北京大学中国经济研究中心
China Center for Economic Research
讨论稿系列
Working Paper Series

E2026006 2026-04-21

State Ownership and Corporate Compliance：Evidence from China's Cybersecurity Law

Shengqiao Lin Xuan Wang Lixing Li Jiayi Hou

Abstract

How does state ownership influence corporate compliance? Existing studies offer two opposing views: state connections may invite regulatory forbearance and encourage noncompliance or may promote greater compliance due to political control. We argue that both dynamics coexist, and the net effect depends on the strength of state ties. Using China's Cybersecurity Law as a natural experiment, we probe this debate, empirically drawing on two original datasets: (1) an app–month panel tracking the security performance of China's top 5% most downloaded mobile apps and (2) the national business registration database covering all Chinese firms. Our difference-in-differences analyses reveal a nonlinear relationship: firms with strong state ties quickly complied with regulatory requirements by reducing security loopholes, and weakly connected firms showed lower compliance than purely private ones. Further analysis suggests regulatory compliance is driven by a dual mechanism: constraint by political control from above and reinforcement by firm-level risk management from within.

Keywords: State–business Relations, Digital Regulation, Corporate Compliance, China

State Ownership and Corporate Compliance:
Evidence from China's Cybersecurity Law*

Shengqiao Lin Xuan Wang Lixing Li Jiayi Hou

First Version: March 2025
This Version: January 2026

Abstract

How does state ownership influence corporate compliance? Existing studies offer two opposing views: state connections may invite regulatory forbearance and encourage noncompliance or may promote greater compliance due to political control. We argue that both dynamics coexist, and the net effect depends on the strength of state ties. Using China's Cybersecurity Law as a natural experiment, we probe this debate, empirically drawing on two original datasets: (1) an *app–month* panel tracking the security performance of China's top 5% most downloaded mobile apps and (2) the national business registration database covering *all* Chinese firms. Our difference-in-differences analyses reveal a nonlinear relationship: firms with strong state ties quickly complied with regulatory requirements by reducing security loopholes, and weakly connected firms showed lower compliance than purely private ones. Further analysis suggests regulatory compliance is driven by a dual mechanism: constraint by political control from above and reinforcement by firm-level risk management from within.

Keywords: State–business Relations, Digital Regulation, Corporate Compliance, China

*Lin, Assistant Professor, Department of Political Science, University of Toronto (shengqiao.lin@utoronto.ca). Wang, Assistant Professor, China Center for Economic Research and National School of Development, Peking University. Li, Professor, China Center for Economic Research and National School of Development, Peking University. Hou, Postdoctoral Researcher, Faculty of Business and Economics, University of Hong Kong. We note that the first two authors contributed equally to this manuscript and should be recognized as co–first authors. We appreciate comments from Martin Dimitrov, Lingnan He, Xiaobo Lü, and Kunyuan Qiao, and thank the panelists at the Chinese Politics Mini Conference at APSA 2025, the *Political Economy of Government and Business* conference hosted by the Weatherhead Center for International Affairs at Harvard University, the *Politics and Technology in Non-Democratic Contexts* conference hosted by NYU Abu Dhabi, the *Research XChange Workshop* hosted by the Harvard Center for International Development, the Cambridge Chinese Political Research Workshop, and the *Chinese Political Speaker Series*. We appreciate excellent research assistance from Tianyu Huang. All remaining errors are our own.

1 Introduction

Regulatory politics is often theorized as a contest between the state and private firms: the state designs and enforces rules to advance policy goals, and private firms respond strategically while seeking to maximize shareholder value (Stigler, 1971; Baldwin, Cave and Lodge, 2011; Viscusi, Harrington and Sappington, 2018; Wilson, 2021). Yet the resurgence of state capitalism documented in recent studies may challenge this arm's-length view (Alami and Dixon, 2024). Governments around the world increasingly invest in, and become shareholders of, ostensibly private firms, especially in strategic industries (Musacchio and Lazzarini, 2014; Cazurra, 2018; Babic, 2023). When the state is simultaneously regulator and shareholder, it occupies a dual role as both player and referee (Konisky and Teodoro, 2016). This development raises a new question: how does state ownership affect regulation? In particular, do state-connected firms comply more or less with regulation?

Existing research offers two competing perspectives (Zhang, Marquis and Qiao, 2016). One argument emphasizes the *buffering* effects of state ties, suggesting that state-connected firms often enjoy preferential treatment or forbearance from the government, allowing them to prioritize profit maximization and opportunistic behavior over regulatory conformity (Harding et al., 2023; Holland, 2015; Heitz, Wang and Wang, 2023). State ownership thus functions as a mechanism of risk management, dampening firms' incentives to adjust behavior in response to new regulations. A contrasting argument highlights the *binding* effects of state ties on corporate compliance. Equity positions in firms equip the state with the capacity to directly influence corporate strategies, appoint key personnel, and shape organizational priorities from within (Ennser-Jedenastik, 2014; Konisky and Teodoro, 2016; Leutert and Vortherms, 2021). Under this mechanism, the state embeds connected firms into its broader governance agenda through corporate decision making, aligning business strategy making more closely with regulatory requirements and policy objectives (Bertrand et al., 2020; Naoi, Shi and Zhu, 2022; Shleifer and Vishny, 1997).

To empirically adjudicate between *buffering* and *binding* effects, we examine corporate responses to China's 2016 Cybersecurity Law. This case provides strong leverage for three reasons.

First, the law imposes costly security requirements that generate meaningful firm-level variation in compliance efforts. Second, focusing on a single institutional setting avoids cross-national confounders, especially differences in enforcement capacity. Third, because China is often viewed as a high-capacity state in monitoring and enforcement, the case provides a conservative test: variation in firms' compliance and its implications for regulatory effectiveness should be at least as relevant in contexts where top-down enforcement is weaker.

Our analysis draws on two original datasets that offer rare, fine-grained measures of both compliance behavior and state ownership. The first is an app–month panel tracking the security performance of mobile applications in the top 5% of downloads in China, covering more than 6,000 apps. By focusing on month-to-month changes in security vulnerabilities before and after the law, we avoid biases common to studies that rely on detected violations, enforcement actions, or self-reported misconduct. The second dataset comprises nationwide firm registration records for *all* firms registered in mainland China, which we use to construct a continuous measure of each firm's degree of state ownership, including indirect and minority stakes. This continuous measure moves beyond conventional binary classifications (i.e., state-owned versus private) and enables a more nuanced assessment of how state ownership shapes corporate compliance.

Difference-in-differences analyses reveal the coexistence of both *binding* and *buffering* effects, contingent on the strength of firms' state ties. Compared with purely private firms, companies with substantial state ownership, particularly those officially registered as state-owned enterprises (SOEs), responded promptly to the law by improving the security performance of their applications by about 5–7%. In contrast, relative to private firms, those with minor state ownership exhibited weaker compliance and achieved roughly 2–3% smaller improvements in software security after the law's enactment. These patterns are consistent across subgroup estimations and quadratic specifications. Overall, the results indicate that strong state ties generate binding effects, whereas weak state ties confer buffering effects.

Further analyses show that corporate compliance is shaped by both top-down political control and firm-level risk management. Binding effects appear only among firms with shorter in-

vestment distances from state shareholders; that is, those more directly connected to the state through ownership ties tend to respond more promptly to the regulation. At the same time the influence of state ownership forms part of firms' risk management strategies. Both the binding and buffering effects emerge only under moderate levels of regulatory risk and compliance costs but not when such risks or costs are extremely high or low.

This article contributes to the literature on political connections by engaging the binding–buffering debate in regulatory politics (Hillman, Keim and Schuler, 2004; Parker and Nielsen, 2011; Short, 2021; Zhang, Marquis and Qiao, 2016). Existing studies often conceptualize state–business connectedness as a dichotomous attribute, either present or absent, thereby overlooking its gradational nature (Granovetter, 1983). We advance a continuum-based framework that helps reconcile mixed findings by showing that the intensity of state ties conditions whether they operate as a *buffering* or *binding* force. In doing so, we move beyond binary classifications and simple comparisons between state-owned and private firms. Importantly, our mechanisms do not hinge on authoritarian institutions per se but arise from the state's dual role as shareholder and regulator. Similar arrangements exist in democracies through public equity stakes, sovereign wealth funds, and policy-driven state investment, though institutional constraints may condition their effects (Ennser-Jedenastik, 2014; Musacchio and Lazzarini, 2014; Konisky and Teodoro, 2016).

Furthermore, this article highlights the governance implications of state–business relations in weakly institutionalized settings. In advanced democracies, private businesses often capture public institutions and distort policymaking for private gain, undermining the public good (Stigler, 1971; Busemeyer and Thelen, 2020; Valdez, 2022). In China's party-state capitalism, by contrast, the state increasingly penetrates the private sector for political ends, even at the cost of higher managerial burdens for firms (Colonnelli, Li and Liu, 2024; Megginson, 2017; Pearson, Rithmire and Tsai, 2023); yet few studies have examined the governance consequences of this process. This article fills that gap empirically, showing that expanding state–business ties may ultimately undermine governance performance by enabling corporate opportunism and regulatory slack.

Finally, this article also contributes to our understanding of corporate political strategies.

Conventional wisdom emphasizes the advantages of political connections, including preferential access to government resources, regulatory leniency, and influence over policymaking (Fisman, 2001; Li et al., 2008; Earle and Gehlbach, 2015; Chen and Xu, 2023; Rexer, 2025). Recent research, however, highlights their potential costs, particularly their distorting effects on corporate strategy and market perceptions (Li, 2022; Wang, 2015). We identify a strategic "sweet spot" when cultivating political connections: firms maximize business interests when they maintain moderate, rather than strong, ties with the state (Granovetter, 1983).

2 How State Ownership Shapes Corporate Compliance

Although conventional wisdom on state–business relations emphasizes individual and informal ties, such as personal friendships, campaign contributions, revolving-door appointments, and positions in elected office (Fisman, 2001; Harding et al., 2023; Kung and Ma, 2018; Li, 2022; Szakonyi, 2020), recent scholarship has increasingly highlighted a broader resurgence of state ownership in the private sector, particularly amid intensifying international competition (Alami and Dixon, 2024; Babic, 2023; OECD, 2024). While China is well known for its extensive state investments and sprawling state-owned enterprise sector (Bai et al., 2021), similar dynamics are now visible elsewhere: a salient recent example is the United States government's decision to become a major shareholder in Intel, one of the world's largest semiconductor manufacturers, as well as in two major rare earth startups (Intel, 2025; MP Materials, 2025; Reuters, November 2025).

Existing research spans cross-national comparisons (Cazurra, 2018; Francis and Kubinec, 2025; James and Vaaler, 2018; Tihanyi et al., 2019) and regional or single-country studies, including work on African economies (Freyburg, Garbe and Wavre, 2022), Norway (Christensen, 2024), Russia (Panibratov and Michailova, 2019), and China (Naoi, Shi and Zhu, 2022), and consistently documents systematic differences in corporate strategy and performance between purely private firms and those with state ownership stakes. However, when it comes to regulatory behavior, this literature yields two contrasting expectations: the buffering and binding hypotheses (Zhang,

Marquis and Qiao, 2016). The buffering view holds that state ties insulate firms from regulatory scrutiny and thereby encourage noncompliance, whereas the binding view emphasizes state ownership as an instrument of political control that strengthens regulatory compliance.

2.1 Buffering Effect

On the one hand, state ownership serves as a buffer against regulatory enforcement. This buffering effect arises because the state's dual role as regulator and shareholder undermines enforcement credibility, the alignment of state–business interests fosters regulatory forbearance, and informational collusion enables strategic noncompliance.

First, when acting simultaneously as a regulator and a stakeholder, the state assumes a dual role that generates conflicts of interest undermining effective oversight and accountability (Milhaupt and Pargendler, 2017; Yasuda, 2021). This "player–referee" dilemma erodes the credibility of enforcement and weakens the threat of punishment that normally sustains compliance. For instance, Konisky and Teodoro (2016) find that government-owned utilities in the United States are more likely to violate regulations yet less likely to be fined as regulators hesitate to sanction their governmental counterparts. Similarly, Hou and Moore (2010) show that in China, firms with higher state ownership faced fewer penalties for financial fraud because regulators and SOEs were embedded within the same political hierarchy. Even where ownership and regulatory authority are formally separated, state ownership itself can signal a firm's de facto political protection to lower-level bureaucrats who determine enforcement intensity, thereby fostering regulatory leniency (Gordon and Hafer, 2005; Hou, 2019).

Second, equity ties between governments and firms create overlapping interests that often lead to regulatory forbearance (Fisman and Wang, 2015; Harding et al., 2023; Holland, 2015). The performance of state-connected firms directly affects government outcomes like economic growth, fiscal revenues, and policy implementation, which in turn shape officials' career advancement (Liu et al., 2024; Oi, 1995). When bureaucratic and corporate incentives align, regulators may tolerate noncompliance rather than risk undermining growth targets or employment sta-

bility. In Ukraine's electricity sector, regulators refrained from penalizing state-owned utilities to avoid disrupting public services and further straining the government's finances (Berg, Lin and Tsaplin, 2005). Likewise, in Brazil, the state-controlled oil company Petrobras benefited from regulatory leniency in order to keep fuel prices low in pursuit of macroeconomic objectives (Milhaupt and Pargendler, 2017).

Third, state-connected firms often enjoy superior access to regulatory information (Truex, 2014). These firms obtain privileged access to information about regulatory expectations and policy adjustments through state shareholders and may even receive advance notice of enforcement details and inspection timing (Guo, Pan and Tian, 2024). Informational advantages enable firms to strategically calibrate compliance or obscure violations, minimizing costs while evading penalties, especially during campaign-style enforcement, when the government abruptly tightens regulatory scrutiny in targeted sectors (He and Peng, 2022). By contrast, private firms lacking such access are prone to either excessive caution or delayed responses to new enforcement pressures. For instance, local state-owned coal mines in China often received advance notice of inspections, allowing them to suspend production and hide safety violations. As Nie (2017, p. 115) notes, "before the inspection team could come, factories had closed temporarily."

2.2 Binding Effect

On the other hand, state ownership functions as a mechanism of political control that binds firms to regulatory goals. This binding effect arises when political appointees align managerial behavior with policy objectives, state shareholdings allow direct intervention in corporate decisions, and firms' dependence on state resources strengthens compliance incentives.

First, state ownership reinforces political control through personnel appointments (D'Souza and Nash, 2017; Kikeri and Burdescu, 2020; Leutert and Vortherms, 2021), which tighten the principal–agent link between the state and corporate managers, reducing managerial autonomy while ensuring compliance. Politically appointed executives internalize policy directives and align corporate strategies with government priorities—even at the expense of business perfor-

mance (Alok and Ayyagari, 2020; Bertrand et al., 2018, 2020; Shleifer and Vishny, 1997; Willner, 2001). Noncompliance is not merely a managerial failure but a signal of political disloyalty. Evidence from Eastern Europe shows that board appointments in SOEs remain highly politicized, government offices often making direct nominations without competitive selection processes (Böwer, 2017). In Austrian SOEs, managers affiliated with governing parties enjoying longer tenures (Ennser-Jedenastik, 2014). These patterns indicate that personnel control strengthens regulatory compliance through hierarchical accountability.

Second, even without direct appointments, minority state shareholders can influence corporate decision-making through internal channels (Haggard, Maxfield and Schneider, 2018; Lioukas, Bourantas and Papadakis, 1993). Such influence may occur via board representation, strategic consultation, or implicit veto power over key business decisions despite limited equity ownership (Liu et al., 2024; Pargendler, Musacchio and Lazzarinim, 2013; Zhang et al., 2024). Lazzarini and Musacchio (2018) show that state investors in Brazil used board seats to advance developmental goals like employment stabilization and price control, aligning private firms with government priorities. A similar pattern appeared in France, where the government temporarily raised its stake in Renault in 2015 to block governance reforms, overriding other shareholders (Reuters, 2015). Colonnelli, Li and Liu (2024) show that such excessive political interference and weakened managerial autonomy discourage private investors from co-investing with governments.

Third, firms' dependence on government resources amplifies the informal influence of state ownership in corporate decision making (Pfeffer and Salancik, 1978). Extensive research shows that state ties provide access to critical policy resources, including procurement contracts, preferential loans, administrative approvals, and property rights security in transition economies (Che and Qian, 1998; Fisman, 2001; Kung and Ma, 2018). Noncompliance with regulatory demands can lead to the loss of these preferential treatments, threatening firms' survival and reinforcing compliance incentives. Formerly state-owned firms in postcommunist economies, often comply with government directives to maintain property rights security(Frye, 2006). State-connected firms in China similarly pay taxes above statutory requirements to help local governments meet fiscal

targets in exchange for continued credit access (Han, Li and Oi, 2022).

2.3 Dual Impact: Binding and Buffering

We argue that binding and buffering effects coexist, and their relative strength depends not simply on whether a firm is connected to the state but on the intensity of that connection. These seemingly contradictory findings may stem from the tendency to conceptualize state–business ties as a dichotomous attribute, either present or absent. Although this binary approach helps identify the general effects of state ownership, it overlooks its gradational nature and the distinct dynamics operating within various levels of ownership (Granovetter, 1983).

More specifically, as state ownership increases, both political control and regulatory leniency expand—but at different rates. On the one hand, state–business equity linkages foster regulatory leniency through incentive-compatible arrangements that align firms' performance with government objectives (Berg, Lin and Tsaplin, 2005; Konisky and Teodoro, 2016; Yasuda, 2021). Greater state ownership brings corporate and governmental interests into closer alignment, prompting regulators to tolerate minor violations, thereby encouraging noncompliance. On the other hand, degrees of state shareholding entail a range of forms of political control (Francis and Kubinec, 2025; Leutert and Vortherms, 2021; Musacchio and Lazzarini, 2014). When state ownership is limited, governmental influence remains informal. Once it surpasses a critical threshold and exceeds that of private investors, the state becomes a dominant shareholder with formal authority over managerial appointments, sharply increasing political oversight.

The observed outcomes, therefore, reflect a shifting balance between these countervailing forces of political control and regulatory leniency. Whereas leniency tends to rise gradually with state ownership, political control escalates quickly once ownership concentration crosses a critical threshold. Consequently, the relationship between state ownership and compliance is nonlinear, shifting from buffering to binding as state influence deepens.

To examine this variation, we distinguish between two types of firms with state ownership. The first category comprises **state-owned enterprises (SOEs)**, in which the state holds a domi-

nant equity stake. SOEs generally face lower regulatory risks than private firms but are subject to stronger political control. Their senior executives are politically appointed, and their career advancement depends not only on business performance but also on alignment with state priorities. For these firms, compliance with government directives is not merely a regulatory obligation but also a demonstration of political loyalty. Hence, even when regulatory penalties are unlikely, political incentives compel SOE managers to prioritize obedience over profitability.

The second category comprises **state-connected enterprises (SCEs)**, privately owned firms with minor or indirect state ownership (Bai et al., 2021). SCEs face lower regulatory risks than private firms but are subject to weaker state control than SOEs. When responding to regulation, they benefit from regulatory forbearance and informational advantages that enable strategic noncompliance. Even when violations are detected, state ties can facilitate lenient enforcement. With lower expected penalties, SCEs enjoy the buffering benefits of state ties while avoiding political oversight, making them comply less with regulatory requirements than purely private firms.

Together, we hypothesize a nonlinear relationship between state ownership and corporate compliance, which initially declines as state ownership increases from zero (buffering effect). Beyond an intermediate threshold, however, further increases in state ownership strengthen political control and enhance compliance (binding effect). At low to moderate levels of state ownership, firms can leverage state ties for regulatory forbearance, whereas at higher levels, state control compels compliance. We therefore expect an U-shaped relationship between state ownership and compliance, summarized in the following hypotheses:

Hypothesis 1. *Relative to private firms, state-owned enterprises exhibit higher compliance.*

Hypothesis 2. *Relative to private firms, state-connected enterprises exhibit lower compliance.*

3 Context: State Capitalism and Digital Regulation in China

3.1 State–Business Equity Ties in China

Because of the legacy of its planned economy, China has maintained a vast state-owned sector. As of the end of 2024, state-owned enterprises and financial institutions held total assets of approximately USD 125 trillion, including 85 firms listed in the 2023 Fortune Global 500 (Xinhua News, 2025). The state-owned sector accounts for roughly 40% of total market capitalization in China's domestic stock markets and generates about 50% of total revenue while holding monopolistic positions in strategic sectors like telecommunications, energy, and finance (Leutert, 2024).

At the same time, however, China's private sector constitutes the primary body of market activity. In 2017, four decades after the launch of the Reform and Opening period, the private economy in China exhibited what is commonly referred to as the "56789" structure: contributing over 50% of tax revenue, over 60% of GDP, over 70% of technological innovation, over 80% of urban employment, and over 90% of the total number of enterprises (Paper News, 2018).

Nevertheless, the boundary between the state and private firms in China has become increasingly blurred (Bai et al., 2021). Beyond personal ties formed through revolving-door employment and kinship networks, a large share of private firms have forged direct or indirect equity linkages with the state, with governments assuming roles as either major or minority shareholders. The emergence of these equity relationships reflects both industrial policy objectives and broader economic goals: on the one hand, government investment as an instrument of industrial policy provides strategic emerging industries with financial support, enabling firms to scale up and invest in R&D; on the other hand, it allows the state to retain control over critical sectors such as energy and finance, thereby safeguarding macroeconomic stability (Pearson, Rithmire and Tsai, 2023; Leutert, 2024). For firms, these arrangements constitute a formal, organizational type of political connection through which they can secure regulatory forbearance and privileged access to government-controlled resources (Chen and Xu, 2023; Lin, 2025*b*).

This deepening penetration of state capital unfolds through multiple channels. SOEs have ex-

panded beyond traditional monopolistic sectors and increasingly acquired equity stakes in private firms. By 2018 more than 60% of China's privately listed firms had state-connected shareholders, a share that has continued to rise as SOEs increasingly invest in private firms in strategic industries (Sun and Liu, 2021). Beyond SOEs, both central and local governments have established a wide range of investment vehicles, commonly referred to as "Government Guidance Funds" (Colonnelli, Li and Liu, 2024; Pan, Zhang and Wu, 2021; Wei, Ang and Jia, 2023). Between 2015 and 2021, more than 1,500 such funds were launched, accounting for 40% of all equity investments and 50% of total funds raised over the past decade (Lin, 2025*b*). As a result, a growing number of small and medium-sized enterprises and high-profile unicorns, particularly in emerging sectors, now include minor state capital in their ownership structures.

These state equity linkages are often more invisible than officially recognized. Under current Chinese regulations, firms with majority state ownership are expected to register as SOEs. In practice, however, many private firms hold small or indirect state stakes without formally registering as SOEs. A representative example is Ant Group. Following China's internet crackdown in 2021, the company introduced state shareholders as its second-largest investor after divesting its credit and lending businesses; yet it continued to operate as a private firm (Lin, 2025*b*). Our data show that only 15% of firms with state capital are officially registered as SOEs.

3.2 China's Cybersecurity Law

China first mentioned the need to "accelerate the drafting of the Information Security Law" in 2003 (General Office of the CPC Central Committee, 2003). In 2014, when Xi Jinping established *the Central Leading Group for Cybersecurity and Informatization*, safeguarding cybersecurity was formally placed on the agenda; however, local governments paid limited attention to the remediation of security vulnerabilities. In 2015 the National Computer Network Emergency Response Technical Team (CNCERT) reported nearly 24,000 incident-level security vulnerabilities involving government agencies and critical information systems, yet most were not addressed in a timely manner. In fact, the patching rate for government websites one month after notification

was only 52.7% (CNCERT, 2016).

In June 2015 the Standing Committee of the National People's Congress conducted the first reading of the draft Cybersecurity Law, which was then made public and opened for nation-wide public comment. The second draft reading in June 2016 was followed by a third reading later in November, when the law was adopted with 154 votes in favor and one abstention. It officially took effect in June 2017. The law focuses on four main areas: (1) regulating the collection and use of personal information, (2) clarifying the security responsibilities of network operators, (3) emphasizing the protection of critical information infrastructure, and (4) restricting the transmission of sensitive data. Enterprises and responsible personnel who fail to fulfill these obligations may face administrative warnings and fines. In severe cases, the relevant authorities may order the suspension of operations, business closure, website shutdown, revocation of business licenses, or other penalties. Notably, the security of network products and services is a key concern throughout the law. Articles 21, 22, 25, and 26 of the final version emphasize network operators' obligation to inform both users and authorities about security flaws and vulnerabilities and to prepare security contingency plans. We include bilingual excerpts of these articles in Appendix A.

The main substantive provisions of the Cybersecurity Law were largely finalized during the second reading. As shown in Appendix Table D.1, we compared the text similarity between different versions of the law and found significant changes between the initial draft and the second reading but near-identical language after the second reading (with similarity reaching 85% to 98%). One of the major changes between the first and second drafts was the addition of a corporate obligation to report security vulnerabilities to the relevant authorities, accompanied by clearly defined penalties. Whereas the first draft relied on general warnings, orders to correct, and fines, the second reading introduced specific monetary ranges, categorized the types of infractions, and distinguished responsibilities between organizations and individuals. Particularly, it established a two-tiered penalty mechanism that allows for fines on both the company (ranging from 50,000 to 500,000 RMB) and the responsible personnel (up to 100,000 RMB). Following the second reading, the law received preliminary approval and entered the final legislative stage.

The establishment of clear responsibilities and penalty mechanisms made network operators more accountable, thereby increasing their incentives to improve security performance, especially in addressing and fixing software loopholes, which pose operational risks to firms in two main ways. First, if a vulnerability exists and the company fails to fulfill its disclosure obligation, it may face administrative penalties if detected by regulators. Second, if the vulnerability leads to a security incident, such as a data breach or service disruption, the consequences can be more severe, including potential suspension or shutdown of business operations.

Following the law's passage, regulatory enforcement escalated markedly. In 2017 more than 20,000 websites were shut down under legal authority, a tenfold increase from 2016 (Cyberspace Administration of China, 2016, 2018). Government cybersecurity authorities and police engage in regulation at three stages: ex-ante, interim, and ex-post. Ex-ante regulation involves proactive inspections of key industries and apps by enforcement agencies. These inspections may also be triggered by media reports or user complaints and can lead to mandated rectifications based on the findings (Ministry of Industry and Information Technology, 2019). Interim regulation refers to instances where, during investigations of other cases, security vulnerabilities are identified and penalized under the provisions of the Cybersecurity Law (Ministry of Public Security, 2019). Ex-post regulation occurs after major security incidents have taken place. Authorities initiate investigations in such cases, to determine whether the incident resulted from an operator's failure to fulfill obligations, for example, the obligation to report vulnerabilities in a timely manner (China Banking and Insurance Regulatory Commission, 2019).

4 Research Design

4.1 Data

Existing evidence remains inconclusive because of persistent empirical challenges. In measuring state ownership, most studies rely on firm registration data or identify the ultimate controlling shareholder, typically coding this information as binary indicators rather than continuous mea-

sures (Berg, Lin and Tsaplin, 2005; Ennser-Jedenastik, 2014; Naoi, Shi and Zhu, 2022). Such an approach obscures meaningful variation across different degrees of state ownership (Francis and Kubinec, 2025). Measuring compliance poses additional difficulties: corporate compliance is inherently difficult to observe, and prior studies often used the incidence of regulatory penalties or inspection as a proxy (Konisky and Teodoro, 2016; Gordon and Hafer, 2005; Rousseau, 2007). This indicator is, however, confounded by variation in enforcement intensity, obscuring the distinction between genuine compliance and selective enforcement (Holland, 2015; Zu and Lin, 2025).

To address these measurement challenges, we leverage two original datasets. First, we utilize the *Chinese Business Administrative Registration Database*, which provides detailed equity information for all firms in China. Using an iterative equity penetration method, we quantify the total state ownership of each firm. Specifically, we begin by identifying the state units, such as *State-owned Assets Supervision and Administration Commissions* (SASACs) and the *Ministries or Bureaus of Finance* at the national, provincial, and prefectural levels. We then trace the firms and financial institutions in which these state units invested directly as well as those that received investments indirectly through subsequent layers. Finally, we calculate the total proportion of shares in each firm that is ultimately controlled by the state across all levels through these equity ties. This approach yields a continuous measure of state ownership, allowing us to capture potential nonlinear effects.

Second, to more directly capture corporate regulatory compliance, we partnered with a third-party platform that conducted security assessments for every historical version of the top 5% most-downloaded Android apps in the Chinese mainland annually from 2012 to 2023 (N>1.65 million). These assessments examine whether the app versions contained security vulnerabilities, the severity of these vulnerabilities, and the number of software development kits (SDKs) embedded in each version. The scope and standards of vulnerability detection remained consistent, with each version assessed for 120 types of security loopholes. This process enabled us to construct an app–month panel dataset. For months without updates, we imputed the information from the current version. If multiple versions existed in the same month, we took the average

values. We treated apps without updates for 12 consecutive months as withdrawn. Notably, the third-party platform shared the assessment results with app developers as part of the security enhancement services they offered. Thus, developers were made fully aware of the security performance of their apps and were therefore able to make targeted improvements.[1]

To assess the impact of China's Cybersecurity Law, we analyze data from 2016 to 2017. After precisely matching the two datasets using firms' unique social credit codes, the final sample contains 89,672 observations, covering 4,558 corporate developers and 6,211 mobile applications. Among them, only 91 apps were developed by firms officially registered as state-owned enterprises, whereas 1,058 apps were developed by privately registered firms with indirect or minority state ownership. To capture firm-level heterogeneity, we further incorporate information from *Tianyancha*, a widely used business database in China that reports employment size, administrative penalties, software and patent registrations, and government procurement contracts. Descriptive statistics are reported in Appendix Table D.2.

4.2 Measurement

4.2.1 State Ownership: Binary and Continuous Measures

We measure a firm's state ownership in three ways. First, the variable ***Registered SOE*** is a binary indicator equal to 1 if a firm is registered as a state-owned enterprise. This includes wholly state-owned enterprises, enterprises absolutely controlled by state capital, and enterprises relatively controlled by state capital with effective control. In our sample, only 1,479 observations (1.6%), corresponding to 91 apps and 72 firms, fall into this category.

Second, we construct a continuous variable, ***SOE%***, which captures the total proportion of direct and indirect state capital in a firm, ranging from 0 to 1. A total of 18% of the sample has a nonzero *SOE%*, with a mean of 0.33, a median of 0.10, and a standard deviation of 0.38. To capture

[1]Due to confidentiality agreements with the data provider, the raw dataset cannot be publicly released. The data contain sensitive commercial information about app vulnerabilities that, if disclosed, could pose security risks to both developers and users. However, detailed summary statistics and the analysis code are available to enable replication and verification of our findings. Additional information on the data provider, detection procedures, and relevant national standards is provided in Appendix B.

potential nonlinear effects, we also include a squared term, $SOE\%^2$, in some model specifications.

Third, based on *SOE%*, we classify firms into three ownership groups: ***Private*** firms are those with no state capital; ***State-Connected Enterprises***, or ***SCEs***, have partial but minority state ownership (0 < SOE% < 50%); and *SOE-Owned Enterprises* or ***SOEs***, are those with at least 50% state ownership (SOE% ≥ 50%). In our sample, 82% of observations are classified as *Private* (3772 firms and 5153 apps), 13% as *SCEs* (550 firms and 769 apps), and the remaining 5% as *SOEs* (236 firms and 289 apps).

4.2.2 Compliance Outcome: App-Level Security Loopholes

We use the number of security loopholes to measure the level of corporate compliance with China's Cybersecurity Law. A reduction in the number of loopholes within an app indicates a higher level of compliance. This measure is justified based on a cost–benefit framework from the firm's perspective. First, the law places strong emphasis on the information security of mobile applications, holding developers accountable for user privacy and data breaches. Cybersecurity accidents caused by security loopholes, such as user privacy leaks, can result in penalty fines or even business suspension for app developers. As a result, the Cybersecurity Law creates strong incentives for firms to address and fix security vulnerabilities.

Second, fixing loopholes is costly for firms, making the observed reduction in loopholes a credible indicator of corporate compliance compared to other low-cost or purely symbolic actions. On the one hand, improving app security requires technical capacity and labor resources. Firms may have to increase investment in human capital or outsource this task, both of which involve additional costs. On the other hand, enhancing app security can sometimes hurt business performance. For example, some app developers heavily rely on advertising revenue and expose users to in-app advertisements through embedded software development toolkits (Ad SDKs). These Ad SDKs are often sourced from open-code repositories and developed by external programmers, making them a significant source of security loopholes in mobile apps.

Moreover, relative to existing evidence, this indicator is less affected by variations in gov-

ernment enforcement. These loopholes are assessed against a time-invariant technical standard, offering a more direct and objective measure of corporate compliance. In the sample, the number of loopholes ranges from 0 to 57, with a mean of 25.6 and standard deviation of 14.

4.2.3 Control Variables and Fixed Effects

We also include a rich set of firm-level covariates measured prior to treatment, as of the end of 2015. These include the number of software products operated by the firm (*Software*), the number of patents owned by the firm (*Patent*), the number of government-issued certificates such as Certificates of National High-Tech Companies (*Certificate)*, and the number of procurement contracts signed between the firm and government agencies (*Procurement*). Since these covariates are time-invariant within firms, we interact them with the time dummy in the model specifications.

In addition, we control for a rich set of fixed effects, including *Time* (measured by year and month), *Province* (based on the firm's registered location), *Sector* (defined according to the 13 industry categories designated by the China Securities Regulatory Commission), and *App Type* (classified into 16 categories by a third-party platform). To assess the impact of firms' profit models on corporate compliance, we use the number of (*Ad SDK*) embedded in each app and an index standardized within each *App Type* category.

4.3 Identification

Employing a difference-in-differences estimation, we use the preliminary approval of China's Cybersecurity Law in June 2016 as the treatment and code it as a binary variable (*Law*). The interaction between state ownership and treatment timing is considered exogenous for two reasons. First, state ownership is relatively stable and cannot be easily altered by firms in the short run. Changing ownership structure typically requires external financing and the introduction of new investors, which is far more costly and complex than fixing security loopholes. As a result, firms have limited ability and incentive to self-select into various ownership categories in anticipation of regulatory change. Second, China's legislative process is relatively opaque and driven by pub-

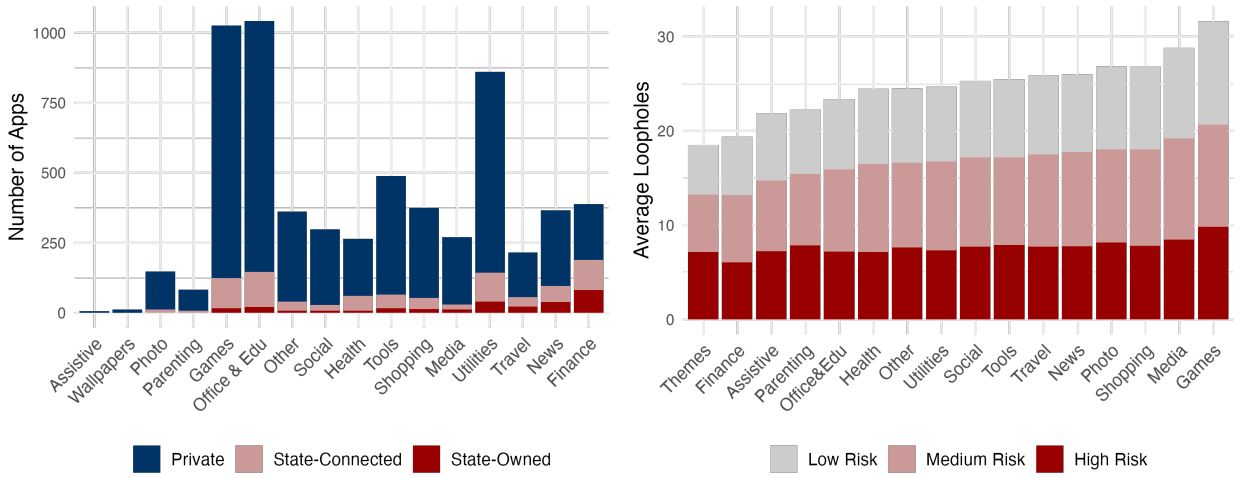
lic attention and top-down political priorities (Ding and Javed, 2020; Truex, 2020). For firms to foresee whether a particular law will be passed or to anticipate the specific provisions of the draft is difficult; thus their capacity to respond strategically in advance is limited. By leveraging these two variations, the following model is estimated:

$$Loopholes_{it} = \beta_1 \, State\ Ownership_i \times Law_t + \beta \, X_i \times Law_t + \sigma_i + \mu_t + \epsilon_{it},$$

where the outcome variable is the number of loopholes identified in app i at time t. *State Ownership*$_i$ refers to the ownership structure of the developer company of app i, measured in multiple ways. X_i denotes a vector of time-invariant firm-level covariates associated with app i. Specifically, β_1 is the parameter of interest, capturing the effect of state ownership on corporate compliance in response to the preliminary approval of China's Cybersecurity Law. σ_i represents app fixed effects, μ_t captures time-specific shocks, and ϵ_{it} is the error term. For further analysis, in some model specifications, we replace μ_t with *Time* $\times$ *Sector*, *Time* $\times$ *Province*, and *Time* $\times$ *App Type* fixed effects to account for location-, sector-, and app type-specific temporal shocks. All the standard errors are clustered at the app level.

5 Main Finding

We begin by presenting several graphical descriptive statistics. Figure 1 visualizes the number of apps and security loopholes across 15 app categories. Regarding state ownership, Figure 1a shows that the three categories with the highest proportion of state-connected and state-owned apps are *Finance and Investment*, *News and Information*, and *Travel*. This pattern largely reflects the state-dominated nature of China's financial institutions, news media, and public transportation sectors. In other areas like education, private firms constitute the majority, but a substantial share of apps remain state-connected. Figure 1b displays the average number of security loopholes by category. The riskiest three types are *Games*, *Video and Media*, and *Online Shopping* apps. The risk is likely the result of the heavy use of Ad SDKs embedded in these apps. These SDKs are often



(a) App Numbers **(b)** Loopholes

Figure 1: Descriptive Stats

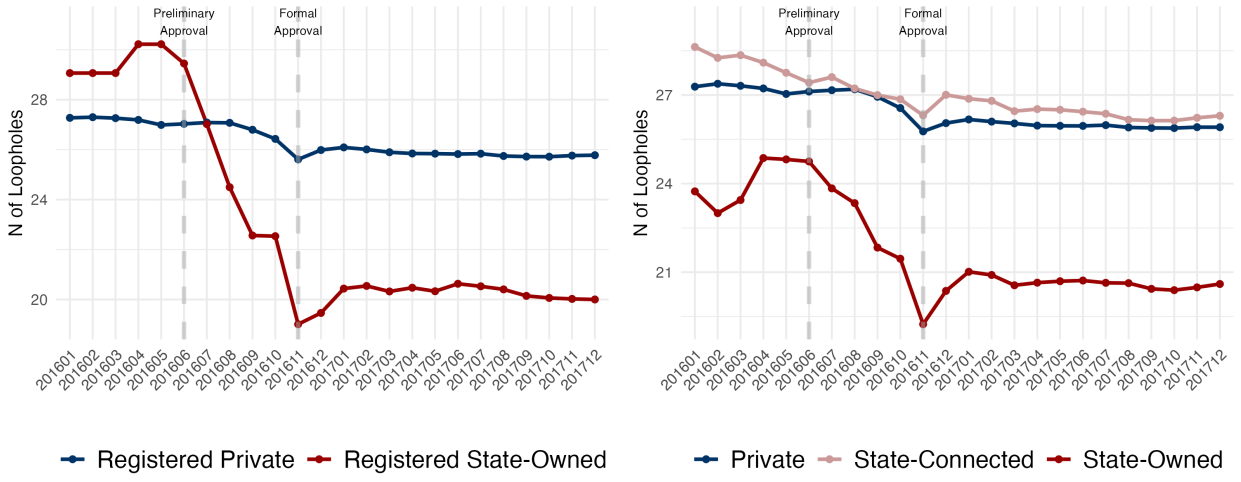
Note: Panel (a) plots the distribution of mobile applications across 15 categories, highlighting sectors with higher proportions of state-connected and state-owned apps, such as finance, news, and transportation. Panel (b) reports the average number of detected security loopholes by category. The riskiest categories include games, video and media, and online shopping, largely a result of the embedded advertising software development kits (Ad SDKs). All figures are based on the app–month panel used in the main analysis.

used to collect user data and deliver targeted ads, generating additional revenue for developers and frequently introducing significant security vulnerabilities.[2]

Figure 2 presents the temporal distribution of the outcome variables in 2016 and 2017. Figure 2a shows the average number of loopholes for firms registered as state-owned enterprises and those that are not. As indicated by the red line, apps developed by registered state-owned enterprises had a higher number of loopholes prior to the treatment. These firms rapidly improved their security performance following the preliminary approval of China's Cybersecurity Law and the publication of the law manuscript in June 2016, whereas other firms remained largely unchanged until the law's formal approval in November 2016.

Figure 2b displays the average number of loopholes for firms categorized by the level of state ownership. Similarly, apps developed by private firms remained relatively unchanged until the law's formal approval. Apps developed by firms with more than 50% state ownership exhibited

[2]Over the course of our study period, five specific types of security loopholes appeared most frequently across app-month observations. These include *Risk of SO File Tampering* (90%), *WebView Remote Code Execution Vulnerability* (86%), *Janus Signature Bypass Vulnerability* (82%), *Exported Activity Component Risk* (78%), and *Exported BroadcastReceiver Component Risk* (76%).



(a) Registration **(b)** State Ownership Group

Figure 2: Mean Loopholes by Firm Ownership Type

Notes: Panel (a) compares the average number of security loopholes between apps developed by SOEs and non-SOEs from 2016 to 2017. SOEs initially had more vulnerabilities but improved rapidly after the preliminary approval of China's Cybersecurity Law in June 2016. Panel (b) distinguishes private, state-connected (SCEs), and SOEs. SOE apps show a marked decline in loopholes, whereas SCEs exhibit weaker or reversed improvements. All data come from the app–month panel described in Section 4.

a sharp reduction in loopholes following the preliminary approval, with a slight rebound after the formal approval. The pattern for apps developed by firms with partial but less than 50% state ownership is slightly more complex: the average number of loopholes decreased faster than that of private firms but returned to a higher level after the law was formally approved. One possible explanation is that after the law's formal passage and initial enforcement, state ownership served as a buffer for SCEs, allowing them to scale back their efforts in maintaining high security performance, suggesting a potentially nonlinear impact of state ownership.

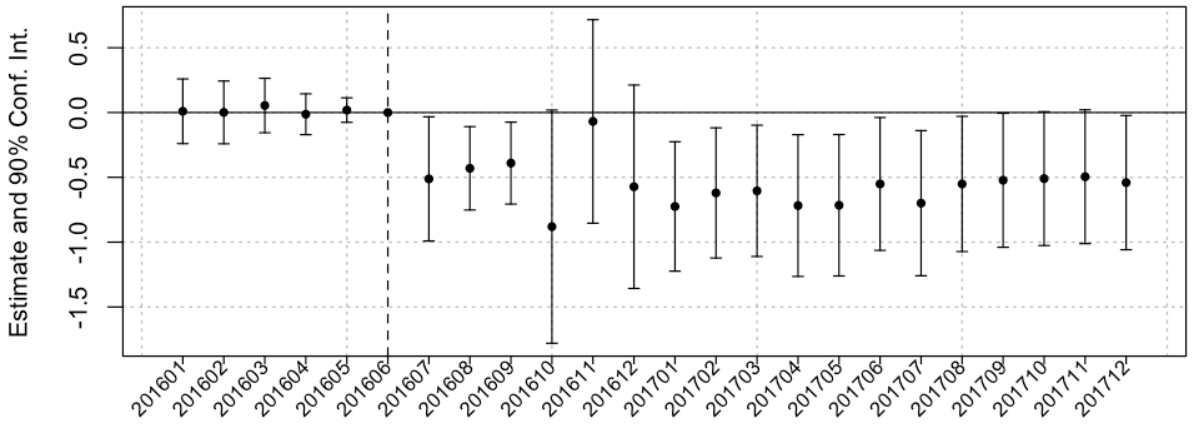
To quantify these effects, we conduct the analysis at the app–month level and present the results in Table 1. Models 1 to 3 employ difference-in-differences estimations to assess the impact on apps developed by registered state-owned enterprises. Model 2 includes additional fixed effects to control for sector-, province-, and app type-specific time shocks. Model 3 further adds a rich set of firm-level control variables in the form of $X_i \times Law_t$. The results remain consistent across all specifications, showing that registered SOEs reduce their loopholes by 2.3 units, roughly 10% of the mean outcome, in response to the Cybersecurity Law, relative to other apps.

Table 1: Main Finding: State Ownership and Corporate Compliance

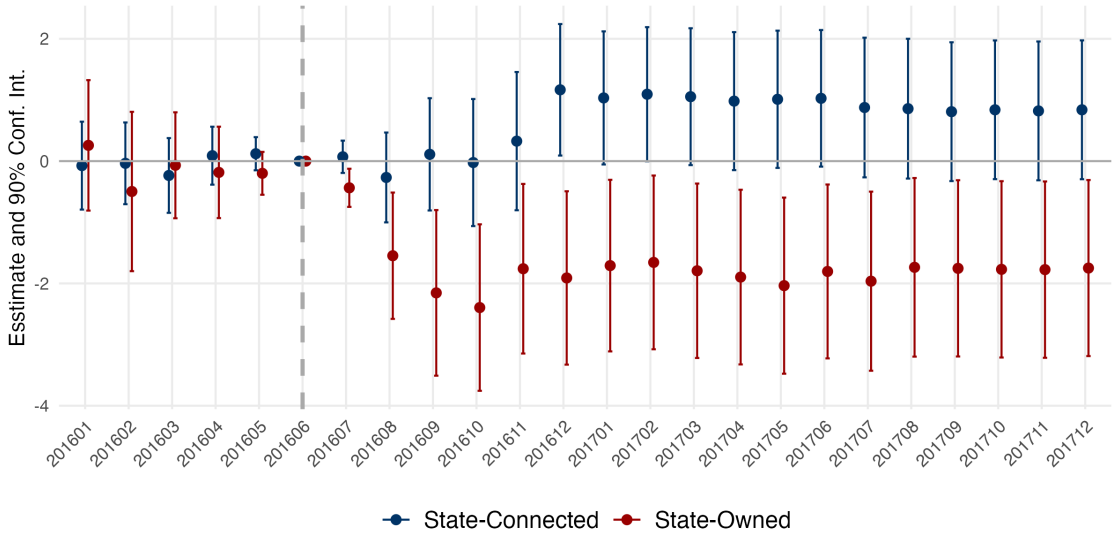
Dependent Variable:	Loopholes						
Control Group:	Registered Private Firms			Private/Connected	Private		
Model:	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Variables							
Registered SOE × Law	-0.572**	-2.34**	-2.38**				
	(0.270)	(1.04)	(1.04)				
State-Owned × Law				-1.82**	-1.66**		
				(0.803)	(0.764)		
State-Connected × Law					0.714		
					(0.617)		
SOE% × Law						-1.30	11.0*
						(0.913)	(6.28)
SOE%^{2} × Law							-13.0**
							(6.36)
Controls × Law			✓	✓	✓	✓	✓
Fixed-effects							
Time	✓						
App ID	✓	✓	✓	✓	✓	✓	✓
Time × App Type		✓	✓	✓	✓	✓	✓
Time × Province		✓	✓	✓	✓	✓	✓
Time × Sector		✓	✓	✓	✓	✓	✓
Fit statistics							
Observations	88,789	88,789	88,789	88,789	88,789	88,789	88,789
Squared Correlation	0.96283	0.96395	0.96397	0.96398	0.96400	0.96397	0.96402

Notes: Signif. codes: ***: 0.01, **: 0.05, *: 0.1. Robust standard errors clustered at the *App ID* level are in parentheses. The outcome variable is the number of loopholes. *Registered SOE* is a binary variable indicating whether a firm is registered as a state-owned enterprise; *SOE%* refers to the share of state capital in a firm. *Law* is a binary variable equal to 1 if the observation occurs after the preliminary approval of China's Cybersecurity Law in June 2016. *App Type* is a categorical variable with 8 levels. *Province* and *Sector* are categorical variables based on firm registration information. Control variables include the number of software and patents developed by a firm, professional certificates, and procurement contracts a firm received before 2016. Detailed results can be found in Table D.3.

In Model 4 we estimate the differential effects between apps developed by firms with more than 50% state ownership (SOEs) and those developed by other firms, including private firms and SCEs. The effect remains negative and statistically significant, suggesting that apps developed by SOEs improved their security performance following the policy change. Model 5 examines the heterogeneity of the effect across different levels of state ownership. The results show a consistent reduction in loopholes among apps developed by SOEs, the coefficients for SCEs remaining positive but statistically insignificant, indicating limited compliance among this group.



(a) Registered as State-owned vs. Others



(b) State Ownership Groups

Figure 3: Event Studies by Registration and State Ownership Groups

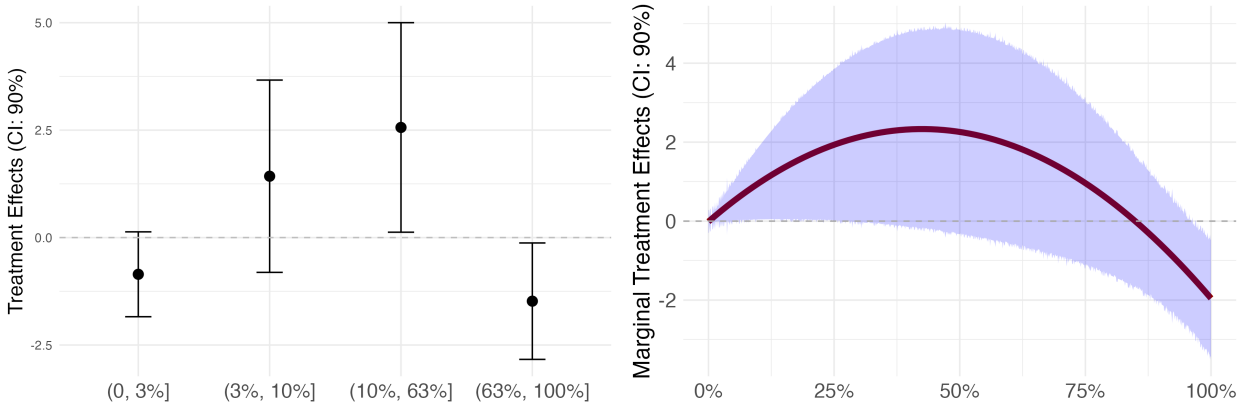
Note: Panel (a) presents the dynamic treatment effects comparing apps developed by registered SOEs and non-SOEs. Before the *Cybersecurity Law*, both groups followed similar trajectories, but SOEs improved significantly afterward. Panel (b) compares apps by levels of state ownership, showing that highly state-owned firms reduced security loopholes most sharply after the law's preliminary approval, whereas partially state-connected firms exhibited smaller or even reversed improvements following its formal passage. The analysis supports Hypotheses 1 and 2, suggesting heterogeneous and nonlinear compliance responses across ownership types. Regression results correspond to Models (3) and (5) in Table 1.

To verify the parallel trends assumption, we conduct event studies and present the dynamic treatment effects over time. Figure 3a displays the differences between firms registered as SOEs and others (Model 1 in Table 1). The insignificant coefficients prior to the treatment suggest that

the intergroup difference in the number of loopholes remained consistently limited before the enactment of the Cybersecurity Law. This supports the notion that in the absence of the Law, SOEs and non-SOEs would have followed similar trajectories in security performance. After the treatment the coefficients become significantly negative and remain so in most post-treatment periods, indicating registered SOEs improved their security performance more than the others.

Figure 3b examines changes in the number of loopholes for apps developed by firms with high versus low levels of state ownership (Model 5 in Table 1). Prior to the preliminary approval of the Cybersecurity Law, the differences between highly state-owned and purely private firms remain small and stable, supporting the assumption of parallel trends. Following the preliminary approval, however, apps developed by highly state-connected firms exhibit a significant and sustained reduction in the number of loopholes, suggesting that high state ownership incentivizes compliance with regulatory expectations even in the absence of formal enforcement. In contrast, firms with minor state ownership show a slight increase in the number of loopholes relative to purely private firms after the treatment, implying that partial state ownership may serve as a buffer and encourage noncompliance.

To further explore the impact, Model 6 in Table 1 uses the continuous measure of state ownership, *SOE%*. The estimated coefficient remains negative, but it is not statistically significant at the 0.1 level, suggesting a potentially nonlinear relationship between state ownership and compliance. Model 7 incorporates a squared term of *SOE%* and interacts it with the treatment indicator. The results demonstrate an inverted-U pattern: when state ownership rises from 0 to 20%, the number of security loopholes increases by about 1.7, indicating weaker compliance. The effect peaks around 40-45% ownership, where loopholes are roughly 2.3 greater than in private firms. Beyond this point the effect reverses: at 80% ownership the gap nearly disappears, and at full ownership SOEs exhibit about two fewer loopholes than private firms. The estimated turning point is 0.425, with a standard error of 0.449. This value lies well within the empirical range of SOE% (0 to 1), and 805 observations fall within ±0.05 of the turning point, providing sufficient support for inference (Haans, Pieters and He, 2016). This pattern supports the hypothesized shift



(a) Quartiles of State Ownership **(b)** Marginal Effects

Figure 4: Inverted-U Shaped Impact

Note: Panel (a) plots the treatment effects across quartiles of state ownership among nonprivate firms (*SOE%*>0), showing each group's average change in security loopholes relative to private firms after the preliminary approval of China's Cybersecurity Law. Compliance initially declines and then rises as state ownership increases. Panel (b) illustrates the marginal effects of state ownership on regulatory compliance, revealing an inverted-U relationship: minor state ties are associated with weaker compliance, and high levels of state ownership strengthen compliance. Estimates are based on Model (7) in Table 1.

from buffering to binding. Using the mean-centered *SOE%* yields similar results (Appendix Table D.4), suggesting that the findings are not driven by extreme observations.

To support the hypothesis of a nonlinear effect, we conduct two additional analyses. Figure 4a presents the results of a subgroup analysis in which apps are divided into quartiles based on the level of state ownership. Although the coefficients are statistically insignificant, likely the result of the reduced sample sizes, the direction of the treatment effects is consistent: the first three quartiles show positive effects, but the effect turns negative in the subgroup with the highest state ownership. Figure 4b provides a visual illustration of the nonlinear pattern, in which the marginal effect of state ownership on compliance initially rises with increasing ownership but declines beyond a midrange threshold. Sparse observations widened the confidence intervals at the extremes, but the overall inverted-U relationship remains clear and consistent with the regression results reported in Table 1 Model 7. Because lower loopholes indicate higher compliance, an inverted-U in loopholes corresponds to a U-shaped pattern in compliance.

Taken together, these findings are consistent with Hypotheses 1 and 2. Compared to purely private firms, minor state ownership may serve as a buffer that encourages noncompliance,

whereas major state ownership is associated with adherence to the Cybersecurity Law. Because firms' total state ownership may have changed overtime, we conduct two robustness analyses in the Appendix. First, Table D.5 shows results remaining robust after excluding all firms that received post-treatment financing or experienced an increase in state ownership. Second, Table D.6 reconstructs *SOE%* in 2014 based on historical investment records. Although the incompleteness and potential inaccuracy of these historical data introduce some missing values, the results remain consistent with our hypothesis.

6 Mechanisms

State ownership may shape corporate regulatory compliance through two distinct yet potentially coexisting channels. The first is political control where the government exerts direct influence on corporate decision making. When the Cybersecurity Law was first enacted, state shareholders had strong incentives to ensure follow-up implementation. The passage of the law signaled a clear political directive to address cybersecurity concerns, and active compliance served as a demonstration of political loyalty. If a state-owned firm failed to improve its cybersecurity practices and an incident occurred, the connected state agencies would be held accountable politically.

Second, firms incorporate state ownership into their strategic calculus when weighing regulatory risks against compliance costs. Regulatory risk, that is, the probability and severity of punishment for noncompliance, is particularly salient for firms subject to intense scrutiny. Compliance cost, which correlates with firm size, technological capability, and business model, is typically higher for smaller firms, those with weaker technological capacity, or those heavily dependent on advertising revenues.

6.1 Top-Down Political Control

To examine the mechanism of political control, we construct a measure of *equity distance*, defined as the number of ownership layers separating a firm from state entities. A distance of one indi-

cates that a state entity is a direct shareholder; a distance of two means the firm is a subsidiary of a state-invested company; a distance of three corresponds to a subsubsidiary, and so forth.

Since 2017 the Chinese government has promoted a shift in state asset supervision "from managing enterprises to managing capital," requiring local governments to delineate regulatory boundaries according to investment relations, clarify the responsibilities of governance entities, and streamline administrative oversight (SASAC, 2017) Although no official regulation specifies exactly how far down subsidiaries should be monitored, reforms undertaken between 2016 and 2022 aimed to cap the number of hierarchical layers in SOE structures at four or fewer (Xinhua News, 2022). We therefore use this benchmark as a fuzzy cutoff to classify SOEs as either within or beyond the scope of government control. Based on this classification, we distinguish between "Private," "State-connected," "SOE under Government Control," and "SOE beyond Government Control" and reestimate the baseline DID model accordingly.

Table 2 reports results using three alternative thresholds (three, four, and five layers). Findings show that the decline in security vulnerabilities following the enactment of the Cybersecurity Law was concentrated among SOEs under government control (i.e., within the threshold of equity distances), whereas SOEs beyond the control threshold exhibited no significant change. This pattern is robust regardless of whether the cutoff is set at three, four, or five layers. For example, firms within three layers of government ownership, including state-invested firms, their subsidiaries, and their sub subsidiaries, experienced an average reduction of three loopholes relative to private firms after the law's passage, nearly twice the baseline estimate (Model 5 in Table 1). Moreover, the magnitude of the effect diminishes as the government–firm distance increases. Models 4 and 5 further distinguish between ownership links to the central government and to local governments, showing consistent results; yet ties to local governments appear stronger.

Overall, these findings suggest that the impact of state ownership operates primarily through political control. A SOE responds swiftly to the Cybersecurity Law only when it falls under the effective reach of government oversight. By contrast, SOEs without direct control exhibit a far weaker response when political oversight becomes attenuated with distance.

Table 2: Mechanism: Top-down Political Control

Dependent Variable:	Loopholes				
Measure of Govt Control:	Dist. ≤ 3	Dist. ≤ 4	Dist. ≤ 5	Central ≤ 4	Local ≤ 4
Model:	(1)	(2)	(3)	(4)	(5)
Variables					
SOE under Govt Control × Law	-3.02**	-2.61***	-1.79**	-1.78**	-2.69**
	(1.38)	(0.868)	(0.846)	(0.767)	(1.07)
SOE beyond Govt Control × Law	-0.997	0.867	-0.699	0.707	-1.33
	(0.789)	(1.39)	(0.593)	(1.92)	(0.855)
State-Connected × Law	0.711	0.716	0.704	0.632	0.697
	(0.617)	(0.616)	(0.616)	(0.614)	(0.617)
Controls × Law	✓	✓	✓	✓	✓
Fixed-effects					
App ID	✓	✓	✓	✓	✓
Time × App Type	✓	✓	✓	✓	✓
Time × Province	✓	✓	✓	✓	✓
Time × Firm Industry	✓	✓	✓	✓	✓
Fit statistics					
Observations	88,523	88,523	88,523	87,027	88,789
Squared Correlation	0.96391	0.96392	0.96390	0.96353	0.96400

Notes: Signif. codes: *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$. Robust standard errors clustered at the *App ID* level are in parentheses. Models 1 to 3 use different distance thresholds to define *Govt Control*. *State-owned w/ Govt Control* refers to state-owned enterprises located within the threshold distance of government units, whereas *State-owned w/o Govt Control* refers to those located beyond the threshold. Models 4 and 5 estimate the impact on firms situated within four equity layers of central and local governments, respectively. *Law* is a binary variable equal to 1 if the observation occurs after the preliminary approval of China's Cybersecurity Law in 2016 June. *App Type* is a categorical variable with 8 levels. *Province* and *Sector* are categorical variables based on firm registration information. Control variables include the number of software and patents developed by a firm, professional certificates, and procurement contracts a firm received before 2016. Detailed results can be found in Table D.7.

6.2 Corporate Risk–Cost Tradeoff

This section provides evidence consistent with the proposed risk–cost mechanism. If firms weigh regulatory risk against compliance costs, differences in ownership should matter most under moderate levels of scrutiny or cost where discretion exists. When regulatory risks are either very high (high-risk loopholes) or very low (micro firms) or when compliance is too costly (apps with high Ad SDKs), ownership differences should diminish.

Models 1–3 estimate the effects of using loopholes categorized by different levels of security risk based on third-party classifications. High-risk loopholes attract intense regulatory scrutiny

Table 3: Mechanism: Corporate Risk–Cost Tradeoff

Dependent Variables:	High Risk	Med. Risk	Low Risk	Loopholes			
Sample:		Full Sample		Med/Large	Micro	Low Ad	High Ad
Model:	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Variables							
SOE% × Law	1.82	4.61**	4.65*	9.02	18.5	19.2*	-3.44
	(1.79)	(2.26)	(2.50)	(6.59)	(22.7)	(10.1)	(4.41)
SOE%^{2} × Law	-2.15	-5.38**	-5.47**	-11.6*	-18.1	-21.8**	2.96
	(1.81)	(2.32)	(2.56)	(6.75)	(22.5)	(10.0)	(4.55)
Controls × Law	✓	✓	✓	✓	✓	✓	✓
Fixed-effects							
App ID	✓	✓	✓	✓	✓	✓	✓
Time × App Type	✓	✓	✓	✓	✓	✓	✓
Time × Province	✓	✓	✓	✓	✓	✓	✓
Time × Firm Industry	✓	✓	✓	✓	✓	✓	✓
Fit statistics							
Observations	88,412	88,412	88,412	56,817	31,157	42,816	45,929
Squared Correlation	0.96188	0.96391	0.96407	0.95961	0.97735	0.96409	0.96411

Notes: Signif. codes: *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$. Robust standard errors clustered at the *App ID* level are in parentheses. The outcome variables are the numbers of loopholes with high, medium, and low risk in Models 1 to 3, and the total number of loopholes in Models 4 to 7. *Registered SOE* is a binary variable indicating whether a firm is registered as a state-owned enterprise; *SOE%* refers to the share of state capital in a firm. *Law* is a binary variable equal to 1 if the observation occurs after the preliminary approval of China's Cybersecurity Law in 2016 June. *App Type* is a categorical variable with 8 levels. *Province* and *Sector* are categorical variables based on firm registration information. *Micro* refers to firms with minimal employees and sales (e.g., fewer than 10 employees and less than 500,000 yuan in annual sales in the Internet and software industries), while *Med/Large* refers to medium-size and large firms. *Low Ad* refers to app types with a pretreatment number of software development kits for advertisement lower than the median, and *High Ad* refers to the others. Control variables include the number of software and patents developed by a firm, professional certificates, and procurement contracts a firm received before 2016. Detailed results can be found in Table D.8.

and pose serious operational risks, so firms tend to fix them regardless of ownership. In contrast, medium- and low-risk loopholes allow firms more discretion to allocate resources strategically. The results align with this expectation: the effects are significant only for medium- and low-risk loopholes, not for high-risk ones. This pattern suggests that ownership-based differences emerge primarily when regulatory risks are moderate, SOEs under political control tending to comply more readily and SCEs showing weaker incentives to do so.

Models 4 and 5 further account for firm size, regulatory scrutiny typically varying by firm scale. Microenterprises receive less attention from authorities than larger firms, a pattern also reflected in public reports showing that penalties mainly target major companies (Ministry of

Public Security, 2019). *Micro* firms in our classification are those with minimal employment and sales in their respective industries, based on Tianyancha data and National Bureau of Statistics of China (2018); *Med/Large* firms exceed those thresholds. For example, firms in the Internet and software sectors with fewer than 10 employees and less than RMB 500,000 in annual sales are coded as microenterprises. The results indicate that heterogeneous responses to the Cybersecurity Law exist only among medium and large firms. A likely explanation is that microenterprises face minimal regulatory scrutiny and thus have limited incentives to improve security. When regulatory risks are very low, state ownership also loses its influence because SOEs gain no additional incentive to comply and SCEs receive no extra protection.

Finally, apps' profitability models may moderate this relationship by affecting how firms absorb compliance costs. Fixing loopholes is costly, not only in technical resources but also in potential advertising losses, with developers often integrating more *Ad SDKs* at the expense of security. To capture this profitability incentive, we divide the sample by the median number of pretreatment *Ad SDKs* at the app-type level into *Low* and *High AD* groups in Models 6 and 7. The results show that the inverted U-shaped relationship between state ownership and compliance appears only among apps less dependent on advertising income. When compliance improvements threaten profitability, both state-owned and state-connected firms behave like private firms, indicating that cost pressures offset political incentives.

The heterogeneity analysis provides suggestive evidence for the risk–cost mechanisms through which state ownership shapes corporate compliance. State ownership influences firms' discretion only under moderate levels of regulatory risk and compliance cost. When regulatory risks are either very high (e.g., high-risk loopholes) or very low (e.g., microenterprises) or when compliance directly threatens profitability (e.g., apps with high Ad SDK usage), the marginal impact of state ownership diminishes as firms prioritize basic survival and operational constraints over political considerations. Figure C.1 in the Appendix illustrates these dynamics over time: the left panels (medium- and low-risk loopholes, medium and large firms, and apps with low Ad SDKs) show distinct post-treatment responses across ownership types, consistent with theoretical ex-

pectations, whereas the right panels display no discernible differences. Robustness checks using categorical variables (Appendix Table D.9) yield consistent results.

7 Conclusion

This study examines how various forms of state ownership influence corporate compliance with regulatory rules. Drawing on firm responses to China's Cybersecurity Law, we find a nonlinear relationship between state ownership and compliance outcomes. Firms with strong state ties, namely state-owned enterprises, are more likely to improve their software security as a result of direct political control. In contrast, firms with minor state ownership—the state-connected enterprises—exhibit lower levels of compliance, lagging behind in security performance. These findings suggest that state ties simultaneously produce *buffering* and *binding* effects and that the strength of these connections determines the direction and magnitude of corporate compliance.

The Chinese experience offers a valuable empirical lens on how state capitalism shapes governance outcomes (Busemeyer and Thelen, 2020; Pearson, Rithmire and Tsai, 2023). Similar patterns are likely to emerge in other regulatory domains such as environmental protection (Wang, 2015), as well as in non-mandatory policy arenas such as social welfare (e.g., poverty alleviation) and geopolitical strategies (e.g., the Belt and Road Initiative), where achieving governmental objectives hinges on firms' active responsiveness (Lin, 2025*a*; Naoi, Shi and Zhu, 2022).

This nonlinear pattern also helps reconcile the mixed buffering and binding effects of state ownership observed in the United States (Konisky and Teodoro, 2016), Russia (Frye, 2006; Panibratov and Michailova, 2019), Ukraine (Berg, Lin and Tsaplin, 2005), Austria (Ennser-Jedenastik, 2014), and Brazil (Musacchio and Lazzarini, 2014). Documented in a setting with comparatively strong monitoring and enforcement, our results further suggest that compliance heterogeneity may be even more pronounced where governments face stronger institutional constraints or where top-down enforcement is weaker.

References

Alami, Llias and Adam D. Dixon. 2024. *The Spectre of State Capitalism.* Oxford University Press.

Alok, Shashwat and Meghana Ayyagari. 2020. "Politics, State Ownership, and Corporate Investments." *The Review of Financial Studies* 33(7):3031–3087.

Babic, Milan. 2023. *The Rise of State Capital.* Agenda Publishing.

Bai, Chong-En, Chang-Tai Hsieh, Zheng Song and Xin Wang. 2021. "The Rise of State-Connected Private Owners in China.".

Baldwin, Robert, Martin Cave and Martin Lodge. 2011. *Understanding regulation: theory, strategy, and practice.* Oxford university press.

Berg, Sanford, Chen Lin and Valeriy Tsaplin. 2005. "Regulation of state-owned and privatized utilities: Ukraine electricity distribution company performance." *Journal of Regulatory Economics* 28(3):259–287.

Bertrand, Marianne, Francis Kramarz, Antoinette Schoar and David Thesmar. 2018. "The Cost of Political Connections." *Review of Finance* 22(3):849–876.

Bertrand, Marianne, Matilde Bombardini, Raymond Fisman and Francesco Trebbi. 2020. "Tax-exempt lobbying: Corporate philanthropy as a tool for political influence." *American Economic Review* 110(7):2065–2102.

Böwer, Uwe. 2017. "State-Owned Enterprises in Emerging Europe: The Good, the Bad, and the Ugly." *IMF Working Papers* 17(221):1.

Busemeyer, By Marius R and Kathleen Thelen. 2020. "Institutional sources of Business power." *World Politics* pp. 1–33.

Cazurra, Alvaro Cuervo. 2018. *State-Owned Multinationals.* Springer International Publishing.

Che, Jiahua and Yingyi Qian. 1998. "Insecure Property Rights and Government Ownership of Firms." *The Quarterly Journal of Economics* 113(2):467–496.

Chen, Frederick R and Jian Xu. 2023. "Partners with Benefits : When Multinational Corporations Succeed in Authoritarian Courts." *International Organization* .

China Banking and Insurance Regulatory Commission. 2019. "Administrative Penalty Disclosure Form Doc. No. 12 [2019].". Accessed May 2025.

Christensen, Sverre A. 2024. "Explaining State Ownership in Listed Companies in Norway." *Enterprise & Society* 25(3):907–932.

CNCERT. 2016. "2015 China Internet Security Report.". Accessed May 2025.

Colonnelli, Emanuele, Bo Li and Ernest Liu. 2024. "Investing with the Government: A Field Experiment in China." *Journal of Political Economy* 1(132).

Cyberspace Administration of China. 2016. "The 'Clean and Clear' Campaign: Targeting Persistent Online Misconduct with Sustained Deterrence in 2016.". Accessed May 2025.

Cyberspace Administration of China. 2018. "Cyberspace Authorities across China Conducted Lawful Interviews with 2,003 Websites Nationwide in 2017.". Accessed May 2025.

Ding, Iza and Jeffrey Javed. 2020. "The Autocrat's Moral-Legal Dilemma: Popular Morality and Legal Institutions in China." *Comparative Political Studies* .

D'Souza, Juliet and Robert Nash. 2017. "Private benefits of public control: Evidence of political and economic benefits of state ownership." *Journal of Corporate Finance* 46:232–247.

Earle, John S. and Scott Gehlbach. 2015. "The Productivity Consequences of Political Turnover: Firm-Level Evidence from Ukraine's Orange Revolution." *American Journal of Political Science* 59(3):708–723.

Ennser-Jedenastik, Laurenz. 2014. "Political Control and Managerial Survival in State-Owned Enterprises." *Governance* 27(1):135–161.

Fisman, Raymond. 2001. "Estimating the Value of Political Connections." *The American Economic Review* 91(4):1095–1102.

Fisman, Raymond and Yongxiang Wang. 2015. "The mortality cost of political connections." *Review of Economic Studies* 82(4):1346–1382.

Francis, David C. and Robert Kubinec. 2025. "Beyond political connections: a measurement model approach to estimating firm-level political influence in 41 countries." *Political Science Research and Methods* pp. 1–20.

Freyburg, Tina, Lisa Garbe and Véronique Wavre. 2022. "The political power of internet business: A comprehensive dataset of Telecommunications Ownership and Control (TOSCO)." *The Review of International Organizations 2022 18:3* 18(3):573–600.

Frye, Timothy. 2006. "Original Sin, Good Works, and Property Rights in Russia." *World Politics* 58:479–504.

General Office of the CPC Central Committee. 2003. "Opinions of the National Informatization Leading Group on Strengthening Information Security Work.". Accessed November 2025.

Gordon, Sanford C. and Catherine Hafer. 2005. "Flexing Muscle: Corporate Political Expenditures as Signals to the Bureaucracy." *American Political Science Review* 99(2):245–261.

Granovetter, Mark. 1983. "The Strength of Weak Ties: A Network Theory Revisited." *Sociological Theory* 1(1983):201.

Guo, Huimin, Zheyao Pan and Gary Tian. 2024. "Shareholders' political hierarchy and regulatory enforcement: Evidence from corporate risk management." *The British Accounting Review* 56(6):101372.

Haans, Richard F.J., Constant Pieters and Zi Lin He. 2016. "Thinking about U: Theorizing and testing U- and inverted U-shaped relationships in strategy research." *Strategic Management Journal* 37(7):1177–1195.

Haggard, Stephan, Sylvia Maxfield and Ben Ross Schneider. 2018. Theories of Business and Business-State Relations. In *Business and the State in Developing Countries*. Cornell University Press pp. 36–60.

Han, Chaohua, Xiaojun Li and Jean C. Oi. 2022. "Firms as Revenue Safety Nets: Political Connections and Returns to the Chinese State." *China Quarterly* 251(2):683–704.

Harding, Robin, Mounu Prem, Nelson Ruiz and David Vargas. 2023. "Buying a Blind Eye: Campaign Donations, Forbearance, and Deforestation in Colombia." *American Political Science Review* pp. 1–19.

He, Guojun and Wenwei Peng. 2022. "Guns and roses: Police complicity in organized prostitution." *Journal of Public Economics* 207:104599.

Heitz, Amanda, Youan Wang and Zigan Wang. 2023. "Corporate Political Connections and Favorable Environmental Regulation." *Management Science* 69(12):7838–7859.

Hillman, Amy J., Gerald D. Keim and Douglas Schuler. 2004. "Corporate political activity: A review and research agenda." *Journal of Management* 30(6):837–857.

Holland, Alisha C. 2015. "The Distributive Politics of Enforcement." *American Journal of Political Science* 59(2):357–371.

Hou, Wenxuan and Geoff Moore. 2010. "Player and Referee Roles Held Jointly: The Effect of State Ownership on China's Regulatory Enforcement Against Fraud." *Journal of Business Ethics* 95(SUPPL. 2):317–335.

Hou, Yue. 2019. *The Private Sector in Public Office.* Cambridge University Press.
Intel. 2025. "Intel and Trump Administration Reach Historic Agreement to Accelerate American Technology and Manufacturing Leadership.". Accessed September 2025.
James, Barclay E. and Paul M. Vaaler. 2018. "Minority Rules: Credible State Ownership and Investment Risk Around the World." *Organization Science* 29(4):653–677.
Kikeri, Sunita and Ruxandra Burdescu. 2020. State-Owned Enterprises. In *Enhancing Government Effectiveness and Transparency*, ed. Rajni Bajpai and C. Bernard Myers. Vol. 1 World Bank Group.
Konisky, David M and Manuel P Teodoro. 2016. "When Governments Regulate Governments." *American Journal of Political Science* 60(3):559–574.
Kung, James Kai-Sing and Chicheng Ma. 2018. "Friends with Benefits: How Political Connections Help to Sustain Private Enterprise Growth in China." *Economica* 85(337):41–74.
Lazzarini, Sergio G. and Aldo Musacchio. 2018. "State ownership reinvented? Explaining performance differences between state-owned and private firms." *Corporate Governance: An International Review* 26(4):255–272.
Leutert, Wendy. 2024. *China's State-Owned Enterprises: Leadership, Reform, and Internationalization.* Business and Public Policy Series Cambridge: Cambridge University Press.
Leutert, Wendy and Samantha A. Vortherms. 2021. "Personnel Power: Governing State-Owned Enterprises." *Business and Politics* pp. 1–19.
Li, Hongbin, Lingsheng Meng, Qian Wang and Li-An Zhou. 2008. "Political connections, financing and firm performance: Evidence from Chinese private firms." *Journal of Development Economics* 87(2):283–299.
Li, Zeren. 2022. "Connections as Liabilities : The Cost of the Politics-Business Revolving Door." *British Journal of Political Science* 4(53):1252–1272.
Lin, Shengqiao. 2025*a*. "Addressing Risk by Doing Good: Business Response to Government Policy Initiative." *Journal of Politics* .
Lin, Shengqiao. 2025*b*. "Partnership as Assurance: Regulatory Risk and State–Business Equity Ties in China.".
Lioukas, S., D. Bourantas and V. Papadakis. 1993. "Managerial Autonomy of State-Owned Enterprises: Determining Factors." *Organization Science* 4(4):645–666.
Liu, Xiumei, Fangbo Si, Chenxin Xie and Lu Xie. 2024. "Minority state ownership and firm performance: Evidence from the Chinese stock market crash in 2015." *Financial Management* 53(2):291–325.
Megginson, William L. 2017. "Privatization, State Capitalism, and State Ownership of Business in the 21st Century." *Foundations and Trends® in Finance* 11(1-2):1–153.
Milhaupt, Curtis J. and Mariana Pargendler. 2017. "Governance Challenges of Listed State-Owned Enterprises around the World: National Experiences and a Framework for Reform." *Cornell International Law Journal* 50:473–542.
Ministry of Industry and Information Technology. 2019. "Notice on the Quality of Telecommunication Services (No. 2 [2019]).". Accessed May 2025.
Ministry of Public Security. 2019. "Ministry of Public Security Released Typical Cases under the "Clean Net 2019" Special Campaign.". Accessed May 2025.
MP Materials. 2025. "MP Materials Announces Transformational Public-Private Partnership with the Department of Defense to Accelerate U.S. Rare Earth Magnet Independence.". Accessed November 2025.

Musacchio, Aldo and Sergio G Lazzarini. 2014. *Reinventing state capitalism: Leviathan in business, Brazil and beyond.* Havard University Press.

Naoi, Megumi, Weiyi Shi and Boliang Zhu. 2022. "'Yes-Man' Firms: Government Campaigns and Policy Positioning of Businesses in China." *International Studies Quarterly* 66(1-14).

National Bureau of Statistics of China. 2018. "Categorization Criteria for Large, Medium, Small, and Micro Enterprises (2017).". Accessed May 2025.

Nie, Huihua. 2017. *Collusion, Local Governments and Development in China.* Palgrave Macmillan.

OECD. 2024. *Ownership and Governance of State-Owned Enterprises 2024.* OECD Publishing.

Oi, Jean C. 1995. "The Role of the Local State in China's Transitional Economy." *The China Quarterly* 144(144):1132–1149.

Pan, Fenghua, Fangzhu Zhang and Fulong Wu. 2021. "State-led financialization in China: The Case of the Government-guided Investment Fund." *China Quarterly* 247(August 2020):749–772.

Panibratov, Andrei and Snejina Michailova. 2019. "The role of state ownership and home government political support in Russian multinationals' internationalization." *International Journal of Emerging Markets* 14(3):436–450.

Paper News. 2018. "From '0' to '56789': The Code of China's Private Economy over 40 Years.". Accessed May 2025.

Pargendler, Mariana, Aldo Musacchio and Sergio G. Lazzarinim. 2013. "In strange company: The puzzle of private investment in state-controlled firms." *Cornell International Law Journal* 46(3):569–610.

Parker, Christine and Vibeke Lehmann Nielsen. 2011. *Explaining compliance: Business responses to regulation.* Edward Elgar Publishing.

Pearson, Margaret M., Meg Rithmire and Kellee S. Tsai. 2023. *The State and Capitalism in China.* Cambridge University Press.

Pfeffer, Jeffrey and Gerald R Salancik. 1978. "The external control of organizations: A resource dependence approach.".

Reuters. 2015. "French govt completes controversial Renault stake hike.". Accessed October 2025.

Reuters. November 2025. "US, Vulcan Elements ink deal to boost rare earth magnet supplies.". Accessed November 2025.

Rexer, By Jonah M. 2025. "Corruption as a Local Advantage : Evidence from the Indigenization of Nigerian Oil." *American Economic Review* 115(3):1019–1057.

Rousseau, Sandra. 2007. "Timing of environmental inspections: Survival of the compliant." *Journal of Regulatory Economics* 32(1):17–36.

SASAC. 2017. "Plan for Advancing the Transformation of Functions with a Focus on Managing State Capital.". Accessed September 2025.

Shleifer, Andrei and Robert W. Vishny. 1997. "A survey of corporate governance." *Journal of Finance* 52(2):737–783.

Short, Jodi L. 2021. "The politics of regulatory enforcement and compliance: Theorizing and operationalizing political influences." *Regulation and Governance* 15(3):653–685.

Stigler, George J. 1971. "The Theory of Economic Regulation." *The Bell Journal of Economics and Management Science* 2(1):3–21.

Sun, Liang and Chun Liu. 2021. "Why do private firms introduce state-owned shareholders? Evidence from downward earnings management." *Journal of Finance and Economics (in Chinese)* 47(08):109–122.

Szakonyi, David. 2020. *Politics for Profit.* Cambridge University Press.

Tihanyi, Laszlo, Ruth V. Aguilera, Pursey Heugens, Marc van Essen, Steve Sauerwald, Patricio Duran and Roxana Turturea. 2019. "State Ownership and Political Connections." *Journal of Management* 45(6):2293–2321.

Truex, Rory. 2014. "The returns to office in a rubber stamp parliament." *American Political Science Review* 108(2):235–251.

Truex, Rory. 2020. "Authoritarian Gridlock? Understanding Delay in the Chinese Legislative System." *Comparative Political Studies* 53(9):1455–1492.

Valdez, Jimena. 2022. "The politics of Uber: Infrastructural power in the United States and Europe." *Regulation and Governance* .

Viscusi, W Kip, Joseph E Jr Harrington and David E M Sappington. 2018. *Economics of regulation and antitrust*. MIT press.

Wang, Yuhua. 2015. "Politically connected polluters under smog." *Business and Politics* 17(1):97–123.

Wei, Yifan, Yuen Yuen Ang and Nan Jia. 2023. "The Promise and Pitfalls of Government Guidance Funds in China." *The China Quarterly* 256:939–959.

Willner, Johan. 2001. "Ownership, efficiency, and political interference." *European Journal of Political Economy* 17(4):723–748.

Wilson, James Q. 2021. The Politics of Regulation. In *The Political Economy: Readings in the Politics and Economics of American Public Policy*. Routledge pp. 82–103.

Xinhua News. 2022. "Promoting Further Streamlining of Central SOEs: SASAC Launches a New Round of "Cutting and Reduction"."". Accessed September 2025.

Xinhua News. 2025. "Authoritative Bulletin: Latest Report on State-Owned Assets."". Accessed November 2025.

Yasuda, John K. 2021. "Regulatory State Building under Authoritarianism: Bureaucratic Competition, Global Embeddedness, and Regulatory Authority in China." *Comparative Politics* 54(1):123–147.

Zhang, Jianjun, Christopher Marquis and Kunyuan Qiao. 2016. "Do political connections buffer firms from or bind firms to the government? A study of corporate charitable donations of Chinese firms." *Organization Science* 27(5):1307–1324.

Zhang, Liguang, Liao Peng, Xinyu Liu, Zhe Zhang and Yunchen Wang. 2024. "The Governance Role of Minority State Ownership in Non-state-owned Enterprises: Evidence from Corporate Fraud in China." *British Journal of Management* 35(3):1489–1511.

Zu, Gary Ziwen and Shengqiao Lin. 2025. "Fiscal Origin of Selective Enforcement: Evidence from China's Administrative Penalties.".

Online Supplemental Information (Not for Publication)

A. China's Cybersecurity Law

Note: Original articles in Chinese are from official texts and the English translation is drawn from Digital China hosted by Stanford University.

> Article 22: Network products and services shall comply with the relevant national and mandatory requirements. Providers of network products and services must not install malicious programs; when discovering that their products and services have security flaws or vulnerabilities, they shall immediately adopt remedial measures, and follow provisions to promptly inform users and report to the competent departments. (第二十二条网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。)

> Article 25: Network operators shall formulate emergency response plans for cybersecurity incidents and promptly address system vulnerabilities, computer viruses, cyber attacks, network intrusions, and other such cybersecurity risks. When cybersecurity incidents occur, network operators should immediately initiate an emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with relevant provisions. (第二十五条网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。)

> Article 26: Those carrying out cybersecurity certification, testing, risk assessment, or other such activities—or publicly publishing cybersecurity information such as system vulnerabilities, computer viruses, network attacks, or network incursions—shall comply with relevant national provisions. (第二十六条开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。)

> Article 59: Where network operators do not perform cybersecurity protection duties provided for in Articles 21 and 25 of this Law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to harm to cybersecurity or other such consequences, a fine of between RMB 10,000 and 100,000 shall be levied; and the directly responsible management personnel shall be fined between RMB 5,000 and 50,000. (第五十九条网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。)

> Article 60: Where Article 22 Paragraphs 1 or 2 or Article 48 Paragraph 1 of this Law are violated by any of the following conduct, the relevant competent departments shall order corrections and give warnings; where corrections are refused or it causes

harm to cybersecurity or other consequences, a fine of between RMB 50,000 and 500,000 shall be levied; and the persons who are directly in charge shall be fined between RMB 10,000 and 100,000: (第六十条违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：)

(1) Installing malicious programs; (（一）设置恶意程序的；)

(2) Failure to immediately take remedial measures for security flaws or vulnerabilities that exist in products or services, or not informing users and reporting to the competent departments in accordance with regulations; (（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；)

(3) Unauthorized ending of the provision of security maintenance for their products or services. (（三）擅自终止为其产品、服务提供安全维护的。)

Article 62: Where Article 26 of this Law is violated in carrying out cybersecurity certifications, testing, or risk assessments, or publishing cybersecurity information such as system vulnerabilities, computer viruses, cyber attacks, or network incursions, corrections are to be ordered and a warning given; where corrections are refused or the circumstances are serious, a fine of between RMB 10,000 and 100,000 shall be imposed, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel shall be fined between RMB 5,000 and 50,000. (第六十二条违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。)

B. Data Availability Statement

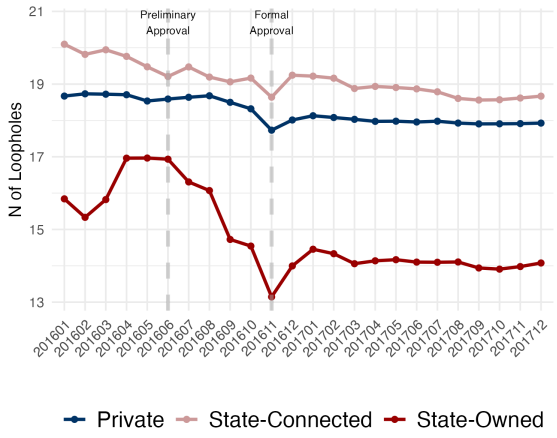
Our app security data were obtained from a major Chinese network security firm that is among the earliest and primary technical partners of China's national regulatory authorities. The firm is a leading provider of mobile and internet security services in China, offering end-to-end solutions covering app development, testing, deployment, and continuous monitoring. Its security analytics support a wide range of industries, including finance, telecommunications, government, and e-commerce, protecting over one million mobile applications and reaching approximately one billion mobile devices.

The firm conducts systematic and standardized vulnerability assessments for mobile applications in China, with near-complete coverage of Android apps available on domestic app stores. The detection workflow consists of three stages. First, the firm collects app installation packages and metadata from virtually all major Chinese app stores using an automated web-crawling and monitoring system that is continuously updated. Second, machine learning algorithms are applied to clean, deduplicate, and validate the collected data to ensure both accuracy and consistency across versions and over time. Third, the firm employs standardized security protocols to evaluate more than 120 types of vulnerabilities for each app, generating detailed diagnostic reports that include risk classification, severity level, and specific threat descriptions.

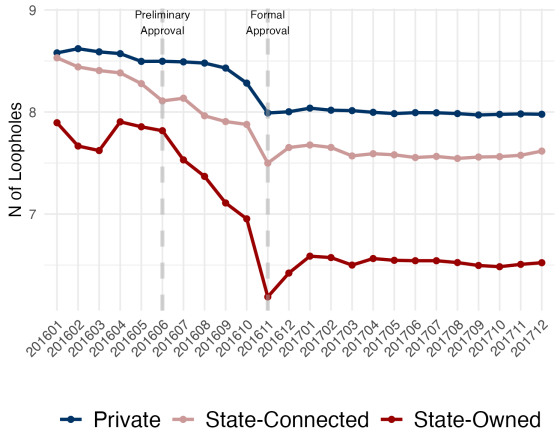
The firm's vulnerability assessment protocols are fully aligned with China's official cybersecurity standards, including *Information security technology—Guidelines for categorization and classification of cybersecurity vulnerability* (信息安全技术网络安全漏洞分类分级指南) and *Information security technology—Personal information security specification* (信息安全技术个人信息安全规范). These standards define the categories, severity levels, and reporting requirements for security vulnerabilities, ensuring comparability and reproducibility of results.

Due to the proprietary nature of the dataset and confidentiality agreements with the data provider, the raw data cannot be publicly released. The dataset contains sensitive commercial and cybersecurity information that, if disclosed, could pose risks to app developers and end users. To maintain transparency and replicability, we provide detailed summary statistics in Appendix Table D.2 and release all analysis code, allowing independent verification of our empirical results.

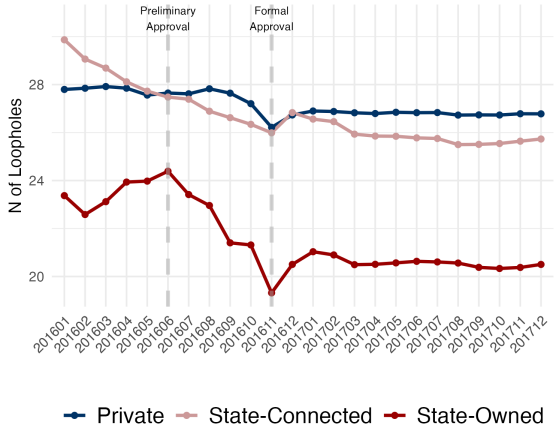
C. Figures



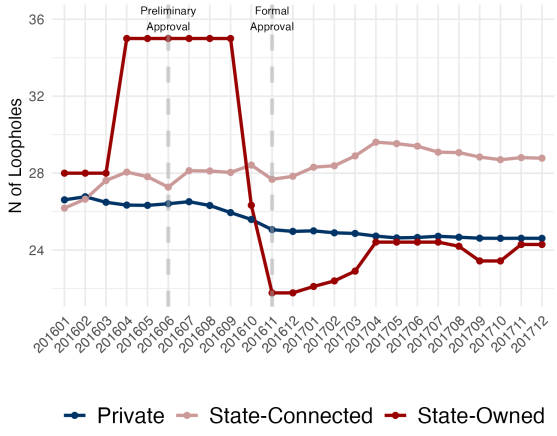
(a) Medium and Low Risk



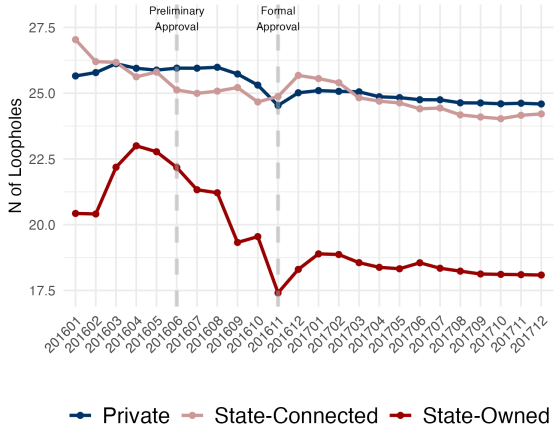
(b) High Risk



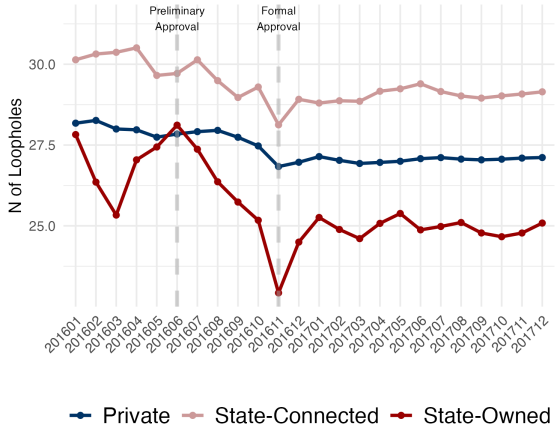
(c) Medium and Large Firms



(d) Micro Enterprises



(e) Low Ad SDKs



(f) High Ad SDKs

Figure C.1: Firm Responses: Risk Level, Firm Size, and Ad SDKs

D. Tables

Table D.1: Text Similarity Between Different Versions of China's Cybersecurity Law

Stage	Difflib Similarity	TF-IDF Cosine	Jaccard Similarity
1st Draft → 2nd Reading	0.770	0.605	0.876
2nd Reading → 3rd Reading	0.919	0.850	0.981
3rd Reading → Final Version	0.922	0.913	0.984

Note: *Difflib Similarity* measures textual overlap based on matching sequences of characters. *TF-IDF Cosine Similarity* evaluates similarity based on word importance and frequency. *Jaccard Similarity* calculates similarity based on shared unique words relative to all unique words.

Table D.2: Descriptive Statistics for Variables Used in the Regressions

		Summary Statistics			
Label	Description	Min	Max	Mean	SD
Loopholes	Number of detected security vulnerabilities per app version	0.00	57.00	25.95	14.07
SOE Share	Percentage of state ownership	0.00	1.00	0.06	0.21
SOE Share2	Squared term of state ownership share	0.00	1.00	0.05	0.19
Software	Number of software copyrights held by the firm	0.00	97.00	6.13	11.51
Patents	Number of patents held by the firm	0.00	100.00	1.13	5.63
Certificates	Number of qualification certificates obtained	0.00	99.00	1.18	5.43
Procurement	Number of government procurement projects won	0.00	27.00	0.17	1.24
Ad SDK (std)	Standardized number of advertising SDKs	-1.18	9.72	-0.01	0.99
High-risk Loopholes	Number of high-risk loopholes per app version	0.00	18.00	7.96	3.54
Medium-risk Loopholes	Number of medium-risk loopholes per app version	0.00	24.00	9.47	5.80
Low-risk Loopholes	Number of low-risk loopholes per app version	0.00	23.00	8.52	5.56
SOE_Group: Private	Purely private firms			81.73%	
SOE_Group: <50%	Firms with partial state ownership (<50%)			13.19%	
SOE_Group: >50%	Firms with majority state ownership (>50%)			5.08%	
Law: 0	Before law approval (pre-2016 June)			8.94%	
Law: 1	After law approval (post-2016 June)			91.06%	
Tiny: 0	Medium or large enterprise			64.80%	
Tiny: 1	Microenterprise			35.20%	
Weak: 0	Higher tech capability			93.64%	
Weak: 1	Low-level tech capability			6.36%	
HighCost: 0	Low advertising cost			48.19%	
HighCost: 1	High advertising cost			51.81%	
SOE_HighControl (Dist≤3)	SOE% ≥50% with strong government control			1.88%	
SOE_LowControl (Dist>3)	SOE% ≥50% without strong government control			2.92%	
SOE_HighControl (Dist≤4)	SOE% ≥50% with strong government control			3.38%	
SOE_LowControl (Dist>4)	SOE% ≥50% without strong government control			1.42%	
SOE_HighControl (Dist≤5)	SOE% ≥50% with strong government control			4.27%	
SOE_LowControl (Dist>5)	SOE% ≥50% without strong government control			0.53%	

Note: Dummy/factor variables are displayed as percentage shares (%).

Table D.3: State Ownership and Corporate Compliance

Dependent Variable:				Loopholes			
Control Group:	Registered Private Firms			Private/Connected	Private		
Model:	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Variables							
Registered SOE × Law	-0.572**	-2.34**	-2.38**				
	(0.270)	(1.04)	(1.04)				
State-Owned × Law				-1.82**	-1.66**		
				(0.803)	(0.764)		
State-Connected × Law					0.714		
					(0.617)		
SOE% × Law						-1.30	11.0*
						(0.913)	(6.28)
Software			0.504	0.820	0.886	1.36	2.23
			(792,663.0)	(793,900.4)	(788,984.8)	(796,014.4)	(791,751.7)
Law × Software			-0.005	-0.005	-0.005	-0.005	-0.005
			(0.007)	(0.007)	(0.007)	(0.007)	(0.007)
Law × PatentN			0.039*	0.041*	0.040*	0.041*	0.038*
			(0.021)	(0.021)	(0.021)	(0.021)	(0.021)
Law × Cerficiates			-0.021	-0.022	-0.023	-0.020	-0.025
			(0.045)	(0.044)	(0.044)	(0.045)	(0.044)
Law × Procurement			0.033	0.031	0.029	0.032	0.025
			(0.071)	(0.071)	(0.071)	(0.071)	(0.071)
State-Owned				1.73**			
				(0.770)			
State-Connected					-2.26**		
					(1.01)		
SOE%						1.25	-9.85*
						(0.879)	(5.96)
SOE%^{2}							11.7*
							(5.99)
Law × SOE%^{2}							-13.0**
							(6.36)
Fixed-effects							
Time	Yes						
App ID	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time × App Type		Yes	Yes	Yes	Yes	Yes	Yes
Time × Province		Yes	Yes	Yes	Yes	Yes	Yes
Time × Sector		Yes	Yes	Yes	Yes	Yes	Yes
Fit statistics							
Observations	88,789	88,789	88,789	88,789	88,789	88,789	88,789
Squared Correlation	0.96283	0.96395	0.96397	0.96398	0.96400	0.96397	0.96402

Clustered (App ID) standard-errors in parentheses
*Signif. Codes: ***: 0.01, **: 0.05, *: 0.1*

Table D.4: Centralized State Ownership and Corporate Compliance

Dependent Variable:	Loopholes		
Model:	(1)	(2)	(3)
Variables			
SOE_centered × Law	0.096	-1.30	9.47*
	(0.690)	(0.913)	(5.53)
SOE_centered	-0.093	1.25	-8.45
	(0.665)	(0.878)	(5.25)
Law × Software	-0.005	-0.005	-0.005
	(0.007)	(0.007)	(0.007)
Law × PatentN	0.039*	0.041*	0.038*
	(0.023)	(0.021)	(0.021)
Law × Certificates	-0.010	-0.020	-0.025
	(0.046)	(0.045)	(0.044)
Law × Procurement	0.045	0.032	0.025
	(0.070)	(0.071)	(0.071)
SOE_centered2			11.7*
			(5.99)
Law × SOE_centered2			-13.0**
			(6.36)
Fixed-effects			
App ID	Yes	Yes	Yes
Time	Yes		
Time × App Type		Yes	Yes
Time × Province		Yes	Yes
Time × Sector		Yes	Yes
Fit statistics			
Observations	88,665	88,595	88,595
Squared Correlation	0.96280	0.96390	0.96395

Clustered (App ID) standard-errors in parentheses
*Signif. Codes: ***: 0.01, **: 0.05, *: 0.1*

Table D.5: Robustness: Firms with Posttreatment Equity Changes Excluded

Dependent Variable:	Loopholes					
Sample	Equity Changes Excluded			Added State Ownership Excluded		
Control Group	Registered Non-SOE	Private		Registered Non-SOE	Private	
Model:	(1)	(2)	(3)	(4)	(5)	(6)
Variables						
Registered SOE × Law	-2.22**			-2.17**		
	(1.10)			(1.01)		
State-Connected × Law		0.865			0.438	
		(0.723)			(0.629)	
State-Owned × Law		-1.59*			-1.64**	
		(0.832)			(0.769)	
SOE% × Law			7.63			8.31*
			(5.31)			(5.02)
Law × Software	-0.009	-0.010	-0.009	-0.004	-0.004	-0.004
	(0.008)	(0.008)	(0.008)	(0.007)	(0.007)	(0.007)
Law × PatentN	0.016	0.019	0.019	0.033	0.035*	0.034*
	(0.018)	(0.018)	(0.018)	(0.020)	(0.020)	(0.020)
Law × Cerfticiates	0.032	0.025	0.025	-0.034	-0.035	-0.036
	(0.060)	(0.059)	(0.059)	(0.046)	(0.046)	(0.046)
Law × Procurement	0.003	0.002	0.001	0.044	0.043	0.040
	(0.077)	(0.076)	(0.076)	(0.073)	(0.073)	(0.073)
State-Connected		-2.29*			-1.97*	
		(1.17)			(1.03)	
SOE%			-6.05			-6.94
			(4.93)			(4.67)
SOE%^{2}			7.94			8.77*
			(4.99)			(4.75)
Law × SOE%^{2}			-9.54*			-10.2**
			(5.45)			(5.15)
Fixed-effects						
App ID	Yes	Yes	Yes	Yes	Yes	Yes
Time × App Type	Yes	Yes	Yes	Yes	Yes	Yes
Time × Province	Yes	Yes	Yes	Yes	Yes	Yes
Time × Sector	Yes	Yes	Yes	Yes	Yes	Yes
Fit statistics						
Observations	73,907	73,907	73,907	85,186	85,186	85,186
Squared Correlation	0.96674	0.96677	0.96677	0.96416	0.96418	0.96419

Clustered (App ID) standard-errors in parentheses
*Signif. Codes: ***: 0.01, **: 0.05, *: 0.1*

Table D.6: State Ownership (by 2014) and Corporate Compliance

Dependent Variable:	Loopholes				
		Full Sample		Est before 2014	Est 2010-2014
Model:	(1)	(2)	(3)	(4)	(5)
Variables					
State-Connected × Law	0.189	0.177	0.288	0.288	0.826
	(0.629)	(0.631)	(0.710)	(0.710)	(0.935)
State-Owned × Law	-1.73**	-1.80**	-1.84**	-1.84**	-1.08**
	(0.746)	(0.743)	(0.805)	(0.805)	(0.537)
State-Connected	-1.78*	-1.83**	-1.98**	-1.98**	-1.90**
	(0.909)	(0.905)	(0.999)	(0.999)	(0.945)
Law × Software	-0.003	-0.004	-0.005	-0.005	-0.004
	(0.007)	(0.007)	(0.008)	(0.008)	(0.014)
Law × PatentN		0.041*	0.040*	0.040*	0.032
		(0.021)	(0.021)	(0.021)	(0.027)
Law × Certificates		-0.019	-0.025	-0.025	-0.085
		(0.044)	(0.045)	(0.045)	(0.083)
Law × Procurement		0.032	0.042	0.042	-0.166
		(0.071)	(0.071)	(0.071)	(0.128)
Fixed-effects					
App ID	Yes	Yes	Yes	Yes	Yes
Time × App Type	Yes	Yes	Yes	Yes	Yes
Time × Province	Yes	Yes	Yes	Yes	Yes
Time × Sector	Yes	Yes	Yes	Yes	Yes
Fit statistics					
Observations	88,166	88,166	62,343	62,343	35,731
Squared Correlation	0.96408	0.96410	0.96031	0.96031	0.96637

Clustered (App ID) standard-errors in parentheses
*Signif. Codes: ***: 0.01, **: 0.05, *: 0.1*

Table D.7: Mechanism: Top-down Political Control

Dependent Variable:	Loopholes				
Measure of Govt Control:	Dist.≤3	Dist.≤4	Dist.≤5	Central≤4	Local≤4
Model:	(1)	(2)	(3)	(4)	(5)
Variables					
Law × SOE% ≥50% w/ Govt Control	-3.02**	-2.61***	-1.79**	-1.78**	-2.69**
	(1.38)	(0.868)	(0.846)	(0.767)	(1.07)
Law × SOE% ≥50% w/o Govt Control	-0.997	0.867	-0.699	0.707	-1.33
	(0.789)	(1.39)	(0.593)	(1.92)	(0.855)
SOE% <50%	-1.63	0.239	-1.40	0.133	-2.03*
	(1.04)	(1.55)	(0.913)	(2.05)	(1.12)
SOE% ≥50% w/ Govt Control	1.80	3.38**	0.963	2.41	1.04
	(1.36)	(1.55)	(0.953)	(1.99)	(1.12)
Software	-1.19	-1.15	0.868	0.621	-0.466
	(990,708.0)	(986,596.0)	(991,610.9)	(2,277,209.0)	(787,682.1)
Law × SOE% <50%	0.711	0.716	0.704	0.632	0.697
	(0.617)	(0.616)	(0.616)	(0.614)	(0.617)
Law × Software	-0.006	-0.007	-0.005	-0.006	-0.005
	(0.007)	(0.007)	(0.007)	(0.007)	(0.007)
Law × PatentN	0.038*	0.040*	0.040*	0.038*	0.040*
	(0.021)	(0.021)	(0.021)	(0.021)	(0.021)
Law × Certificates	-0.023	-0.022	-0.023	-0.025	-0.023
	(0.044)	(0.044)	(0.044)	(0.044)	(0.044)
Law × Procurement	0.031	0.030	0.029	0.027	0.028
	(0.071)	(0.071)	(0.071)	(0.070)	(0.071)
Procurement				0.141	
				(1,411,121.3)	
Fixed-effects					
App ID	Yes	Yes	Yes	Yes	Yes
Time × App Type	Yes	Yes	Yes	Yes	Yes
Time × Province	Yes	Yes	Yes	Yes	Yes
Time × Firm Industry	Yes	Yes	Yes	Yes	Yes
Fit statistics					
Observations	88,523	88,523	88,523	87,027	88,789
Squared Correlation	0.96391	0.96392	0.96390	0.96353	0.96400

Clustered (App ID) standard-errors in parentheses
*Signif. Codes: ***: 0.01, **: 0.05, *: 0.1*

Table D.8: Mechanism: Corporate Risk–Cost Tradeoff

Dependent Variables:	High Risk	Medium Risk	Low Risk		Loopholes		
Sample:		Full Sample		Med/Large	Micro	Low Ad	High Ad
Model:	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Variables							
SOE% × Law	1.82	4.61**	4.65*	9.02	18.5	19.2*	-3.44
	(1.79)	(2.26)	(2.50)	(6.59)	(22.7)	(10.1)	(4.41)
SOE%	-1.63	-4.13*	-4.16*	-7.84	-19.0	-16.7*	3.43
	(1.68)	(2.16)	(2.37)	(6.24)	(23.2)	(9.39)	(4.40)
SOE%^{2}	1.93	4.84**	4.92**	10.3	28.8	18.9**	-2.95
	(1.68)	(2.19)	(2.41)	(6.35)	(35.7)	(9.24)	(4.54)
Software	1.99	3.18	0.998	0.298		0.202	
	(251,193.6)	(345,647.0)	(343,670.8)	(422,720.0)		(1,050,260.3)	
Law × SOE%^{2}	-2.15	-5.38**	-5.47**	-11.6*	-18.1	-21.8**	2.96
	(1.81)	(2.32)	(2.56)	(6.75)	(22.5)	(10.0)	(4.55)
Law × Software	-0.0005	-0.001	-0.003	-0.014	0.004	-0.020	0.007
	(0.002)	(0.003)	(0.003)	(0.011)	(0.007)	(0.016)	(0.007)
Law × PatentN	0.011*	0.015*	0.015*	0.028	0.032	0.051	0.025
	(0.006)	(0.008)	(0.009)	(0.026)	(0.028)	(0.043)	(0.018)
Law × Cerfticiates	-0.002	-0.015	-0.007	0.021	0.006	0.042	-0.053
	(0.012)	(0.019)	(0.016)	(0.069)	(0.020)	(0.086)	(0.044)
Law × Procurement	-0.011	7.15×10^{-5}	0.030	-0.006	-0.064	-0.042	0.053
	(0.017)	(0.022)	(0.051)	(0.080)	(0.293)	(0.118)	(0.091)
Fixed-effects							
App ID	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time × App Type	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time × Province	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time × Firm Industry	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fit statistics							
Observations	88,412	88,412	88,412	56,817	31,157	42,816	45,929
Squared Correlation	0.96188	0.96391	0.96407	0.95961	0.97735	0.96409	0.96411

Clustered (App ID) standard-errors in parentheses
*Signif. Codes: ***: 0.01, **: 0.05, *: 0.1*

Table D.9: Robustness: Regulatory Scrunity and Corporate Profitability

Dependent Variables:	High Risk	Medium Risk	Low Risk		Loopholes		
Sample:		Full Sample		Med/Large	Micro	Low Ad	High Ad
Model:	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Variables							
State-Connected × Law	0.036	0.337	0.331	0.957	0.255	2.00	-0.309
	(0.191)	(0.235)	(0.246)	(0.825)	(0.999)	(1.32)	(0.402)
State-Owned × Law	-0.274	-0.629*	-0.732**	-2.09**	-0.172	-2.03*	-0.599
	(0.214)	(0.334)	(0.313)	(0.855)	(0.350)	(1.15)	(0.408)
State-Connected	-0.295	-0.920**	-1.01**	-6.11		-3.77**	-0.290
	(0.289)	(0.424)	(0.411)	(963,322.9)		(1.64)	(0.540)
Software	1.75	2.55	0.352			-2.98	
	(251,610.9)	(344,082.1)	(341,674.4)			(1,041,246.3)	
Law × Software	-0.0005	-0.001	-0.003	-0.015	0.004	-0.021	0.007
	(0.002)	(0.003)	(0.003)	(0.011)	(0.007)	(0.016)	(0.007)
Law × PatentN	0.011*	0.015*	0.016*	0.029	0.033	0.056	0.026
	(0.006)	(0.008)	(0.009)	(0.026)	(0.029)	(0.043)	(0.019)
Law × Cerficiates	-0.002	-0.015	-0.006	0.020	0.007	0.044	-0.053
	(0.012)	(0.019)	(0.016)	(0.070)	(0.019)	(0.086)	(0.044)
Law × Procurement	-0.011	0.002	0.032	-0.002	0.054	-0.045	0.046
	(0.017)	(0.022)	(0.051)	(0.080)	(0.251)	(0.118)	(0.088)
State-Owned				-3.21			
				(963,323.4)			
Fixed-effects							
App ID	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time × App Type	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time × Province	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time × Firm Industry	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fit statistics							
Observations	88,412	88,412	88,412	56,817	31,157	42,816	45,929
Squared Correlation	0.96187	0.96389	0.96406	0.95961	0.97731	0.96406	0.96411

Clustered (App ID) standard-errors in parentheses
*Signif. Codes: ***: 0.01, **: 0.05, *: 0.1*