Hindawi
Security and Communication Networks
Volume 2022, Article ID 9517769, 12 pages
https://doi.org/10.1155/2022/9517769

Research Article

An Empirical Study of Platform Enterprises' Privacy Protection Behaviors Based on fsQCA

Yaojia Tang [1] **and Luna Wang** [1,2]

[1]*Economic Academy, Zhejiang University of Finance and Economics, Hangzhou 310018, China*
[2]*School of Shangmaoliutong, Zhejiang Technical Institute of Economics, Hangzhou 310018, China*

Correspondence should be addressed to Luna Wang; luna.wang@zufe.edu.cn

Received 2 September 2021; Revised 1 December 2021; Accepted 11 December 2021; Published 3 January 2022

Academic Editor: Rutvij Jhaveri

Firms' privacy protection strategies are affected by multiple factors. This study adopted a configurational perspective to examine how regulation policy environment, market structure, and the heterogeneity among enterprises affect their privacy protection policies. Using a fuzzy set qualitative comparative analysis of Chinese listed platform enterprises, we found that three configuration conditions were associated with enterprises formulating a privacy policy with a high level of protection and two configuration conditions were associated with enterprises formulating a privacy policy with a low level of protection. The results showed that privacy protection laws were a necessary condition to ensure that enterprises actively exercised privacy protection. Coordinated regulation systems based on the Personal Information Protection Law and industry standards are recommended as the best practice to safeguard privacy protection in China. As lack of competition can result in two polarized privacy protection strategies, regulatory policies should emphasize the balance between data protection and encouraging necessary data sharing. Furthermore, the conjunctive effect between market structure and business models affected privacy policy formulation, which suggests that the positive effects of users' rational choices in a competitive market should be further reinforced.

1. Introduction

In the digital economy, personal data are an important resource and strategic asset for an enterprise and a necessary investment for platform operation and business model innovation. The collection and commercial application of user data has boosted the quality and innovative development of online platforms. However, the value of data has propagated the malicious collection and excessive use of private data, raising an important issue that affects both user privacy and the healthy development of the digital economy. Therefore, privacy protection on digital platforms has become an important topic in regulatory policies for managing the digital economy. As the privacy protection decisions of platform enterprises are driven by various factors, research on the endogenous mechanisms behind such decisions is beneficial for governments formulating corresponding incentive-based regulatory policies.

The circumstances under which platform enterprises are more likely to formulate a user-friendly privacy policy have been a consistent focus in privacy economics. Previous studies have revealed that the privacy protection implemented by enterprises is influenced by a range of factors. Under different external and internal environmental influences, enterprises implement varying levels of privacy protection. Casadesus-Masanell and Hervas-Drane [1] focused their research on exploring the impact of competition on the implementation of enterprises' privacy protection measures and found that competition stimulated privacy protection implementation. Shapiro [2] and Mai et al. [3] asserted that when the level of privacy protection becomes an influential factor for online transaction decisions, businesses that have implemented such protection have a competitive advantage over those that have not. User demand for privacy protection has subsequently become a dimension of purchase decisions and thus another motivator

for enterprises to actively formulate privacy policies. Furthermore, Fainmesser et al. revealed that the business model influenced the type of privacy policy formulated by enterprises [4]. Ramadorai et al. determined that data-sharing behavior was associated with factors such as corporate size, market share, and technological capital, indicating that privacy protection was affected by heterogeneous factors [5]. Concerning technological capital, Juneja et al. [6] and Gupta et al. [7] discovered that technological improvement such as cyber-twin technology and image encryption could increase a firm's ability in maintaining a secure network. Existing studies focused on how individual factors influence firms' privacy protection behaviors and have revealed that some individual factors, such as the level of market competition, business model, and heterogeneous factors, could affect firms' intention to protect users' data privacy. However, as the design of incentive compatible privacy regulatory policies should consider the decision-making patterns of firms which are the result of the interactions among multiple factors, the existing findings are not meaningful enough for guiding government in formulating specific regulatory policy. In our study, we studied the factors that drive enterprises' privacy protection behaviors from an integrated perspective and formulated a comprehensive framework to analyze firms' privacy protection behaviors, thus assisting government in formulating incentive compatible privacy regulatory policies.

Online platforms are important players in privacy protection. First, they exert privacy protection in the digital economy. Second, they are subject to corresponding data protection regulations. Therefore, our study focused on online platforms and constructed an integrated analytical framework from the perspective of the policy environment, the heterogeneity among firms, and the market structure to investigate the decision-making mechanisms and factors that drive platform privacy protection. To achieve this, fuzzy set qualitative comparative analysis (fsQCA) was adopted to explore the configuration conditions of high- and low-level privacy protection policies and reveal the mechanisms that lead to variance in privacy protection policies. Theoretically, we established a framework to analyze how government regulatory policies, market environment, and enterprises' endogenous factors interact with specific enterprise decisions and why enterprises implement different privacy protection policies. Empirically, by conducting the behavioral research from the fine-grained microperspective of enterprises and applying a mixed-method (quantitative and qualitative) design, we analyzed how multiple conditions impact the formulation of privacy policy among Chinese platform enterprises and revealed some of the complex reasons underlying the emergence of these conditions. By examining the behavioral patterns of online platforms, the findings provide a practical reference for governments in formulating specific cooperative supervision plans.

1.1. Literature Review and Theoretical Framework. The formulation of privacy protection policies for platform enterprises is affected by factors at different levels. To discover the optimal configuration of conditions that promote the implementation of privacy protection by enterprises, a systematic review of existing research, from the perspective of privacy economics, was undertaken to uncover the factors that influence enterprises' private data utilization and management behavior.

1.2. Policy Environment. Privacy legislation is an effective approach to regulate firms' privacy-related behavior. The European Union has focused on legislation solutions, establishing General Data Protection Regulation (GDPR) to provide principles that govern the use of data across multiple sectors, including the need for certain data processing activities [8]. The enforcement of GDPR has been effective and led to a reduction in third-party cookies [9], updated online privacy statements [10], and reduced online display ad effectiveness [11]. According to Goldberg et al. [12], the rollout of GDPR increased firms' cost of collecting consumer data which has supported the belief that local regulatory practices play a role in firms' reactions. Zhou et al. [13] stated that China needs privacy legislation to regulate the processing and collection of personal information and that the policymakers should learn from international experience and embody the characteristics of incentive compatibility. Determann [14] stated that if the draft of the Personal Information Protection Law of China is enacted, it will effectively regulate the process of Chinese residents' personal data in both the private and public sectors. All the above studies demonstrate that privacy legislation has a positive effect on platforms' privacy protection behaviors. Legislation notwithstanding, industry standards are also an important factor in regulating firms' behavior. Hahn and Layne-Farrar [15] suggested that, considering the high cost of online privacy legislation, defining industry self-regulated standards is more efficient. Koops et al. [16] defined industry standards as norms and rules that are formulated and enforced by specific organizational units. They suggested that, by formulating industry standards, firms would develop effective self-regulation systems as all rules would be created by interest groups and built on internalized values, such that it would be easy for relevant parties to conform to and apply such rules.

1.3. Market Competition. Many economists have suggested a market-based approach to solve privacy issues. Posner [17, 18] and Stigler [19] suggested that privacy issues can be solved by organized personal-information transactions. Laudon [20] proposed the concept of *national information markets* and suggested that an effective market-based approach is a powerful and low-cost method. In the absence of a dedicated private data market, transactions between users and the platform frequently occur during the exchange of private data for extra services and discounts. Under this premise, market structure can influence how enterprises conduct privacy protection. Casadesus-Masanell and Hervas-Drane [1] asserted that competitive effects drive enterprises to implement privacy protection. Their model demonstrated that less leakage of private information

occurred in competitive markets compared to monopolistic markets; hence, users are likely to have greater protection and benefits in a competitive market environment. Shapiro [2] and Mai et al. [3] suggested that if privacy protection becomes a consideration for users when making online transaction decisions, businesses that implement privacy protection are likely to have a competitive advantage. As price discrimination is one of the phenomena of the abuse use of personal information which can severely reduce consumer welfare, prior research focused on exploring the reason and level of platform conducting price discrimination. Li et al. [21] built a vertical differentiated duopoly model and indicated that the reason for the price discrimination is a lack of competition between platforms rather than the absence of privacy protection law. Chen [22] found that the ability to extract consumer surplus through price discrimination mostly depends on the market structure, and when platform occupies a monopoly position in the market, it can extract all consumer surplus through price discrimination. These all demonstrate that market competition can drive enterprise to improve privacy protection.

1.4. Heterogeneity among Firms. Enterprise privacy protection capabilities and intentions are affected by the heterogeneity among firms. By establishing the utility function of enterprises, users, and third parties, Fainmesser et al.'s model revealed the important influence of business models on enterprises' privacy policy decisions [4]. They further analyzed enterprises' use of private data under two extreme business models: purely data and purely usage driven. The results showed that data-driven businesses exhibited higher data collection behaviors and more third-party requirements for user data than user-driven businesses, indicating that data-driven business models led to lower privacy protection (Fainmesser et al. [4] categorized the business models of platforms into data-driven, ad-driven, and user-driven. The data-driven business model can be understood as a platform that provides free services while generating profit through sharing data with data aggregators. The ad-driven business model can be understood as companies whose main revenue is offering targeted advertising, such as Facebook and Google. The user-driven business model can be understood as a platform that generates profit through users' payments in the form of subscription fees or commissions, such as online ride-hailing). Ramadorai et al. found that data-sharing behaviors were negatively correlated with corporation size, market share, and technology capital [5]. When a company exhibits market power and substantial technology advantage, it may be more inclined to analyze and apply collected consumer data internally rather than trading it to third parties for profit. Data processing and privacy enhancing technology have been the major issues in front of researchers working in this field and the findings demonstrated that technology investment could affect firms' privacy protection behaviors. For example, Gupta et al. discovered that technological improvement in image encryption could increase a firm's ability in maintaining a secure network [7]. Moreover, Juneja et al. [6] discovered that, by applying cyber-twin technology, the network system can become more reliable and safer. Furthermore, firms' privacy usage behavior may be affected by the type of firm. Acquisti and Varian [23] discovered that conducting conditioning price is more attractive for certain types of firms as they find it more profitable. Such firms are those in industries in which transactions are computer mediated, with repeated and frequent purchases, or where anonymous purchase is difficult or costly. Their study demonstrated that firms' intertest in commercialize users' privacy data are varied according to its type. In summary, heterogeneity among enterprises, including market power, technological capital, and business models, influence a firm's development of privacy protection policy.

1.5. Interactions among Explanatory Factors. There exist complex mutual influences among the policy environment, market competition, and heterogeneity among firms. These interactions necessitate adopting a configurational perspective when evaluating the drives for privacy protection behaviors. First, the effects of competition on privacy protection differ across heterogeneous firms. Casadesus-Masanell and Hervas-Drane [1] constructed a model in which firms compete through private data disclosure levels and prices and found that, in a competitive marketplace, when target users have higher valuation of the product/service and a greater willingness to pay for the services, market competition causes enterprises to gravitate toward a policy of lower privacy disclosure alongside price increases. However, when target users have lower valuation of the product/service and a lower willingness to pay for it, market competition tends to result in firms reducing prices and increasing privacy disclosure. This finding demonstrates that, to pursue higher profit with personal data, market competition effects differ according to the user base.

Second, market-based approaches and government regulation are complementary and mutually influential. Researchers have suggested that the interaction between the market and government regulation is thus what motivates enterprises to protect consumer privacy. For example, Cassidy and Chae [24] expressed doubt in the effectiveness of a single regulation approach to address privacy issues, claiming that regulation cannot completely solve externalities caused by privacy misuse. Laudon [20] demonstrated that first-generation regulatory models that rely on the principle of informed consent and prohibit the secondary use of information are no longer feasible in the current data age. Technology, economy, and organizational behavior have weakened the power of regulatory methods; while economic benefits, political interests, and bureaucratic advantages have made it impossible for regulatory mechanisms to be fully functional. When government regulation cannot completely resolve problems, dedicated markets are needed. Therefore, Laudon [20] suggested that market-based approaches can supplement deficiencies in government regulation. In Laudon's theory, the proposed information market requires the presence of government regulation when establishing regimes and orders. Hence, the market

and government regulation are not antagonistic but rather complementary aspects of a complete system of administration. In addition, studies have found that government regulation affects market structure. Gal and Aviv [25] found two harmful effects on competition and innovation of the GDPR: the GDPR restricts competition in the data market, which is not conducive to the entry of start-ups and thus consolidates the market position of incumbent market leaders, creating a more concentrated market structure. Similarly, Campbell et al. [26] found that privacy regulation that relies on enforcing opt-in consent will strengthen the dominant position as users tend to give their consent to established platforms rather than start-ups.

The preceding literature indicates that market structure, policy environments, and heterogeneity among firms have a joint impact on privacy protection, and there are complex complementary and mutual influences among the three constructs. Therefore, the argument presented in this paper is that the privacy policies of Chinese platform enterprises are self-selected under the co-constraints and joint influence of policy environment, market structure, and firm heterogeneity. These factors were further divided into six subconditions and analyzed in a configurational perspective. The policy environment was defined as an exogenous and uncontrollable condition, while other conditions were endogenously controllable for enterprises. The theoretical framework of this study is shown in Figure 1.

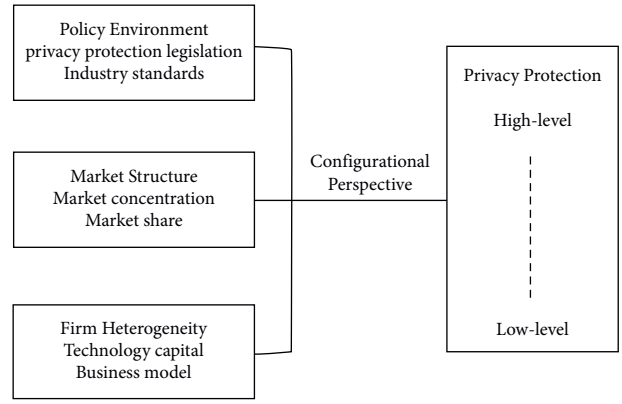

Figure 1: Theoretical framework of the research.

2. Materials and Methods

2.1. Data Analysis Methods. The theoretical framework shows that the formulation of privacy policy for an enterprise is the result of the interactions of various factors. Conventional statistical methods based on individual factors and pairwise analysis of interactive effects have limitations. Conventional econometric statistical methods, such as multiple linear regression or interaction effect analyses, tend to adopt single causal assumptions, in which each explanatory variable acts on the outcome variable individually, and the external environment and internal attributes of the organization have a one-way causal relationship [27]. Therefore, these methods do not fully explain the mechanisms underlying privacy policy formulation under the combined influence of various internal and external conditions, such as policy, market environments, and heterogeneity among firms.

In the present study, the fsQCA method was applied to study the factors that drive platform enterprises' privacy protection policies. Contrary to traditional statistical methods, QCA neither relies on *additivity* nor the *net effects* of variable independence [27]; instead, the conditions interact within the boundaries of its analytical framework. QCA can be used to explain *multiple concurrent* causalities formed by different combinations of conditions. Such an approach allows for expanded and in-depth interpretation of privacy protection decisions at the firm level from the perspective of both exogenous environmental and endogenous firm-level conditions, which allows for the findings to be better employed as a reference for government to formulate practical privacy protection policies. In addition, the fsQCA method is suitable for the analysis of small- and medium-sized samples and hence pairs well with the sample size of this study.

2.2. Sample Selection. Since the analysis of firm heterogeneity requires data from various dimensions, only listed platform enterprises were selected. Given that some Chinese platform enterprises are listed overseas (such as in Hong Kong or the United States), in addition to the A-share companies, all Chinese concept stocks listed in Hong Kong and the United States were also included in the study. Thus, 6,975 listed companies were selected, including 4,049 A-share listed companies and 2,926 companies listed overseas. A web crawler, combined with manual checking, was used to screen the selected companies further, of which only 507 companies disclosed complete privacy policy statements on their official websites. After manually checking the 507 listed enterprises, we found 70 enterprises that had platform attributes. According to Thomann and Maggetti [28], the external validity of the fsQCA method requires that the case study should typically select cases purposively according to theoretical criteria that determine the cases' relevance to the research question. Therefore, by comprehensively considering the unitary nature of the business' scope and the availability of industry-level data, 34 platform enterprises in representative types of platforms were selected for further analysis. The types of platforms were divided according to the classification of platform enterprises identified in the "2021–2025 China's Platform Economy In-Depth Survey and Investment Prospect Forecast Report" (Table 1). According to Marx [29], for six conditions, the study requires at least 26 samples. In our study, the sample meets the standard. By controlling the ratio of number of cases to number of conditions, the internal validity of the finding can be guaranteed in this regard.

2.3. Variable Selection

2.3.1. Outcome Variable: Privacy Protection Level. Drawing on the evaluation method of Ramadorai et al. [5], this study used the legal clarity index of the privacy

Table 1: Platforms selected for the study.

Platform type	Platform name
E-commerce	JD.com, Secoo, Pinduoduo, Sunlands technology, Beijing Zhidemai tech, Baozun, Vip.com, Light in the box, and Mogu Street
Property brokerage	ke.com, fangdd.com, Q&K international group, and Fang.com
Search engine companies	Sogou and Youdao
Game streaming	Huya and DOUYU.com
Online educational	51Talk
Online travel	Tuniu, Ctrip, and Elong.com
Video streaming service	Bilibili and iQIYI.com
Music streaming service	Tencent Music
Vehicle	Tuanche.com and Autohome.com
Stranger communication	Momo
Social media	Qutoutiao
Group discount	Meituan
Recruitment	51job.com and Liepin.com
Instant delivery	SF Express, STO Express, and DEPPON Express

protection policy as a proxy variable. A web crawler was used to seek the privacy policy statements of the listed companies. A fuzzy evaluation method was then used to quantify the degree of consumer privacy protection that is reflected in the privacy policy. Evaluation factors, factor weights, and expert-assigned weights were used to parameterize the qualitative evaluation data into quantitative evaluations. The detailed procedures are as follows: since the fuzzy comprehensive evaluation works best with a sample of suitable size, the privacy policies of all 507 listed companies were collected, among which 20 companies were selected for manual expert evaluation. Next, legal experts were invited to rate the selected privacy policies along six dimensions (data collection, consumer consent, responsible use, user rights, cookies policy, and overall) according to the "Information Security Technology–Personal Information Security Specification." A 3-point scale was used to rate each item ("−1" = "low user-privacy protection," "0" = "medium user-privacy protection," and "1" = "high user-privacy protection"). Then, the mean ratings of each dimension were calculated, and natural language processing (NLP) semantic analysis was adopted to obtain a word cloud for high and low privacy protection, respectively (Figure 2). A machine learning library in R was then used to calculate the degree of privacy protection for the full sample and to obtain the legal clarity indices of the 507 companies (the specific method of determining the legal clarity index is as follows: assume that G and B are the sets of words in Figure 2(a) and Figure 2(b), respectively. Let $\widehat{P}_{ij}$ be the term frequency and inverse document frequency (tf-idf) of word j in policy i. In the NLP-semantic analysis, the tf-idf is determined as follows: $tf_{i,j} = n_{i,j}/\sum_k n_{k,j}$. On this basis, the policy quality is calculated as Legal Clarity Index $= \sum_{j\in G}\widehat{P}_{ij} * Rank_j - \sum_{j\in B}\widehat{P}_{ij} * Rank_j$, where $Rank_j$ is the ranking of importance of the keywords.). As the final 34 platform enterprises selected for the study were included in these 507 companies, their legal clarity indices were also obtained.

2.3.2. Condition Variables. For firm heterogeneity, technology capital and the firm's business model were used as proxy variables. We calculated technology capital by accumulating past research and development expenditures for firms according to Peters and Taylor [30]. Firms may utilize a combination of business models. That is, most platform enterprises tend to incorporate both data-driven and user-driven business models (we categorized the business model of platforms as data-driven and user-driven. We combined both ad-driven and data-driven as in Fainmesser et al. [4] into data-driven, as both revenue models focus on the exploitation of users' data.), with only minor differences in emphasis. Data-driven platforms primarily rely on offering targeted advertising and selling data to data aggregators as sources of revenue [4]. Therefore, based on the availability of data present in the company annual reports, this study used the proportion of advertising revenue to total operating revenue as a measure of the proportion of profit generated through the exploitation of personal data, which represents the scale of data-driven business models in the overall business model.

Market share and market concentration were employed as indicators to represent the market structure. Market share was determined from industry reports and extrapolated by the corresponding platform classification, while the four-firm concentration ratio (CR4) was used as a proxy variable for market concentration. The CR4 was determined by adding the market shares of the top four platform enterprises with the highest sales in the corresponding classification category.

With the strengthening of national privacy protection legislation, Chinese companies, especially technology companies, are required to disclose the use of private data to local security regulators when they go public and adjust their policies following local regulatory requirements. Therefore, the presence of privacy protection legislation in the region in which the companies were listed was included as one of the proxy variables for the policy environment. A dummy dichotomous variable was also used to measure the presence of

(a) (b)

Figure 2: Word cloud of privacy policy. Note that the words in the word cloud were generated using the term frequency and inverse document frequency keyword extraction method based on the ratings provided by the experts. (a) Privacy policy with high ratings. (b) Privacy policy with low ratings.

local government policy: "1" = "with local policy" and "0" = "without local policy." In addition, industry standards also restrict company behavior. Some industries have formulated more detailed industry standards based on data characteristics, processing characteristics, and interaction patterns with users. At present, regulations related to the use of personal information by platform enterprises include the "Provisions on Security Management of Personal Information for Delivery Service Users," "China Railway's Trial Measures for Online Information Management," "Specification for e-commerce Data Transaction Privacy Protection," "Provisions on Protection of Personal Information of Telecommunications and Internet Users," and "Specification for Civil Aviation Network and Information Security Management." The implementation of these industry standards indicates industry differences in privacy regulation at the policy level. Hence, industry standards were also included as a proxy variable. A dummy dichotomous variable was used to measure the presence of industry standards: "1" = "with industry standards" and "0" = "without industry standards."

2.4. Data Collection and Calibration. Our data comprised corporate data extracted from the Wind-Economic (WIND) Database, China Stock Market and Accounting Research (CSMAR) Database, Lixinger.com, Compustat, Cninfo.com, and official websites of the US Securities and Exchange Commission (SEC). Industry data were extracted from the reports of various research institutions such as iiMedia Research. Specifically, the Chinese-listed firm data were collected from the WIND and CSMAR Database to obtain the index data of all A-share listed companies. Lixinger.com and Compustat were used to obtain the index data of Hong Kong stocks and US stocks-listed Chinese concept stock companies. Cninfo.com and the official website of the SEC contain the full annual reports of A-share listed companies and US-listed companies, respectively. The extracted data were used to calculate the proportion of advertising revenue to total operating revenue. Market structure-related variables (market share and market concentration) were extracted from the industry reports of research institutions such as iiMedia research, Intelligence Research Group, and the Chinese Academy of Industry Economy Research.

Calibration is defined as the process of assigning membership values to a sample set. Referring to relevant theories, knowledge, and experience, the direct calibration method [31] was used to calibrate all conditions and outcomes (with the only exception being market concentration) into fuzzy membership scores. The 75%, 50%, and 25% quantiles are commonly used as thresholds for full membership, cross-over point, and full nonmembership, respectively. For market concentration, Bain [32] defined market concentration as follows: 65% < CR4 < 75% = high concentration, 35% < CR4 < 65% = medium concentration, and 30% < CR4 < 35% = low concentration. Therefore, in this study, CR4 = 35% and 65% were used as the thresholds for full membership and full nonmembership and the intermediate value of 50% was used as the cross-over point. To deal with skewed data and improve internal validity, we applied the calibration points according to the distribution of the data itself, and with this approach, we avoided the impact of extreme values on the calibration procedures. To avoid discarding samples with membership less than 0.5, we manually adjusted 0.5 to 0.501 according to Campbell et al. [33]. Table 2 shows the calibration results of the conditions and fuzzy set outputs.

3. Results

3.1. Necessary Conditions' Analysis. First, the *necessity* for each condition was tested. Referring to the standard approaches to QCA, each input condition was tested individually to see if it was necessary for the formulation of a user privacy protection policy. Then, the configuration conditions with the highest explanatory power were identified. A necessary condition was defined as a condition that was required for a given outcome to occur with a consistency level greater than 0.9 [31]. In this study, fsQCA 3.0 software was used to obtain the necessary conditions for high/low privacy protection. Table 3 shows that the consistency score for "with local policy" exceeded 0.9, and the coverage reached 0.536, indicating that the presence of privacy protection legislation in the region in which the company

Table 2: Calibrations and descriptive statistics.

	Conditions and outputs	Calibration			Descriptive statistics			
		Full membership	Cross-over point	Full nonmembership	Mean	Std. deviation	Minimum	Maximum
Output variable	Legal clarity	237533.00	182476.30	98531.50	183794.40	96385.45	10100.00	483070.50
Heterogeneity among firms	Technology capital	582013.80	111795.00	0	663766.60	1438137.00	0	6207494.00
	Business model	0.22	0.06	0	0.20	0.30	0	0.95
Market structure	Market concentration	0.65	0.5	0	0.81	0.22	0.27	0.99
	Market share	0.37	0.11	0.35	0.20	0.25	0	0.92
Policy	Industry standards	1		0				
	Local policy from where the enterprise is listed	1		0				

Table 3: Analysis of necessary conditions.

Condition variables	High privacy protection		Low privacy protection	
	Consistency	Coverage	Consistency	Coverage
High-technology capital	0.667	0.710	0.386	0.396
Not high-technology capital	0.432	0.432	0.709	0.667
High % of advertising revenue	0.557	0.604	0.457	0.466
Not high % of advertising revenue	0.507	0.499	0.611	0.564
High market concentration	0.872	0.518	0.888	0.495
Not high market concentration	0.150	0.588	0.135	0.499
High market share	0.593	0.657	0.443	0.460
Not high market share	0.512	0.494	0.670	0.607
With local policy	0.949	0.536	0.872	0.464
Without local policy	0.051	0.300	0.128	0.700
With industry standards	0.263	0.384	0.449	0.616
Without industry standards	0.737	0.587	0.551	0.413

was listed had a considerable driving effect on the establishment of a highly protective privacy policy.

3.2. Sufficiency Analysis of Configuration Conditions. Although a necessary condition is a condition that must exist for the outcome to occur, its existence does not guarantee that the outcome occurs [34]. Therefore, sufficiency analysis of the configuration conditions was required to reveal how combinations of conditions drive the formulation of highly protective privacy policies. Before analysis of sufficiency, it is necessary to determine the consistency and frequency thresholds. In this study, the determination principles were as follows: (1) the consistency threshold of the conditional configuration should not be less than 0.75 [35] and the specific value should be determined according to the research context, such as 0.8 [36] or 0.76 [37], and (2) the frequency threshold should be determined by the sample size. For small and medium samples, the frequency threshold is normally set to 1, while for large samples, the frequency threshold should be greater than 1 [34]. Combining the principles and the observed samples in this study, the raw consistency threshold and the frequency threshold were set to 0.8 and 1, respectively. Moreover, according to Misangyi and Acharya [38], the PRI threshold was set to 0.75. The configurations in Table 4 can be regarded as sufficient conditions for Chinese platform enterprises to formulate highly protective user privacy policies or less protective user privacy policies.

For configurations associated with high privacy protection, the overall solution consistency was 0.896 and the overall solution coverage value was 0.339. From the perspective of individual configuration (columns), the three configurations were summarized into three driving forces based on the presence and absence of conditions. Configuration H1 (consistency = 0.928, unique coverage = 0.125, and raw coverage = 0.125) was categorized as a combination of *technology driven and regulation driven*, for which technology capital, local policy, and industry standards were present conditions, indicating that platform enterprises with higher technological resources under government regulations were more inclined to adopt user privacy protection policies. Configuration H2 (consistency = 0.947, unique coverage = 0.039, and raw coverage = 0.041) was categorized as being promulgated through a *user-driven business model and market competition (user-driven + competition effect)*. In the configuration, data-driven business models, market concentration, and market share were absent, indicating that user-driven enterprises in the market competition environment were more likely to formulate highly protective privacy policies. Configuration H3 (consistency = 0.864, unique coverage = 0.172, and raw coverage = 0.175) was categorized as a *dominant platforms policy*, in which market share and market concentration

Table 4: Configurations for high privacy protection and nonhigh privacy protection.

		High privacy protection			Nonhigh privacy protection	
		Technology + regulation driven	User-driven + competition effect	Dominant platforms policy	Business growth	Data-driven + competition effect
		H1	H2	H3	NH1	NH2
Firm heterogeneity	Technology capital	●	●	⊗	⊗	⊗
	Business model		⊗	⊗	⊗	●
Market structure	Market concentration	●	⊗	●	●	⊗
	Market share	⊗	⊗	●		⊗
Policy	Local policy	●	●	●		●
	Industry standards	●	⊗	⊗	●	⊗
	Raw coverage	0.125	0.041	0.175	0.372	0.064
	Unique coverage	0.125	0.039	0.172	0.372	0.064
	Consistency	0.928	0.947	0.864	0.967	0.964
	Overall solution consistency		0.339			0.437
	Overall solution coverage		0.896			0.966

Note. ●and ● indicate that the condition is present, ⊗ and ⊗ indicate that the condition is absent, ● and ⊗ indicate a core condition, and ● and ⊗ indicate a marginal condition. A blank cell indicates that the condition may or may not be present.

were present and technology capital and business model were absent conditions, indicating that user-driven dominant platforms with no technological advantage tended to formulate higher-level privacy protection policies. From the perspective of individual conditions (rows), the presence of local policy was a core condition in all configurations, indicating that legislation had a significant driving effect on firms' implementation of user privacy protection. This finding also echoed the results of the necessity analysis, in which the consistency score of this variable was greater than 0.9.

In addition, further analysis of the configuration with lower privacy protection was conducted to explore the *causal asymmetry* that emerged during the process and to understand the driving forces behind lower privacy protection policy implementation. For configuration for nonhigh privacy protection (Table 4), the overall solution consistency was 0.966, and the overall solution coverage was 0.437. From the perspective of individual configuration (columns), the configurations were analyzed into two drivers. Specifically, configuration NH1 (consistency = 0.967, unique coverage = 0.372, and raw coverage = 0.372) was categorized as *business growth driven*, for which technology capital was the absence condition and market concentration was the present condition, indicating that when exposed to less competitive market structure, platform enterprises that had no technological advantage tended to profit by formulating less protective privacy policies to achieve growth. Configuration NH2 (consistency = 0.964, unique coverage = 0.064, and raw coverage = 0.064) was categorized as being *driven through the combination of a data-driven business model and market competition* (data-driven + competitive effects), for which the data-driven business model was the core condition alongside the absence of high market concentration and market share, indicating that, driven by market competition, data-driven enterprises were more likely to formulate low protective privacy policy. From the perspective of individual conditions (rows), none of the conditions were core conditions for all configurations, suggesting that the formulation of low privacy protection policies was driven by a combination of different factors rather than any single condition.

3.3. Robustness Test. Given that different consistency levels and calibration standards could lead to varying configurations, thereby affecting the analysis results, Schneider and Wagemann [35] proposed a robustness test by changing the consistency level and adjusting the calibration threshold. For the result of high privacy protection, by adjusting the raw consistency level to 0.9 and the frequency threshold and PRI threshold to 1, we obtained two configurations among which RH1 is consistent with H2 and RH2 is the subset of baseline model H1. Then, according to Bell et al. [39], by keeping the raw consistency level and the PRI consistency unchanged and increasing the frequency threshold to 2, we obtained one configuration RH3 which is consistent with H3 (only differing in core condition). For the nonhigh privacy protection result, by increasing the raw consistency level to 1 and the frequency threshold to 2, we thereby obtain two

configurations and one configuration, respectively. All three configurations are subsets of NH1. As shown in Table 5, by changing thresholds, the configurations were either consistent with the baseline model or presented a clear subset relationship, and by increasing the threshold, the number of configurations decreased. According to Wu et al. [40] and White et al. [41], the robust configurations indicate that the results were indeed robust.

4. Discussion

This study uncovered the necessary conditions for platforms to formulate high protection privacy policy and low protection privacy policy. Additionally, by analyzing the sufficient configuration conditions, we investigated the forces driving platform enterprises to make decisions regarding privacy policies of different protection levels. Under three conditions, platforms intended to formulate privacy policy with a high level of protection. Those conditions involved high-technology-supported platforms under regulation, user-driven business in competitive markets, and dominant platforms driven by strategic intention. In contrast, we found two drivers of platforms formulating privacy policy with a low level of protection: platforms driven by business growth intentions and data-driven business models in a competitive market.

Among the configuration conditions that were necessary for the formulation of high user-privacy protection, the presence of privacy protection legislation in the region in which the companies were listed was crucial. Although the privacy protection legislation of Mainland China has not been completely performed (Mainland China enacted the Personal Information Protection Law in August 2021, and it came into effect in November 2021. Therefore, by the time we collected the data for this study, the law was still in its infancy.), Hong Kong and the United States do have dedicated and mutually implemented privacy protection legislations (Hong Kong has promulgated the Personal Data (Privacy) Ordinance, while the California Privacy Rights Act has a great impact nationwide in the U.S.). Hence, platform enterprises that intend to list in Hong Kong and US stock markets are forced to adjust their privacy protection policies according to local requirements. Privacy protection legislation serves as a rudimentary guarantee to ensure that platform enterprises establish privacy protection policies as well as provide a prerequisite for other conditions to exert their effects. However, industry standards had no driving effect on the formulation of privacy policies in most configurations. This finding showed that, although some subsectors had established standards that restricted corporate behavior, the protection offered in these sectors was not significantly superior to the sectors without corresponding standards; thus, the effect of industry standards was not prominent in the analysis. The result is relatively surprising, and we therefore consider the possible reasons. First, the previously lacking national legislation in mainland China may weaken the effectiveness and enforcement of industry standards as all industry standards are made without an overall guidance. Second, weaknesses in existing industry standards may affect their implementation effectiveness. In some industries, standards are not issued by the respective industry associations; therefore, they do not reflect the balance between the needs of the endogenous development of enterprises and the privacy protection of users. Thus, in such circumstances, enterprises do not intend to conform to the industry standards.

A comparison between the forces driving high and low privacy protection policies revealed that platforms tended to formulate privacy policies based on their strategic motives, and there were noticeable conjunctive effects among various conditions. First, comparing configuration H3 and NH1, we observe that, in less competitive market environments, platforms tended to adopt two polarized approaches (high and low) concerning privacy policy formulation. In NH1, platforms tended to adopt privacy policies with a low level of protection in a highly concentrated market, even with industry standards present. In H3, dominant platforms in highly concentrated markets adopted privacy policies with a high protection level, even without industry standards. The effects of heterogeneity among firms for both configurations were the same, presenting somewhat of a contradiction. However, these findings provide important insight into what personal data means for platforms and how they formulate privacy protection strategies. Configuration NH1 showed that platforms in less competitive market environments did not have the incentives to protect users' privacy, as users had limited options. In this case, personal data served as a dimension of quality in users' rational choice and a less competitive market environment weakened platforms' intentions to increase the quality. In contrast, configuration H3 showed that some dominant platforms in less competitive market implemented high-level privacy protection policies. To maintain a competitive advantage, dominant platforms may have the incentive to implement *data blockades* by reducing third-party data sharing and access, acquiring a "data advantage" over rivals [42–44]. In this case, we infer that data blockade behaviors exist in some platforms. Here, personal data are treated as an important asset in competition between platforms and the implementation of the policies serves as a strategic tool by which to reduce numbers of new entrants, rather than out of the intention to protect users. This may lead to increased consolidation of market dominance and increased market concentration, thus resulting in anticompetitive effect such as loss of innovation and quality [43]. Therefore, although privacy policies might have reduced the risk of data breaches and misuse, protected user information, and satisfied user preferences in the short term, such behaviors were not conducive to the long-term goal of consumer privacy protection nor the high-quality development of the industry.

Second, comparing configuration H2 and NH2, we infer that the conjunctive effects between market structure and business models have different outcomes. Specifically, driven by market competition, platforms that adopted a more user-driven business model tended to formulate highly protective privacy policies. This finding demonstrated that the platforms that provided paid products/services had incorporated privacy protection as a

Table 5: Robust configurations for high privacy protection and nonhigh privacy protection.

Changing thresholds	High privacy protection			Nonhigh privacy protection		
	1/0.9/0.75		2/0.8/0.75	1/1/0.75		2/0.8/0.75
Configuration	RH1	RH2	RH3	RNH1	RNH2	RNH3
Technology capital	●	●	⊗	⊗	⊗	⊗
Business model	⊗	⊗	⊗	⊗	⊗	⊗
Market concentration	⊗	●	●	●	●	●
Market share	⊗	⊗	●		●	⊗
Local policy	●	●	●	⊗		●
Industry standards	⊗	●	⊗	●	●	●
Difference with the baseline model	Consistent with H2	Subset of H1	Consistent with H3, only different under core conditions	Subset of NH1	Subset of NH1	Subset of NH1

Note. ● and ● indicate that the condition is present, ⊗ and ⊗ indicate that the condition is absent, ● and ⊗ indicate a core condition, and ● and ⊗ indicate a marginal condition. A blank cell indicates that the condition may or may not be present.

component of product/service quality, a criterion that users may consider when making rational decisions. Consequently, platforms with user-driven business models were more likely to further develop their privacy protection mechanisms to manage the market competition. Contrastingly, platforms that adopted a more data-driven business model tended to formulate less protective privacy policies. When faced with market competition, these platforms tended to seek further profitability by lowering privacy protection standards and increasing data utilization while offering lower prices or free products/services to attract users. These results reflected the existence of the "privacy paradox" among Chinese platform users, who cared about the safety of personal information but tended to prefer free or low-cost products/services.

The current findings have several practical implications for policymakers. First, a co-regulation system based on the Personal Information Protection Law and industry standards should be established to encourage enterprises autonomously implement policy to protect users. Regarding industry standards, a systematic industry standard is recommended so that firms do not need to refer to different national standards and administrative regulations when formulating privacy policies and processing collected data. In addition, the formulation process should be led by industry associations, considering the interests of concerned parties and more detailed standards that match the needs of the respective businesses. The goal of such an approach would be to avoid the rigid application of laws, ensure flexibility and pertinence, and encourage proactive self-regulation of the enterprises.

Second, the enforcement of the newly enacted Personal Information Protection Law should emphasize balance between data protection and sharing, not being limited to user privacy protection but should also include supervision of malicious industry practices based on "data blockades" to reinforce dominant market positions. Therefore, we suggest the enforcement focusing on data sharing between platforms. Specifically, we suggest emphasizing the guarantee of data portability, which has been included as a users' right in the Personal Information Protection Law to resolve the issue of "locked data" and high conversion costs, as well as to reduce monopoly/oligopoly power and increase market competition [45]. Specifying users' right to data portability is conducive to minimizing monopoly/oligopoly in the market, stimulating market competitiveness, and promoting the privacy protection of the industry. In addition, it is necessary to urge platforms to achieve interoperability, ensuring that user data can run barrier-free between different platforms at a technological level to further ensure data sharing and cross-platform functionality.

Finally, we suggest reinforcing the positive effects of users' rational choice. Many scholars have highlighted that the best solution to privacy protection issues is reinforcing users' rational decision-making capability alongside market-oriented mechanisms [17–19]. The results of this study revealed that the impact of competitive effects on privacy policy was closely associated with users' ability to make rational decisions. Therefore, regulatory agencies are suggested to promote users' rational decision-making from the following two aspects. First is enhancing users' privacy awareness, which is the best means to overcome the "privacy paradox" [46]. Therefore, the government should increase media exposure of platforms that are suspected of misusing user information and implement corresponding educational programs to arouse public attention and awareness. Second is encouraging enterprises to use privacy protection as means of competition and to further visualize privacy policies. Behavioral economics research has demonstrated that evaluating the privacy protection of a given website and specifying the rating on its web page, encourages users to consider privacy protection when selecting services [47]. Hence, we suggest that industry associations issue compliance icons to corresponding platforms and rate the privacy protection standard at the industry level, using visualizations to encourage competition for privacy protection between enterprises and to promote the implementation of corresponding policies.

5. Conclusions

Although considerable attention has being paid to the factors associated with enterprise's privacy protection incentives, to date there has been little research based on a

configurational perspective that considered how multiple factors interact and drive enterprises to make optimal decisions concerning privacy protection. Overall, our study uncovered the causal complexity underlying privacy protection strategies and the role of simultaneous interplay among policy environment, market structure, and heterogeneity among firms.

We demonstrated that privacy protection legislation appears to be a fundamental factor according to which platforms enact a positive privacy protection strategy. Therefore, the privacy protection regulation should fully strengthen the positive effect of users' rational choice and consider enterprises in different contexts. By establishing a co-regulation system and formulating standards for different industries, it would be possible to provide specific guidance for enterprises with different market positions and business models. As such, privacy protection regulation could be more inclusive and capable of addressing the internal incentives of enterprises, thus promoting enterprises to independently commit to protecting user privacy.

5.1. Limitations. As the number of conditions being tested should coincide with the sample size, the study was limited in which the conditions we included were not fully comprehensive. For example, the type of users could be included in future studies, as enterprises are known to implement different privacy protection strategies when faced with different types of users, especially users who differ in price-demand elasticity. Therefore, these aspects need empirical testing. Testing additional conditions in future studies would provide a broader perspective on how enterprises formulate privacy protection strategies and what factors influence their decisions.

Another challenge for future studies is to expand the sample to global platform enterprises and compare differences in driving factors between Chinese platforms and platforms in Europe or the United States. As globalization has enabled platforms to expand widely, it is important that users and local governments understand platforms' behaviors, especially their strategy toward privacy policy. Relevant research that provides additional insight into platform enterprises' behaviors would help users to better conduct rational decision-making and assist governments to better formulate privacy protection regulation for international enterprises.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors are grateful to Haoyang Wang, Haiming Zhang, Jiayi Lin, Fengying Lang, and Yuanting Wei for their help in data collection and their support throughout the course of this study. The authors are also grateful to Dr. He Cui for providing a professional legal evaluation of the privacy policies. This work was supported by the Key Project of the National Social Science Fund of China (Grant no. 19AJY004), Department of Education of Zhejiang Province (Grant no. Y202147800), and Zhejiang Technical Institute of Economics (Grant nos. JKY2021019 and JKY20190160).

References

[1] R. Casadesus-Masanell and A. Hervas-Drane, "Competing with privacy," *Management Science*, vol. 61, no. 1, pp. 229–246, 2015.

[2] C. Shapiro, "Premiums for high quality products as returns to reputations," *Quarterly Journal of Economics*, vol. 98, no. 4, pp. 659–679, 1983.

[3] B. Mai, N. Menon, and S. Sarkar, "Online privacy at a premium," in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS '06)*, NW Washington, DC, US, January 2006.

[4] I. P. Fainmesser, A. Galeotti, and R. Momot, "Digital privacy," *HEC Paris Research Paper No. MOSI-2019-1351*, 2019.

[5] T. Ramadorai, A. Uettwiller, and A. Walther, "The market for data privacy," *SSRN Electronic Journal*, 2020.

[6] S. Juneja, M. Gahlan, G. Dhiman, and G. Dhiman, "Futuristic cyber-twin architecture for 6G technology to support internet of everything," *Scientific Programming*, vol. 2021, Article ID 9101782, 7 pages, 2021.

[7] M. Gupta, K. K. Gupta, M. R. Khosravi, P. K. Shukla, S. Kautish, and A. hankar, "An intelligent session key-based hybrid lightweight image encryption algorithm using logistic-tent map and crossover operator for internet of multimedia things," *Wireless Personal Communications*, vol. 121, pp. 1–22, 2021.

[8] A. Acquisti, C. Taylor, and L. Wagman, "The economics of privacy," *Journal of Economic Literature*, vol. 54, no. 2, pp. 442–492, 2016.

[9] T. Libert, "An automated approach to auditing disclosure of third-party data collection in website privacy policies," in *Proceedings of the 2018 International World Wide Web Conference*, pp. 207–216, Lyon, France, April 2018.

[10] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(Un) informed consent: studying GDPR consent notices in the field," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 973–990, Association for Computing Machinery, London UK, November 2019.

[11] A. Goldfarb and C. Tucker, "Online display advertising: targeting and obtrusiveness," *Marketing Science*, vol. 30, no. 3, pp. 389–404, 2011.

[12] S. Goldberg, G. Johnson, and S. Shriver, *Regulating Privacy Online: An Economic Evaluation of the GDP*, 2019.

[13] H. Zhou, "Geren xinsi Baohu Fa (caoan): lizu Guoqing yu Jiejian Guoji Jingyan de Youyi tansuo" [personal information protection law (draft): an exploration based on national conditions and international experience]," *Tansuo yu Zhengming/Exploration and Free Views*, vol. 2020, no. 11, pp. 9–11, 2020.

[14] L. Determann, Z. J. Ruan, and T. Gao, "China's draft personal information protection law," *Journal of Data Protection & Privacy*, vol. 4, no. 3, pp. 235–259, 2021.

[15] R. W. Hahn and A. Layne-Farrar, "The benefits and costs of online privacy legislation," *Administrative Law Review*, vol. 54, no. 1, pp. 85–171, 2002.

[16] B.-J. Koops, M. Lips, S. Nouwt, C. Prins, and M. Schellekens, "Should self-regulation be the starting point?," in *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, B.-J. Koops, C. Prins, M. Schellekens, and M. Lips, Eds., T.M.C. Asser Press, The Hague , Netherlands, pp. 109–149, 2006.

[17] R. A. Posner, "The right of privacy," *Georgia Law Review*, vol. 12, no. 3, pp. 393–422, 1978.

[18] R. A. Posner, "The economics of privacy," *The American Economic Review*, vol. 71, no. 2, pp. 405–409, 1981.

[19] G. J. Stigler, "An introduction to privacy in economics and politics," *The Journal of Legal Studies*, vol. 9, no. 4, pp. 623–644, 1980.

[20] K. C. Laudon, "Markets and privacy," *Communications of the ACM*, vol. 39, no. 9, pp. 92–104, 1996.

[21] S. Li, W. Yufan, and R. Bao, "Da shuju, geren xinxi he jiage qishi: Jiyu chuizhi chayihua shuangguatou moxing de fenxi" [Big data, personal information protection and price discrimination: Based on a vertically differentiated duopoly model]," *Jingji yanjiu/Economic Research Journal*, vol. 2021, no. 1, pp. 43–57, 2021.

[22] Y. Chen, ""Da shuju shashu? pingtai jiage qishi de shi yu fei" [Right and wrong of price discrimination of platforms]," Jingji cankao Bao/Economic Information Daily, 2018, http://www.eeo.com.cn/2018/0822/335242.shtml.

[23] A. Acquisti and H. R. Varian, "Conditioning prices on purchase history," *Marketing Science*, vol. 24, no. 3, pp. 367–381, 2005.

[24] C. M. Cassidy and B. Chae, "Consumer information use and misuse in electronic business: an alternative to privacy regulation," *Information Systems Management*, vol. 23, no. 3, pp. 75–87, 2006.

[25] M. S. Gal and O. Aviv, "The competitive effects of the GDPR," *Journal of Competition Law and Economics*, vol. 16, no. 3, pp. 349–391, 2020.

[26] J. Campbell, A. Goldfarb, and C. Tucker, "Privacy regulation and market structure," *Journal of Economics and Management Strategy*, vol. 24, no. 1, pp. 47–73, 2015.

[27] Y.-Z. Du and L.-D. Jia, "*Zutai shijiao yu dingxing bijiao fenxi (QCA): Guanli xue yanjiu de yitiao xin daolu* [Configuration conditions and qualitative comparative analysis (QCA): a new approach to management research]," *Guanli shijie/Management World Monthly*, vol. 6, pp. 155–167, 2017.

[28] E. Thomann and M. Maggetti, "Designing research with qualitative comparative analysis (QCA): approaches, challenges, and tools," *Sociological Methods & Research*, vol. 49, no. 2, pp. 356–386, 2020.

[29] A. Marx, *Towards More Robust Model Specification in QCA Results from a Methodological experiment*, American Sociological Association, Philadelphia, PA, USA, 2006.

[30] R. H. Peters and L. A. Taylor, "Intangible capital and the investment-q relation," *Journal of Financial Economics*, vol. 123, no. 2, pp. 251–272, 2017.

[31] C. Ragin, "Net effects analysis versus configurational analysis: an empirical demonstration," in *Redesigning Social Inquiry: Fuzzy Sets and beyond*, C. C. Ragin, Ed., pp. 190–212, The University of Chicago Press, Chicago, IL, USA, 2008.

[32] J. S. Bain, *Industrial Organization*, Wiley, Hoboken, NJ, US, 1968.

[33] J. T. Campbell, D. G. Sirmon, and M. Schijven, "Fuzzy logic and the market: a configurational approach to investor perceptions of acquisition announcements," *Academy of Management Journal*, vol. 59, no. 1, pp. 163–187, 2016.

[34] B. Rihoux and C. C. Ragin, Eds., *Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques*, Sage Publications, Thousand Oaks, CA, US, 2009.

[35] C. Q. Schneider and C. Wagemann, *Set-theoretic Methods for the Social Sciences: A Guide to Qualitative Comparative Analysis*, Cambridge University Press, Cambridge, UK, 2012.

[36] C. Cheng and L.-D. Jia, "*Woguo qiye kuaguo binggou qudong jizhi yanjiu: Jiyu qingxi ji de dingxing bijiao fenxi* [Research on the driving mechanisms of Chinese enterprises' cross-border M&A: crisp-set qualitative comparative analysis]," *Nankai Business Review*, vol. 19, no. 6, pp. 113–121, 2016.

[37] M. Zhang, W.-H. Chen, and H.-L. Lan, ""*Zhongguo qiye "ping shenme" wanquan binggou jingwai gaoxin jishu qiye—jiyu 94 ge anli de mohu ji dingxing bijiao fenxi (fsQCA)* [Why do Chinese enterprises completely acquire foreign high-tech enterprises: a fuzzy set qualitative comparative analysis (fsQCA) based on 94 cases]," *Zhongguo gongye jingji/China Industrial Economics*, vol. 2019, no. 4, pp. 117–135, 2019.

[38] V. F. Misangyi and A. G. Acharya, "Substitutes or complements? A configurational examination of corporate governance mechanisms," *Academy of Management Journal*, vol. 57, no. 6, pp. 1681–1705, 2014.

[39] R. G. Bell, I. Filatotchev, and R. V. Aguilera, "Corporate governance and investors' perceptions of foreign ipo value: an institutional perspective," *Academy of Management Journal*, vol. 57, no. 1, pp. 301–320, 2014.

[40] J. Wu, W. An, X. Zheng, and J. Zhang, "How business model designs influence firm growth in a transforming economy: a configurational perspective," *Management and Organization Review*, vol. 17, no. 2, pp. 226–253, 2021.

[41] L. White, A. Lockett, G. Currie, and J. Hayton, "Hybrid context, management practices and organizational performance: a configurational approach," *Journal of Management Studies*, vol. 58, no. 3, pp. 718–748, 2021.

[42] N. Newman, "Search, antitrust, and the economics of the control of user data," *Yale Journal on Regulation*, vol. 31, no. 2, pp. 401–454, 2014.

[43] M. Stucke and A. Grunes, "Dancing around data," 2021, http://thehill.com/blogs/congress-blog/technology/226502-dancing-around-data Accessed.

[44] M. E. Stucke and A. P. Grunes, *Debunking The Myths over Big Data and Antitrust*, CPI Antitrust Chronicle. University of Tennessee Legal Studies, Knoxville, TN, USA, 2015.

[45] P. Swire and Y. Lagos, "Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique," *Maryland Law Review*, vol. 72, no. 2, pp. 335–380, 2013.

[46] S. Pötzsch, "Privacy awareness: a means to solve the privacy paradox?," in *The Future of Identity in the Information Society*, V. Matyáš, S. Fischer-Hübner, D. Cvrček, and P. Švenda, Eds., pp. 226–236, Springer, 2009.

[47] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, "The effect of online privacy information on purchasing behavior: an experimental study," *Information Systems Research*, vol. 22, no. 2, pp. 254–268, 2011.