST250011

Received: 12 August 2025; Accepted: 20 August 2025; Published: 24 October 2025

ABSTRACT

Due to the growth of the internet and e-commerce, many organizations and customers have dealt with risks resulting from leakage, sharing of customers' data, and enforcement of laws governing data protection. This paper is an attempt to examine impact of e commerce platform policies, user privacy preferences and institutional quality with respect to data protection in global trade. Though measures like GDPR and CCPA that have been put in to curb use of data have been put in to practice, their efficiency differs from one platform to another as well from one jurisdiction to the other. Lack of uniformity in the corporate data policies, consumer awareness, and inadequate enforcement of regulatory policies become a hurdle in the process of maintaining the data protection policy. Thus, this research is to assess the effects of the e- commerce platform policies, user privacy preferences, and institutional quality on data protection in global trade.

Keywords: Data Protection, E-commerce Policies, User Privacy, Institutional Quality, Global Trade

INTRODUCTION

Research Background

Currently, the ability to freely transmit information across borders is essential for conducting international commerce. Additionally, it makes it easier for businesses to operate and acquire the necessary goods and markets to drive economic growth and innovation. However, worries about data security and privacy have contributed to the surge in the volume of bandwidth being exchanged. Anupam Chander (2013) claims that a new geography of privacy and trade is developing, with data privacy rules focusing on global trade.

Current data protection regulations, such as the General Data Protection Regulation (GDPR) of the European Union, have made doing business internationally more difficult. The primary goals of the GDPR, which went into effect in 2018, are to safeguard personal information and uphold the rights of individuals in the EU. Despite how important these rules are for protecting consumers, they present a variety of difficulties for foreign businesses that must adhere to several legal frameworks and laws. According to (Elisabeth Meddin, 2020), the GDPR may infringe many terms of the General Agreement on commerce in Services (GATS) and has restrictive impacts on commerce.

Problem Statement

But because privacy rules vary from one nation to another, there is a chance that regulations may become fragmented, particularly when it comes to cross-border data transfers. These regulations, which differ for trading companies in different countries, raise operating costs and restrict access to new markets. As

governments and businesses strive to integrate the use of data in commerce globally, it is imperative to look at the elements that affect data protection in global trade. A comprehensive approach to data management is necessary since different data models and rules impact the volume of commerce in digital services, according to Martina Ferrcane (2021).

It is concerning because there is a greater chance of data abuse as e-commerce usage increases. Although well-known online marketplaces like Amazon, eBay, and others are supposed to safeguard customer data, privacy violations and cybercriminals are undermining consumer trust. Therefore, even with regional and international laws like the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR), there is an issue with the low efficacy of data protection laws. Many users report instances of identity theft and illegal information exposure, which raises questions about the platforms' policies and their ability to enforce them (Brown, J., 2021).

The varying degrees of dedication to security rules by e-commerce platforms are among the causes of this ongoing issue. Although some platforms have strong data protection features built into their systems, others could take advantage of legal loopholes to restrict user access over their data. Furthermore, user privacy preferences exacerbate the situation. While some users will take every precaution to preserve their privacy and prevent other parties from accessing their data, others may unintentionally give their login credentials to third parties. This discrepancy in user understanding and involvement may make data protection even more problematic (Jones & Lee, 2019).

The examination of other important variables also shows that, while platform regulations and user preferences have a role in how successful data protection systems are, institutional quality is a key determinant of system efficacy. Due to variations in legal protection regimes and how they are enforced, protection standards also vary throughout nations. As previously said, such nations have comparatively lax regulatory enforcement, which results in even worse data privacy safeguards, leaving users uneasy. However, fewer research looked at how platform policies, user preferences, and institutional quality relate to each other and how they affect e-commerce data protection.Consequently, there is a gap in the literature that necessitates the use of a conceptual framework in this study in order to comprehend the dynamic interplay of the factors.

Urgency to Conduct Study

As digitization results in enormous trans-border information transfers, protecting such data has become crucial to international trade. Despite predictions from the OECD (2020) that data flows have increased more than 45 times in the past decade, the data contributes significantly more to the global economy's GDP than the sale of tangible commodities. Despite the remarkable rate of adoption in recent years, only 40% of nations globally have enacted complete data protection laws, which has led to a fragmentation of legal norms. For the protection of international data flow, which is essential to trade liberalization, this mismatch necessitates sensible, coordinated data protection measures (Smith, 2019).

The issue is made worse by the fact that data protection laws are still inconsistent across different jurisdictions. With its General Data Protection Regulation (GDPR), the European Union (EU) has set the standard, affecting almost 25% of global businesses by 2020 (Jones & Patel, 2020). However, just 10% of countries in Sub-Saharan Africa, including the United States, have data protection laws, and many parts of the world still lack them (Kumar, 2018). Because rules differ between nations, the existing regulatory environment becomes problematic when businesses conduct business internationally.

International trade is significantly impacted by data protection laws, particularly in the technology and commerce sectors. According to a World Bank analysis from 2021, countries with stronger data privacy regulations attract more foreign direct investment (FDI) than those with weaker systems; FDI can increase by up to 25% when data is properly safeguarded. However, as the EU-US Privacy Shield conflict showed, protecting personal information can result in the creation of trade barriers and have negative economic effects (Adams, 2020). Therefore, while having strong data privacy laws is ideal for facilitating data in international business, there are drawbacks, such as the need to ensure free and effective cross-border trade.

Research Objective

Research Objective 1:

To determine the relationship between e commerce platform policies and data protection on global trade.

Research Objective 2:

To determine the relationship between user privacy preferences and data protection on global trade.

Research Objective 3:

To determine the relationship between institutional quality and data protection on global trade.

Research Questions

Research Question 1:

Is there any significant relationship between e-commerce platform policies and data protection on global trade?

Research Question 2:

Is there any significant relationship between user privacy preferences and data protection on global trade?

Research Question 3:

Is there any significant relationship between institutional quality and data protection on global trade?

LITERATURE REVIEW

Overview of Factors Influencing Data Protection on Global Trade

Data problems have become a major worry for international industry, consumers, and bureaucracy as e-commerce has expanded dramatically in recent years. Concerns about the cross-border movement of personal data are raised by the amount of digital transactions that expose consumers to risks like cyber-attacks, identity theft, and illegal access and sharing of user data. Therefore, the effectiveness of the protective data is dependent on elements that make up the global trade environment when employing the measures that governments and enterprises implement to improve cybersecurity (International Trade Council, 2023)

This article focuses on three data protection variables and looks at how e-commerce platform policies, user privacy preferences, and institutional quality relate to each other. Because their security standards differ, e-commerce sites have different policies even though they are more responsible for establishing data protection policies. However, consumer privacy regulations about the use of their information are influenced by user privacy preferences, and some people prefer privacy above security, or vice versa. The quality of institutions has an impact on the quality of laws and how they are implemented in relation to the data protection standards that have been established in different regions.

In light of these concerns, this conceptual paper suggests a methodology for examining pertinent variables and how they affect global data protection. Making better policies, raising consumer awareness, and increasing the effectiveness of legislation all depend on an understanding of these relationships. Given the existing gaps in the literature, this study adds to discussions on how to improve digital security in international commerce.

Regulatory Frameworks & Adequacy Decisions

Jurcys, Compagnucci, and Fenwick (2024) propose a user-held data model, utilizing personal data clouds to minimize cross-border data transfers and compliance risk after GDPR's Schrems II ruling. This model decentralizes storage, enhancing both legal compliance and end- user autonomy (Jurcys et al., 2024). The EU–

US Data Privacy Framework, adopted in July 2023, reinstated an adequacy decision enabling data flows from the EU to the US. Yet, European Parliament members and privacy advocates continue challenging its effectiveness, citing concerns over U.S. surveillance laws and insufficient protections (EU Commission, 2023; McCabe & Stevis-Gridneff, 2022; Sovereign Digital Rights NGOs, 2023) Wikipedia.

Trade Agreements & Digital Trade Norms

Setting a standard for digital trade arrangements with Asia-Pacific partners, the EU-Singapore Digital Trade Agreement was signed in July 2024 with the goals of promoting unfettered data flows, e-signatures, consumer protections, and limitations on code localization (Reuters, 2024). Major regional trade agreements such as the CPTPP, USMCA, and RCEP have e-commerce chapters that prohibit forced localization and promote paperless trade (Goldsmith and Gao, 2024). However, obstacles to unified implementation are still created by regional policy differences, particularly between models supported by the US, China, and the EU (Goldsmith & Wu, 2006; Gao, 2024).

Data Localization & Trade Disruption

According to econometric evidence presented by Shuzhong, Sishi, and Peng (2024), data policy restrictions have a considerable negative impact on Chinese cross-border e-commerce exports, particularly for high-tech and distinctive items. These effects are more pronounced in markets where data policy is more dominant (Ma et al., 2024). According to Wikipedia, data localization—which is frequently motivated by national sovereignty and surveillance goals—requires that data be held locally before being transferred internationally. Although it might safeguard privacy, it raises operating expenses and interferes with cloud economics (Wikipedia, 2025).

Cybersecurity, Trust & Compliance

Inconsistent encryption standards, an increase in cyberattacks, and sector-specific regulations (such as the GDPR, China's PIPL, and the U.S. CLOUD Act) pose significant risks and obstacles for multinational corporations, according to Paganini (2025), who describes the difficulties in complying with cross-border cybersecurity regulations. According to Chatzigiannis et al. (2023), privacy-enhancing technologies in financial data sharing, such as encrypted protocols and secure multi-party computation, are essential for balancing data flows and privacy, particularly in light of growing regulatory restrictions like the FCRA and GDPR.

Geopolitics & Digital Sovereignty

Beattie (2024) reports middle-income countries (e.g., India, Indonesia, South Africa) pushing to end the WTO moratorium on digital service tariffs, reflecting geopolitical leverage and signalling a potential shift toward protectionism (Beattie, 2024). The Cyberspace Administration of China (2024) introduced revised data export rules that exempt non-sensitive trade data from security reviews—extending certificate validity and improving clarity—while still enforcing strict oversight of "important data" to maintain sovereignty (Reuters, 2024).

Emerging Systems for Cross-Border Compliance

Zhuang et al. (2024) designed CBCMS, a real-time compliance management system that uses a Policy Definition Language to harmonize diverse legal frameworks, achieving high compliance accuracy (F1 = 97.32%) and low latency (6–13 ms), marking a breakthrough in cross-jurisdictional data compliance (Zhuang et al., 2024).

In the past five years, five intersecting factors—regulatory adequacy, digital trade agreements, localization mandates, cybersecurity, and geopolitical sovereignty—have shaped the evolving landscape of data protection in global trade. While technological and policy mechanisms (e.g., CBCMS, personal data clouds) create pathways to harmonization, sustained progress depends on multilateral alignment, such as through WTO digital trade negotiations or APEC frameworks.

E-Commerce Platform Policies

Online marketplaces are increasingly held responsible for data governance—not only for user data handling but also for compliance with customs and product safety. The European Union's Digital Services Act (DSA) and Digital Markets Act (DMA) (enforced 2023–2024) require platforms (e.g., Amazon, AliExpress, Shein) to ensure transparency in algorithmic operations, user data use, and to share necessary information with authorities before goods enter the EU (Cookie-Script, 2025; Wikipedia, 2025). In July 2024, some 80 WTO members agreed on global e-commerce rules encompassing digital documentation, e-signatures, anti-fraud protections, spam limits, and personal data safeguards—but this framework still excludes the U.S. and remains unratified under WTO law (Reuters, 2024). These developments show how platform policies are becoming integral to global trade compliance. Implication for data protection: Platform-level mandates enforce stricter data governance, embedding privacy via design in trade infrastructure. Future research should assess how these rules affect small vs. large e-commerce firms globally.

User Privacy Preferences

Data policy implementation is increasingly influenced by user opinions. 64% of consumers want personalized experiences, yet 53% are very concerned about data privacy; only 33% trust businesses to use their data responsibly, according to a 2025 global poll with over 23,000 respondents (Green, Scutt, & Quaadgras, 2025). A study by Jha et al. (2024) illustrates the function of consent mechanisms by showing how design affects user consent behavior. One-click "reject all" banners cause 60% of users to opt out, whereas more intricate interactions result in up to 90% of users accepting. According to a different study conducted in Malaysia, Ghana, and the Netherlands (Cetin, 2024), user trust and engagement are greatly impacted by cultural and regulatory contexts (GDPR in the Netherlands; laxer enforcement in Ghana; and reliance on platform security in Malaysia), highlighting preferences as a driver of data protection.Implication for global trade: E-commerce firms must balance personalization benefits with strong consent regimes and transparent privacy design to build trust across diverse consumer bases. Future work could explore how regional UX preferences intersect with trade-driven compliance.

Institutional Quality

The effectiveness of data protection measures is significantly impacted by the strength of institutions, including regulatory clarity, governance quality, and enforcement mechanisms. By establishing a formal governance framework for interagency data exchange, Malaysia's 2025 Data Sharing Act enhances standards and accountability (Securiti, 2025). To illustrate how institutional improvements, reinforce privacy governance, South Korea's PIPC updated its standards in April 2025 to increase transparency in the processing of personal information. These revisions clarified consent, data usage, and AI-based judgments (Securiti, 2025). There is empirical evidence linking policy implementation capacity to governance quality, as evaluated by metrics such as the Worldwide Governance Indicators. According to the World Bank (2025), nations with high scores for rule of law and institutional effectiveness are better equipped to implement cross-border data agreements. Implications for international trade: Robust institutions promote uniform enforcement of data privacy laws and cultivate confidence among trading partners. A useful avenue for future research would be to compare the results of trade compliance with nation-level governance systems (like WGI).

METHODOLOGY

Research Design

This study will employ a mixed-methods approach, combining both quantitative and qualitative techniques to investigate how different factors influence data protection practices in global trade. Quantitative: To analyses statistical relationships between variables (e.g., institutional quality and data protection effectiveness). Qualitative: To explore policy content, user perception, and platform practices in greater depth.

Data Collection Methods

Quantitative Data

i. Secondary Data Sources by World Bank's Worldwide Governance Indicators (WGI) – for institutional quality scores. UNCTAD Digital Economy Database – for e-commerce trade flows. Freedom House Internet Freedom Index – to measure data privacy and freedom of expression. Platform compliance reports (e.g., Amazon, Alibaba transparency reports).

ii. Survey (Primary Data)

The following people will receive an online structured survey: E-commerce users (from three to four countries, such as Malaysia, the Netherlands, and India). Officers of trade and compliance at multinational corporations. Survey topics will include: Perceived value of privacy, familiarity with the privacy policies of platforms, satisfaction with the way data is protected in cross-border transactions. Responses will be scored on a 5-point Likert scale.

Qualitative Data

i. Policy Analysis using Comparative analysis of major e-commerce regulations and trade agreements (e.g., GDPR, CPRA, CPTPP, DSA). Coding of legal documents and platform privacy policies using content analysis techniques.

ii. Expert Interviews

Semi-structured interviews with Data protection officers, Trade law experts, Policy-makers in digital trade.

Sampling Method

Purposive sampling for expert interviews (policy and compliance specialists). Stratified random sampling for survey distribution, ensuring demographic and regional representation (developed vs. developing economies). Sample size: Minimum of 200 survey respondents and 10–15 expert interviewees.

Data Analysis Techniques

Quantitative Analysis

Descriptive statistics to summarize survey responses. Correlation and regression analysis to examine relationships between: Institutional quality and data protection performance, User preference and platform compliance. Tools: SPSS or STATA.

Qualitative Analysis

Thematic analysis of interview transcripts and policy texts. Use of coding software (e.g., NVivo) to identify patterns related to enforcement, transparency, and privacy prioritization.

Ethical Considerations

Informed consent will be obtained from all survey participants and interviewees. Data will be anonymized and securely stored. Ethical clearance will be obtained from the host institution's research ethics board.

Proposed Theoretical Framework

Thus, from the above- mentioned relationship, the hypothesis for this study can be derived as follows:

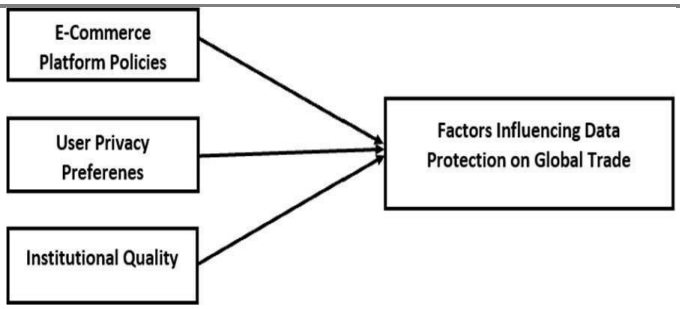

Fig. 1 Proposed Theoretical Framework of Factors Influencing Data Protection on Global Trade

H1: There will be a significant relationship between e-commerce platform policies and data protection on global trade.

H2: There will be a significant relationship between user privacy preferences and data protection on global trade.

H3: There will be a significant relationship between institutional quality and data protection on global trade.

DISCUSSION

Therefore, establishing and upholding data protection standards in the framework of global business is one of the most important effects of e-commerce platform policies. From this, we may infer that the instances of information leakage are reduced wherever platforms provide strict information protection, including the use of encryption, multiple forms of identification, and strict access to such information. However, national differences in the laws governing knowledge-sharing platforms lead to issues with enforcement and disparities in data protection. As a result, businesses in various regions are subject to various legislation, which can have a favorable or unfavorable impact on the stability of the organization's data security. This increases the likelihood of having balanced policies that build a single, replicated model to safeguard client data. Since consumer behavior and understanding determine how securely user data is kept, data protection also depends on the user's privacy preferences. This leads us to the conclusion that users who are more privacy literate tend to have better password habits, share less information, and activate security features, all of which reduce their vulnerability to online attacks. Convenience-driven consumers, on the other hand, consent to the default privacy settings or engage with unreliable sources, giving away their data. This indicates that there should be greater transparency when businesses are collecting data from customers because awareness is still a major obstacle to ensuring data safety.

The cybersecurity environment and the application of data protection rules are determined by the quality of the institution. This leads us to conclude that nations with strong laws and effective regulatory controls have lower rates of identity theft and data breaches because corporations that misuse data face penalties. However, weak institutions could lack the resources or legal authority to completely adopt reformed data protection, which leaves them vulnerable to cybercriminals. This suggests that there would be unavoidable hazards to data protection if institutional breakdowns ever increased. International cooperation is therefore essential to uniform data protection.

CONCLUSION

Privacy is a growing issue in the context of international business and commerce as the number of digital transactions rises steadily. E-commerce has experienced tremendous growth in recent years with corresponding increased risks of fraud such as theft of identity, compromised data and unauthorized disclosure of information, therefore this paper seeks to establish relevant factors that affect data security. The policies adopted by e-commerce platforms, the user preferences of privacy, and the institutional quality are thus discussed as a part of the proposal in this paper. All these factors sum up to define the extent to which consumer data is protected in cross border digital transactions. A ruling with e-commerce platforms establishes fundamental guidelines for personal data protection rules that business organizations must follow

uniformly. However, because users have a role in protecting their information, their effectiveness depends on their privacy preferences. While some people are worried about their security, others may unintentionally expose themselves to leaks due to ignorance. Furthermore, since nations with higher legal rights indices were expected to have greater e-commerce company compliance and responsibility with regard to user data, institutional quality has a substantial impact on the enforcement of data-created protection legislation. The effectiveness of data protection in global company is determined by the interdependence of these three elements.

Thus, by identifying these major factors, this conceptual paper lays theoretical groundwork for the subsequent quantitative analysis of enhancing data protection in cross-national electronic commerce. Closing the regulation gaps in online platforms, raising consumers' awareness and, strengthening the institutional crackdown are some of the possible ways to minimize risks associated with the digital trade. Future research should examine how it is possible to coordinate international effort toward the formation of coherent policies that will minimize disparities within international regulations regarding data protection.

REFERENCES

1. Acemoglu, D., Johnson, S., & Robinson, J. A. (2005). Institutions as a fundamental cause of long-run growth. Handbook of Economic Growth, 1A, 385–472.
2. Adams, L. (2020). The EU-US Privacy Shield Dispute: Economic Impacts of Conflicting Data Protection Policies. International Trade Law Review, 15(4), 200-215.
3. Bannister, F., & Connolly, R. (2015). The role of e-commerce platform policies in shaping customer behavior. Kybernetes, 44(12), 1892–1905. https://doi.org/10.1108/k-12-2015-0318
4. Beattie, A. (2024, February 22). Uncertainty dogs the global digital market. Financial Times.
5. Böhme, R., & Köpsell, S. (2010). Trained to accept? A field experiment on consent dialogs. In
6. R. Sion (Ed.), Information security and cryptology – ICISC 2009 (pp. 239–257).
7. Brown,J. (2021). Victimsof identity theft, 2021. Bureauof JusticE Statistics.
8. Cetin, M. B. (2024). Evaluating the Effects of Digital Privacy Regulations on User Trust. arXiv. Chander, A. (2013). Privacy and trade. The University of Chicago Law Review, 80(1), 221–247.https://lawreview.uchicago.edu/sites/default/files/02_Chander_ART_Final.pdf
9. Chatzigiannis, P., Gu, W. C., Raghuraman, S., Rindal, P., & Zamani, M. (2023). Privacy-enhancing technologies for financial data sharing. arXiv.
10. Choi,Y., & Kim, D. (2023). The role of e-commerce platform policies in promoting fair trade practices. Financial and Business Economics Journal, 19(2), 134-146.
11. Chowdhury, M. J. M., & Masrom, M. (2012). A review on privacy issues in the information age. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 20(4), 471–484.https://doi.org/10.1142/S0218488512400247
12. Christian Cookie-Script™. (2025). E-Commerce Compliance 2025: Digital Services Act & Platform Responsibilities.
13. Coopamootoo, K. P. L. (2020). Dis-empowerment online: An investigation of privacy-sharing perceptions and methodpreferences. https://arxiv.org/abs/2003.08990
14. Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J. H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). Privacy and data protection by design: From policy to engineering. https://arxiv.org/abs/1501.03726
15. Ferracane, M. F., & van der Marel, E. (2021). Regulating personal data: Data models and digital services trade (Policy Research
16. Working Paper No. 9596). World Bank. https://openknowledge.worldbank.org/bitstreams/0b4562ce-777f-567b-8247-9 441ec24a26c/download
17. Gellert, R. (2023). Complete and effective data protection. Current Legal Problems, 76(1), 297-330. https://doi.org/10.1093/clp/cuz017
18. Gibbs, J., Kraemer, K. L., & Dedrick, J. (2006). The definition of e-commerce platform policies: A strategic perspective. Journal of Global Information Technology Management, 9(4), 518.https://doi.org/10.1080/01972240309472
19. Green, D., Scutt, J., & Quaadgras, T. (2025). Consumer Preferences for Privacy and Personalization,

2025. Qualtrics XM Institute.
20. Gupta, I., & Singh, A. K. (2022). A holistic view on data protection for sharing, communicating, and computing environments: Taxonomy and future directions.
21. Huang, L., & Li, H. (2023). E-commerce platform policies: Regulatory frameworks and their impact on consumer behavior. Journal of Electronic Commerce Research, 24(5), 467- 484.
22. Human, S. (2022). Advanced data protection control (ADPC): An interdisciplinary overview.
23.]Islam, R., & Montenegro, C. E. (2004). The institutional determinants of economic growth: A cross-country analysis.
24. Javalgi, R., & Ramsey, R. (2001). E-commerce platform policies: A review and research agenda. International Marketing Review, 18(3), 254-275.
25. Trevisan, M., Mellia, M., Fernandez, D., & Irarrazaval, R. (2024). Privacy Policies and Consent Management Platforms: Growth and User Interactions (2013–2022).
26. Jones, K., & Lee, A. (2019). E-commerce platform policies and data security. E-Commerce Law Review, 18(4), 56-70.
27. Jones, R., & Patel, M. (2020). Data Protection and Cross-Border Data Flows in the EU: A Study of GDPR. Journal of International Law, 21(3), 78-94.
28. Jurcys, P., Compagnucci, M. C., & Fenwick, M. (2024). The future of international data transfers: Managing legal risk with a user-held data model.
29. Kapitsaki, G. M., Kounoudes, A. D., & Achilleos, A. P. (2020). An overview of user privacy preferences modeling and adoption. Proceedings of the 46th Euro micro Conference on Software Engineering and Advanced Applications (SEAA), 2020, 93 -100.
30. Kolter, J., & Pernul, G. (2009). Data mining for the detection of fraudulent financial statements. Proceedings of the 2009 IEEE Symposium on Security and Privacy, 271-285. https://doi.org/10.1109/SP.2009.28
31. Kumar, S. (2018). Regulatory Gaps in Data Protection Across Emerging Economies. International Business Review, 12(1), 112-129.
32. Lupton, D. (2022). Data protection in sociological health research: A critical narrative. Health Sociology Review, 31(2), 214-229
33. Lynskey, O. (2019). The origins and meaning of data protection. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3518386
34. Ma, S., Huang, S., & Wu, P. (2024). Data policy restrictions and cross-border e-commerce: Evidence from China. Journal of Asian Economics
35. Meddin, E. (2020). The GDPR's restriction on cross-border data flows: A violation of the General Agreement on Trade in Services? American University International Law Review,35(4), 731–766.
36. Miao, Y., Li, S., Xu, J., & Sun, X. (2022). A systematic review of privacy-preserving machine learning: From adversarial attacks to federated learning and beyond. AI, 4(3), 576– 600. https://doi.org/10.3390/ai4030034
37. Minkus, T., & Memon, N. (2014). Leveraging personalization to facilitate privacy. https://arxiv.org/abs/1406.2398
38. Molla, A., & Licker, P. S. (2011). E-commerce platform policies: A case study in the digital economy. In E-commerce and Development in the Digital Economy (pp. 73–94). Springer. https://doi.org/10.1007/978-1-4615-1467-1_5
39. Paganini, P. (2025, March 11). Cybersecurity challenges in cross-border data transfers and regulatory compliance strategies. Security Affairs.
40. Reuters. (2024, July 26). Eighty nations strike deal over e-commerce, but lack US backing
41. Reuters. (2024, July 25). EU and Singapore agree digital trade deal. Reuters.
42. Reuters. (2024, March 22). China relaxes security review rules for some data exports. Reuters.
43. Sadeh, N., Hong, J., Cranor, L., & Fette, I. (2008). Understanding and capturing people's privacy policies in a mobile social networking application. Personal and Ubiquitous Computing, 13(6), 401–412.
44. Schomakers, E.-M., Lidynia, C. (2019). Putting privacy into perspective. Comparing technical, legal, and users' view of data sensitivity.
45. Securiti. (2025, April). Privacy Regulation Roundup: Asia-Pacific Developments
46. Singh, N. (2023). Analysis of e-commerce management policies based on the current Situation

development.
47. Smith, J. (2019). The Role of Data Protection in Global Trade. Global Economics Journal, 34(2), 45-56
48. Wang, J., Li, X., & Zhang, Y. (2024). Privacy-enhancing technologies in the era of big data: A comprehensive review. Data Science and Technology, 12(4), Article 1918.
49. Watson, J., Richter Lipford, H., & Besmer, A. (2015). Mapping user preference to privacy default settings. ACM Transactions on Computer-Human Interaction (TOCHI), 22(6), Article 32, 1-20.
50. Wikipedia. (2025). Data localization. Wikipedia.
51. Wikipedia. (2025). EU–US Data Privacy Framework. Wikipedia.
52. Wikipedia. (2025, May). Digital Services Act. Retrieved from Wikipedia
53. Wikipedia. (2025, March). Data Localization. Retrieved from Wikipedia. World Bank. (2025). Worldwide Governance Indicators.
54. Zhao, X., & Zhong, Z. (2012). E-commerce platform policies and international trade: A legal perspective. Journal of World Trade, 46(3), 523-547.
55. Zhuang, Z., Lee, X., Wei, J., Fu, Y., & Zhang, A. (2024, December). CBCMS: A compliance management system for cross-border data transfer.