

AIFE Working Paper
No. 02-2026

Data Privacy Gone Wrong: The Financial Fallout of App Misconduct

**Conggang Li, Jiatao Liu, Ian W. Marsh,
Haotian Shi**

March 2026

JEL classification: G14, G30, L15, L86.

Keywords: Data privacy, Mobile app, Misconduct, Cost of debt,
Event studies.

Andersen Institute for Finance & Economics working papers are written by Andersen Institute economists and associated contributors.

The views expressed within are those of the authors and not necessarily those of the Andersen Institute.

This publication is available on the Andersen Institute website (www.anderseninstitute.org).

©2026 Andersen Institute for Finance & Economics. All Rights Reserved. This material is confidential intellectual property of the Andersen Institute for Finance & Economics. By viewing this Andersen Institute Economic and Working Paper, you agree that you will not directly or indirectly copy, modify, record, publish, or redistribute this material and the information therein, in whole or in part. No warranty or representation, express or implied, is made by the Andersen Institute or any of its affiliates, nor does Andersen accept any liability with respect to the information and data set forth herein. Distribution hereof does not constitute legal, tax, accounting, investment or other professional advice. The information provided herein is not intended to provide a sufficient basis on which to make an investment decision. Recipients should consult their own advisors, including tax advisors, before making any investment decision.

Data Privacy Gone Wrong: The Financial Fallout of App Misconduct*

Conggang Li[†] Jiatao Liu[‡] Ian W. Marsh[§] Haotian Shi[¶]

March 6, 2026

Abstract

We investigate the consequences of data privacy misconduct by mobile apps under China's regulatory framework. Public disclosure of unlawful practices causes negative abnormal returns and increased borrowing costs, particularly severe for those with prior violations, operating in competitive sectors, under financial constraints, or with limited digital innovation. Market reactions are exacerbated by high media attention and competitive, data-driven industries. The rise in debt costs is driven by increased operational risk-taking and reputational damage. Significant negative spillover effects on industry peers indicate broader market implications. These findings underscore the financial impact of data privacy misconduct, emphasizing the importance of regulatory compliance.

JEL Classification: G14, G30, L15, L86

Keywords: Data privacy, Mobile app, Misconduct, Cost of debt, Event studies

*We thank Dan Luo, Jiaping Qiu, Bohui Zhang, Yapei Zhang, and Wei Zhang for helpful comments. We thank Qingyao Xiong for her research assistance. *Reject and Resubmit, Journal of Financial and Quantitative Analysis.*

[†]Shanghai Lixin University of Accounting and Finance; Email: conggangli@163.com

[‡]*Corresponding author:* International Business School Suzhou, Xi'an Jiaotong-Liverpool University; Email: Jiatao.Liu@xjtlu.edu.cn

[§]Bayes Business School, City, University of London; Email: i.marsh@city.ac.uk

[¶]Andersen Institute for Finance and Economics; Email: haotian.shi@andersen.com

1 Introduction

The rapid expansion of the digital economy has fundamentally transformed the landscape of personal data usage (Goldfarb and Que, 2023). Digitization has substantially reduced the costs associated with data collection, storage, transmission, and analysis (Goldfarb and Tucker, 2019) and firms now heavily rely on data to optimize operations, improve customer experience, and gain competitive advantages (Brynjolfsson and McElheran, 2016; Tambe et al., 2020; Goldfarb and Tucker, 2024). Yet, the specter of data breaches and privacy violations looms large, as exemplified by incidents such as the Facebook-Cambridge Analytica scandal, the Equifax breach, and the Google+ data exposure. These cases underscore the serious risks associated with lapses in data privacy and have spurred regulatory responses across the globe. To address these concerns, many countries have proposed comprehensive data protection regulations including the European Union’s General Data Protection Regulation (GDPR) and the California Consumer Privacy Act.

China was the world’s second-largest data producer in 2022, contributing over 10% of global data production, and its digital economy exceeds RMB5 trillion, with an online population surpassing one billion and research and development investment by the top 100 internet enterprises amounting to RMB338.4 billion.¹ Despite these figures, China’s digital governance lags, ranking only 41st in the Global Digital Economy Development Index Report (2023). This disparity between its rapid digital growth and relatively low governance standards creates vulnerabilities and opportunities for misconduct, particularly in data privacy and protection.

China’s Ministry of Industry and Information Technology (MIIT) implemented a special rectification initiative in December 2019 that publicly discloses apps engaged in unlawful data prac-

¹Please find detailed information from the 2022 Digital China Development Report.

tices and issues warnings to offending firms on the government’s website. We leverage this regulatory enforcement setting to examine how capital markets respond when regulators publicly challenge firms’ data-usage practices that exceed evolving legal or ethical boundaries. Since 2019, MIIT has released periodic disclosures identifying mobile applications that violate data-privacy rules—ranging from unauthorized data collection to opaque third-party sharing. Unlike traditional enforcement tools such as fines or litigation, this approach relies primarily on regulatory “naming and shaming” as a reputational sanction designed to discipline firms and deter future violations.

We first identify which firms are more likely to be found to have violated regulations. We link MIIT citations to pre-event corporate characteristics. Data misconduct, in our framework, is a strategic choice that balances the incremental payoff from extracting user information against expected regulatory and reputational costs, moderated by governance discipline. Our cross-sectional evidence shows that larger, intangible-heavy firms are disproportionately cited for misconduct, consistent with scale economies in data exploitation: when the marginal value of an extra record is high, managers have stronger incentives to test regulatory limits. Low-levered firms are also more likely to offend—because a lighter debt load gives them greater capacity to absorb penalties or fund legal defence—whereas asset tangibility, by signalling a business model less reliant on data, attenuates misconduct risk. Prior behaviour matters as well: companies with a recent record of accounting or regulatory infractions are significantly more prone to privacy breaches, implying persistent governance weaknesses and a managerial tolerance for grey-zone strategies. Sectoral exposure amplifies these patterns: membership in NBSC-classified “data-driven” industries—where personal information is a core input—raises violation likelihood, underscoring that the marginal benefit of stretching privacy rules is highest where user data underpins revenue generation. By contrast, stronger internal oversight (larger boards, higher ESG/CSR scores) and tougher external

discipline (greater product-market rivalry) both curb the probability of citation, presumably by heightening scrutiny and increasing the reputational price of non-compliance. Overall, misuses of personal data cluster in firms that combine high incentives and ample capacity to push the frontier with weak internal or market checks on opportunistic behaviour.

We next examine how equity markets respond to the public disclosure of data misconduct and find that the financial consequences are both statistically significant and economically substantial. Firms identified for violations experience market-adjusted cumulative abnormal returns (CARs) of -1.2% to -2.5% within the event window surrounding the disclosure. Given the average market capitalization of RMB 163 billion in our sample, this translates into an average shareholder value loss of nearly RMB 2 billion per incident. These losses reflect not only anticipated compliance and remediation costs, but also broader reputational damage and increased perceived regulatory risk.

Importantly, the magnitude of the market reaction is not uniform. Mainly, the equity draw-down is markedly steeper for firms with large institutional block-holders. Economically, this pattern can be interpreted through two complementary lenses.

First, large blocks are typically held by sophisticated investors with low information-processing frictions. When the MIIT names a portfolio firm, these block-holders update their priors quickly and, if necessary, unwind positions just as quickly. Because their trades are large relative to daily turnover, the immediate selling pressure magnifies the initial price drop.

Second, sizeable block ownership often goes hand-in-hand with high pre-event valuations: analysts view the presence of monitoring institutions as a signal of superior growth prospects and governance quality. A public privacy breach undermines that narrative. Investors now question whether past performance—and the valuation premium it supported—rested on borderline data practices that will be harder to sustain under tighter regulatory scrutiny. The share-price revision

therefore reflects more than the direct cost of remediation; it embeds a downward reassessment of the firm's long-term competitive advantage once aggressive data harvesting is no longer feasible.

We also find that firms whose apps operate on open-source platforms (i.e., systems other than iOS) experience significantly larger negative abnormal returns following misconduct announcements. Given the relatively weaker controls and transparency challenges inherent in open-source operating systems, these platforms are often perceived as more susceptible to data privacy breaches. Consequently, investors may interpret misconduct on such platforms as particularly damaging to a firm's public legitimacy and user trust, critical dimensions of competitive advantage in platform-based markets. Similarly, firms in data-intensive and competitive sectors experience sharper valuation losses, suggesting that when user data is central to business strategy and market discipline is strong, investors respond more harshly to breaches. In short, the enforcement of data governance boundaries imposes disproportionate valuation penalties on firms that are both data-driven and reputationally exposed, especially when their market value is supported by intangibles that rely on continued public and regulatory trust.

We then investigate the contagion effects of data misconduct. Unlike conventional forms of corporate misconduct, such as financial fraud or accounting restatements, data misuse generates reputational and regulatory externalities that more readily spill over across firm boundaries. In cases of financial wrongdoing, the market often treats the event as idiosyncratic, mainly because such misconduct typically stems from firm-specific governance failures or managerial incentives, rather than systemic industry-wide practices. In contrast, data misconduct operates under shared technological and strategic incentives, as personal data has increasingly become a common input in the production processes of digital firms. When one firm is found to have violated data privacy rules, it signals to investors and regulators that similar firms, especially those operating in the same

sector, may be engaging in comparable practices. This leads stakeholders to revise upward the perceived likelihood of broader regulatory scrutiny or future enforcement actions.

Such reputational contagion is particularly pronounced in digital markets, where data governance standards are still evolving and regulatory enforcement remains discretionary and uneven. Consistent with this mechanism, we find that data misconduct announcements trigger negative market-adjusted abnormal returns for industry peers, ranging from -0.3% to -0.96% , as markets anticipate either direct regulatory exposure or rising compliance costs across the sector. These findings underscore the idea that data is not only a strategic asset, but also a source of shared regulatory risk. When one firm is publicly sanctioned for pushing the boundaries of acceptable data use, it effectively resets the perceived limits for the entire industry, prompting a repricing of risk among similar firms.

While equity market reactions reveal how shareholders price the reputational and regulatory risks of data misconduct, they only capture part of the story. Debt holders—unlike shareholders—are primarily concerned with downside risk and the firm's ability to generate stable cash flows. Examining whether creditors respond to data violations therefore offers a complementary perspective on the economic consequences of misconduct. In particular, it allows us to assess whether reputational damage and regulatory exposure translate into heightened perceived default risk. Using a difference-in-differences approach with propensity score matching, we find that firms found guilty of data violations face a significant increase in their cost of debt—approximately 42 basis points on average. This result holds under dynamic panel specifications and is economically meaningful. The increase in borrowing costs is most pronounced among firms with a history of prior violations, those in highly competitive industries, financially constrained firms, and those lacking digital innovation capabilities. These patterns suggest that lenders not only punish mis-

conduct per se, but also incorporate forward-looking concerns about firms' governance quality, regulatory vulnerability, and strategic adaptability. Together with our equity market results, these findings underscore that data governance failures impose a dual financial penalty—lower valuations from investors and tighter credit terms from lenders—amplifying the cost of overstepping the boundaries of legitimate data usage.

Beyond capital market reactions, we find that firms implicated in data misconduct suffer real economic consequences that reflect a deterioration in both operating performance and risk profile. Specifically, following a public notice, sales growth slows sharply and both ROA and ROE contract, outcomes that trace back to reputational damage: customers defect, partners reconsider collaborations, and management must overhaul data-driven product lines to restore trust. At the same time, affected firms exhibit heightened operational volatility, with significantly increased variability in financial performance. This pattern is indicative of greater strategic uncertainty and managerial risk-taking, possibly as firms attempt to recover from reputational damage or reconfigure their digital practices under regulatory pressure. These post-disclosure shifts in firm fundamentals provide a direct channel through which data misconduct increases the cost of capital: investors anticipate weaker cash flow stability, greater downside risk, and elevated compliance costs. Taken together, the evidence underscores that improper data governance invites regulatory scrutiny and undermines the firm's long-run economic resilience.

Related Literature

We contribute to several strands of literature. First, this paper joins the discussion on the implications of data protection regulations and policies. Recent work shows that the enactment of GDPR has led to increased market concentration by benefiting larger firms, significant higher

compliance costs on AI startups, and reduced venture capital funding for startups, consequently stifling innovation and competition (Bessen et al., 2020; Peukert et al., 2022; Aridor et al., 2023). Exploring demand-side effects, Goldberg et al. (2019) and Schmitt et al. (2022) find evidence of the negative impact of GDPR on consumers' website visits. Also, Demirer et al. (2024) document the impact of GDPR on firms' production costs, since data and computing are important inputs in production.

China's special rectification initiative actively scrutinizes firms' conduct with regard to data management and periodically discloses infringing firms. Our study benefits from this periodic political implementation to comprehensively examine the impact of strengthened data regulations on firms' performance. This allows us to identify the causal effect of national-level data regulation on infringing firms compared to compliant firms in data management.

Second, our study examines internally driven data misuse—privacy violations arising from firms' own mobile-app practices—rather than external cyberattacks or inadvertent data breaches. This distinction is important because internal misconduct reflects deliberate managerial choices that fall within the firm's control, whereas external breaches typically stem from outside attacks or security failures.

A parallel literature studies the financial consequences of external data breaches. Kamiya et al. (2021) find that successful cyberattacks impose significant reputational costs, as reflected in negative market reactions and subsequent declines in sales. Ashraf (2022) shows that peer firms respond to breaches by strengthening internal controls, suggesting industry-wide learning effects. On the regulatory side, Ashraf and Sunder (2023) document that mandatory data-breach disclosure laws prompt firms to become more proactive in cybersecurity risk management. Relatedly, Huang and Wang (2021) show that banks tighten loan terms—raising spreads and worsening pricing—for

firms that experience external breaches.

While our empirical design shares the event-driven identification used in this literature, the mechanism we study is fundamentally different. By focusing on privacy violations arising from the firm's own unlawful data-collection and app-management practices, we provide new evidence on how internally initiated data misuse leads to material financial consequences, including shareholder wealth losses, heightened operational risk, and higher borrowing costs.

Third, our paper broadens the scope of the misconduct literature. Recent studies have focused on causes and consequences of financial misconduct, including the reduction of financial statement restatements through proximity to SEC offices ([Kedia and Rajgopal, 2011](#)), the impact of corruption culture on the likelihood of multiple misconducts ([Liu, 2016](#)), increased corporate misconduct due to local newspaper closures ([Heese et al., 2022](#)), and the detection of hidden corporate frauds ([Dyck et al., 2024](#)).² Reflecting the new digital era, studies have considered the effects of misconduct by agents external to the firm, such as data breaches and cyberattacks ([Ashraf, 2022](#); [Huang and Wang, 2021](#); [Kamiya et al., 2021](#)). Our paper adds to the field by examining data misconduct by agents within the firm, highlighting the dark side of technological advancements when used illegally by firms.

Furthermore, previous studies have examined various factors influencing the cost of debt, such as the role of board characteristics and audit committees in ensuring the reliability of financial reports ([Anderson et al., 2004](#)), the impact of earnings information on debt costs ([Jiang, 2008](#); [Mansi et al., 2011](#)), the effect of political rights on reducing bond spreads ([Qi et al., 2010](#)), comprehensive determinants of debt costs ([Van Binsbergen et al., 2010](#)), and the positive relationship between product market competition and the cost of bank debt ([Valta, 2012](#)). Our study adds to

²For comprehensive reviews, see [Amiram et al. \(2018\)](#) and [Velte \(2023\)](#).

this literature by examining whether the illegal use of consumer data gathered by mobile apps leads to higher debt financing costs. To the best of our knowledge, this paper is among the first to investigate the economic consequences of debt financing from the perspective of app misconduct in data collection.

Finally, our paper aligns with ongoing work on data privacy. [Chen et al. \(2021\)](#) finds a puzzling data privacy paradox using survey data from Alipay, suggesting that consumers' data privacy concerns are a byproduct of using digital platforms rather than an innate concern. Similarly, [Sun et al. \(2024\)](#) conducts a field experiment on the Alibaba platform to measure the impact of data regulation policies on e-commerce effectiveness, showing that such regulations can disproportionately affect smaller businesses and less wealthy consumers. Our study, while investigating data regulation in a Chinese context, focuses on a stringent governmental act on data privacy regulation that applies to all firms and individuals, rather than targeting a specific group of users on a digital platform. [Bian et al. \(2021\)](#) is highly related to our use of direct policy on mobile apps. They use Apple's privacy label policy to highlight both the supply of and demand for data privacy. However, the infringing firms in our paper are intentionally managing data illegally, and we explore the impact of regulatory disclosures of these guilty firms. Consequently, our study directly examines the effect of visible government intervention on data and personal information protection, rather than firms' passive compliance with policy changes within a single large digital ecosystem.

2 Institutional Background

In the global digital economy, most jurisdictions have deemed it necessary to have robust data privacy regulations that not only protect the security of personal information but also align with inter-

national standards to facilitate data flows. In Appendix B, we provide the framework for governing data privacy across major jurisdictions. In this section, we detail China’s evolving framework for the regulation of data privacy with a particular focus on the rules applied to mobile applications.

The China Academy of Information and Communications Technology (CAITA) has emphasized the importance of improving digital governance for the development of China’s digitization. According to CAITA’s White Paper on Global Digital Governance (2022), digital platforms are at the core of the digital economy value chain and play a significant role in data aggregation and digital governance. With China ranking highly in terms of digital infrastructure and marketplace yet lagging in terms of governance and regulation, the authorities have implemented a series of laws to regulate data security.

The Cybersecurity Law (CSL), effective since 2017, is the foundational legislation for Chinese cyberspace security regulation that highlights essential regulatory rules of network operation and information security. The Data Security Law (DSL), established in 2021, focuses on balancing security with development and creates a hierarchical data protection system. Concurrently, the Personal Information Protection Law (PIPL) sets rigorous norms for processing “personal information”, enhancing individuals’ rights to be informed and to be able to make decisions, and requires measures such as data classification management, encryption, and de-identification to reduce data security risks.

The PIPL, in particular, closely aligns Chinese regulation with the European Union’s GDPR. However, there are differences between the two. Perhaps the most important for our application is that the PIPL has a much wider scope of what is considered “sensitive” data and thus subject to more stringent protection than the GDPR’s definition of “special category” data.³ Like GDPR,

³Comparisons of GDPR and PIPL can be found at <https://www.china-briefing.com/news/>

PIPL includes stringent penalties. Fines can be as high as RMB50 million (around \$7 million) or 5% of a company's turnover from the previous financial year, and businesses can be required to suspend operations until compliance is demonstrated.

Within this broad regulatory environment more focused interventions are occurring, especially in the realm of mobile applications, where rapid technological advancements and widespread usage pose unique risks. In particular, China is restricting how companies can use algorithms to boost sales. The Cyberspace Administration of China announced a three-year plan to regulate predictive algorithms used by online content providers in September 2021. The proposed regulations, enabled by the PIPL, prohibit algorithms considered to encourage online addiction, and require that users be told about algorithmic recommendation services and have the option to switch them off.

China has also addressed specific challenges related to mobile application operations that compromise data privacy and user rights. Under the overarching guidelines of the DSL and national data security management protocols, the Ministry of Industry and Information Technology (MIIT) is tasked with overseeing data security in the industrial and telecommunications sectors. This includes formulating data security management policies tailored to the nuances of these fields.⁴

The rapid proliferation of apps has led to significant issues, such as unauthorized collection of personal information, excessive permission requests, frequent harassment, and infringement of user rights—emerging as key concerns in personal data security. In response, China has enhanced the protection of personal information handled by apps and standardize their data processing activities. In November 2019, the MIIT issued the “Notice on Conducting Special Rectification Campaign Against the Infringement of User Rights by apps.” This directive mandates specific

[pipl-vs-gdpr-key-differences-and-implications-for-compliance-in-china/](https://pro.bloomberglaw.com/insights/privacy/consumer-data-privacy-eus-gdpr-vs-chinas-pipl/) and <https://pro.bloomberglaw.com/insights/privacy/consumer-data-privacy-eus-gdpr-vs-chinas-pipl/>

⁴Please also see the detailed timeline of Chinese data privacy regulations in Figure 2 under Appendix B.

corrective actions against apps engaging in unlawful data practices. Measures include ordering rectifications, issuing public notices, removing non-compliant apps from platforms, suspending their service access, and including offenders on a blacklist for telecommunications operations or a list of untrustworthy entities. Strict penalties are enforced for app operators who persistently violate regulations or refuse to comply. Further elaborating on the enforcement of regulations, MIIT has identified and categorized ten main types of violations by apps:

- APP forcefully, frequently, and excessively requests permissions.
- Collecting and using personal information beyond the necessary scope.
- Illegally collecting and using personal information.
- Illegally utilizing personal information for automated decision-making.
- Deceiving, misleading, and coercing users.
- Deceiving and misleading users into using products or services.
- Deceiving and misleading users into downloading the APP.
- Inadequate disclosure of APP information on application distribution platforms.
- Forcing users to use targeted push functions.
- Pop-up message harassment of users.

As of December 2023, the MIIT has issued 35 batches of “Notices on Conducting Special Rectification against the Infringement of User Rights,” (hereafter, “Notices”) cumulatively address-

ing nearly 3,000 apps.⁵ The top four misconduct categories are: illegally collecting personal information (32%); apps forcefully, frequently, and excessively requesting permissions (12.5%); collecting and using personal information beyond the necessary scope (10.8%); and illegally utilizing personal information (10.78%).

It is important to note that the authorities' approach to app misconduct has so-far been limited to "naming and shaming." Infringement notices are posted on public websites but neither fines nor cessation of business operations have been invoked. While firms may well have incurred some behind-the-scenes costs in interacting with investigators, this lack of large out-of-pocket expenses such as the payment of fines means that any penalties misbehaving firms face will be due to reputation costs, as explored below.

3 Data

3.1 Misconduct incidents

The Notices issued by MIIT form the basis of our analysis. We collect data on each misconduct announcement from the official MIIT website and manually match each app misconduct notice to public firms listed in the China Stock Market and Accounting Research (CSMAR) database, from the first misconduct event in December 2019 to the end of 2023. The matching procedure yields a final sample of 131 misconduct events across 95 unique firms, with 23 firms guilty of multiple app misconducts during our sample.

Table 1 presents the distribution of the 131 corporate data misconduct events by industry and year. The data reveals a hump-shaped distribution of events over time, with a peak of 64

⁵Please see detailed examples of violated firms in Appendix C.

incidents in 2021. Nearly 50% of the misconduct events occur in information technology and related industries. However, significant numbers of events are also found in the manufacturing, wholesale, and retail trades, as well as in the culture, sports, and entertainment industries. Although ten such events occur in the financial sector, this sector does not drive our analysis, unlike several other studies on corporate misconduct.⁶

3.2 Comparison of guilty and non-guilty firms

To benchmark cited firms against their unaffected peers, we merge the MIIT event list with annual CSMAR accounting data and retain only observations with complete financial information for the two fiscal years bracketing each event. Multiple violations by the same company within a single fiscal year are collapsed into one firm-year. The final panel comprises 106 misconduct firmyears (84 firms) and 19,976 non-misconduct firm-years (4,799 firms). Continuous variables are winsorised at the 1st and 99th percentiles to curb the influence of extreme outliers.

Table 2 summarises the mean and median differences between cited and non-cited firms. Offending firms are demonstrably larger, hold a greater share of intangible assets, and—somewhat paradoxically—display lower day-to-day share-price volatility. Their governance profile is mixed. They operate with smaller boards yet a higher proportion of independent directors, and they are far less likely to issue stand-alone CSR reports. Taken together, the pattern implies that a lean board structure, even one populated by independents, offers limited deterrence when broader stakeholder visibility is weak; in firms already scarred by past misconduct, that gap appears to open the door to more aggressive data practices.

⁶For example, studies by [Karpoff et al. \(2017\)](#) and [Amiram et al. \(2018\)](#) conduct comprehensive reviews on how databases are used in misconduct research.

Environmentally, violators tend to operate in industries with higher Herfindahl indices, consistent with weaker product-market discipline. Finally, companies designated ex ante as “data-driven” under the 2021 National Bureau of Statistics digital-economy taxonomy, are disproportionately represented among offenders, underscoring the heightened boundary risk faced by firms whose business models rely most heavily on personal data.

4 Empirical Analysis

4.1 Likelihood of misconduct

To directly examine the likelihood of firms being guilty of misconduct, we estimate probit regressions where the dependent variable is an indicator that takes the value one if a firm is guilty of misconduct in a given year, and zero otherwise. We include the characteristics discussed in Table 2 as explanatory variables. Each variable is measured one year before the year of the misconduct event. Results are reported in Table 3.

Column (1) of Table 3 indicates that three balance-sheet fundamentals—firm size, asset composition, and leverage—are systematically related to the probability of a privacy citation. The marginal effect of total asset is positive: large firms are more likely to be flagged. When penalties are largely fixed, the Becker–Stigler optimal-crime calculus implies weaker deterrence for large offenders because the expected sanction per unit of revenue is smaller; regulators may also concentrate enforcement on high-visibility targets to maximise deterrence per case.⁷ By contrast, the coefficient on asset tangibility is negative. Tangible-asset-intensive businesses rely less on propri-

⁷Becker (1968) shows that if the monetary component of punishment is not perfectly proportional to offence scale, larger agents face a lower marginal expected penalty.

etary data and therefore obtain a smaller incremental payoff from boundary-pushing. Firms whose value rests on intangibles—data, code, brand—stand to gain more from aggressive harvesting and so accept greater boundary risk.

Leverage enters with a negative sign, indicating that highly indebted firms are less likely to violate privacy rules. Debt can discipline managers through two linked channels. First, fixed contractual payments limit the free cash flow available for discretionary (and potentially opportunistic) projects, thereby reducing the expected benefit of violating uncertain legal boundaries. Second, creditors have strong incentives to monitor compliance when violations threaten cash-flow volatility that would endanger debt service.⁸

Additionally, the board size coefficient in Column (1) reinforces an agency-cost interpretation. A larger board reduces the likelihood of a citation. Expanded director representation broadens monitoring capacity and may create explicit oversight of data-security practices, raising the expected internal cost of opportunistic behaviour.

Column (2) tests an indicator for prior financial misconduct in the preceding three years. Its coefficient is strongly positive, implying that firms with a history of accounting or regulatory infractions are significantly more prone to subsequent privacy violations. This pattern fits a persistent-type story: past offences signal either a managerial disposition that discounts future penalties or control structures that remain deficient.

Column (3) introduces outward-facing responsibility metrics. Firms that publish a CSR report or fall into the top ESG-rating tiers are substantially less likely to be cited. Under the reputation-capital framework, investing in stakeholder goodwill elevates the private cost of being publicly

⁸Jensen's (1986) free-cash-flow theory formalises the disciplining role of leverage; Diamond (1989) and Hart and Moore (1995) analyse creditor monitoring when default risk is state-contingent.

named, thereby sharpening managerial incentives to stay clear of grey-zone data practices.⁹

Column (4) drops industry dummies and substitutes the Herfindahl index. A more concentrated product market is associated with higher misconduct propensity. Intuitively, when rivalry is weak, the competitive penalty of getting caught—customer switching and share loss—is muted, lowering the all-in expected cost of violation.

Finally, Column (5) adds a dummy for “data-driven” sectors. Membership in these industries—where personal data are a core production input—raises the odds of misconduct, as the marginal benefit from boundary-pushing is greatest precisely where data are most valuable.

Taken together, the results depict a consistent economic narrative. Privacy violations cluster in large, intangible-heavy, data-centric firms that operate in concentrated industries and that lack strong creditor or board discipline—especially when the organisation has demonstrated a prior tolerance for regulatory risk. By contrast, robust internal oversight and credible stakeholder commitments materially lower the propensity to cross evolving data-governance boundaries.

4.2 Impact on shareholder wealth

In this section, we use the event study method to investigate the impact of data misconduct events on shareholder wealth. Our sample contains 122 data misconduct events from 91 distinct firms. Abnormal stock returns are calculated using the market-adjusted and market-model approaches. The market model parameters are estimated using 255 trading days of return data beginning 300 days before and ending 46 days before the misconduct event date. Both adjustment methods use an equally weighted return as a proxy for the market return. Daily abnormal stock returns are cumulated to obtain the CAR from day $t-5$ before the misconduct announcement date to day $t+5$

⁹Cabral (2016) models corporate reputation investment and firm persistent performance.

after the misconduct event date.

We gauge the capital-market penalty for privacy overreach with a standard event study. Panel A of Table 4 reports the mean and median CARs for alternative event windows. The mean CAR (-1, 1), CAR (-2, 2), and CAR (-5, 5) computed using the market model are -1.11%, -1.16%, and -1.80%, respectively. Marginal statistical significance falls as the window widens. The corresponding median CARs are -0.96%, -1.45%, and -1.25%, with similar significance patterns. The results from adjusting returns by simply subtracting the equally-weighted index return are consistently larger and more significant for both mean and medians. For example, the mean CARs are -1.19%, -1.25%, and -2.22% for windows (-1, 1), (-2, 2), and (-5, 5), respectively, and all are significant at the 1% level. Median returns are consistently even more negative. With an average market value of approximately RMB163 billion across the 122 misconduct events, the back-of-the-envelope estimate for the loss in market value based on the market-model CAR (-1,1) is around RMB1.79 billion.

How do these estimates compare with those from the financial misconduct literature? [Amiram et al. \(2018\)](#) note that point estimates of shareholder loss vary widely depending on the nature of the misconduct. Our estimates of an approximate 2% loss is similar to the 1.93% average abnormal return around 'less serious' reporting errors estimated by [Hennes et al. \(2008\)](#), and around half the 4.7% found by [Gande and Lewis \(2009\)](#) for firms targeted in securities class-action lawsuits.

[Amiram et al. \(2018\)](#) state that financial reporting misconduct is a significant threat to the existence and efficiency of capital markets, impairing trust between corporations and market participants and undermining capital market's ability to efficiently allocate resources, it is not surprising that financial misconduct has large impact on shareholder value. Though towards the lower end of losses from financial misconduct, our estimates imply that data misconduct is also severely

punished by Chinese capital markets.¹⁰

Panel B of Table 4 presents the results of testing determinants of the shareholder wealth impact of misconduct events using ordinary least squares regressions in which the dependent variable is CAR (-1, +1). All regressions include year-fixed effects, and most include industry-fixed effects. The first column considers a battery of firm-level variables.

Column (1) regresses CAR(-1,+1) on firm-level covariates. A single variable stands out: the coefficient on institutional block ownership is negative and statistically significant. This empirical finding implies that firms with larger blockholdings suffer the deepest announcement losses. Two complementary mechanisms can account for this pattern. First, large blockholders are typically sophisticated, low-latency traders. When the MIIT notice becomes public, they update valuations immediately and sell at scale, creating a concentrated order-flow shock that drives the stock price down more sharply than in firms whose ownership is dispersed. Second, strong blockholder monitoring is already capitalized into the pre-event valuation. A privacy violation at a “well-watched” firm, therefore, constitutes a larger information surprise: if intensive oversight failed to prevent boundary-pushing, investors infer that the underlying governance lapse is severe and that future remediation costs (or additional infractions) are more likely. The Bayesian revision of expected cash flows is consequently steeper, producing the larger negative CAR we observe.

Column (2) probes whether the market differentiates among violations according to the technological surface on which the offending app runs and the intensity of user attachment to that app. First, we construct an indicator that equals one if the cited application is available on any open-

¹⁰Not all alleged misconduct is punished. Haslem et al. (2017) document CARs around litigation filings differentiated by the nature of the suit. They find only small effects (CAR losses < 1%) for antitrust, civil rights, contract, intellectual property, personal injury and product liability cases. Financial misconduct is the standout case where losses are very large (CAR losses of around 9%). In the realm of data management, Kamiya et al. (2021) report mean losses of 0.8-1.2% around cyberattack announcements, noticeably lower than our point estimates.

source or multi-platform operating system (e.g., Android) and zero if distribution is restricted to Apple's closed iOS ecosystem. A privacy breach on an open platform generates a larger valuation shock—a 1.91 percentage-point extra decline in $CAR(-1,+1)$ —which translates into roughly RMB 3.1 billion in additional shareholder losses for the representative firm. The economics are straightforward: open-source architectures rely on a dispersed developer community and permit broader permission sets, so investors infer a higher ex-ante hazard rate of lax data controls. A citation therefore conveys a stronger negative signal about the firm's underlying governance quality and foreshadows more onerous remediation. In contrast, Apple's walled-garden model imposes centralised review and uniform permission standards; the same regulatory notice is thus interpreted as a less severe breakdown in internal discipline. Put differently, the marginal reputational damage from being caught misusing data is increasing in the prior belief that the platform is insecure.¹¹

Second, to gauge consumer reliance on the offending service we hand-collect each app's search index from Qimai—a Chinese analytics provider that back-calculates keyword volumes and download momentum.¹² We take the log of the five-day pre-event average as a proxy for latent user demand. The coefficient on this popularity measure is negative, as theory would predict: when an application is deeply embedded in users' daily routines, the present value of future rents that hinge on trust is larger, so a privacy shock should erase more equity value. However, the estimate is not statistically distinguishable from zero, suggesting that once the platform-governance channel is accounted for, incremental variation in short-term demand does not materially alter investors' reassessment of long-run cash-flow risk. One interpretation is that the market already capitalises broad popularity through fundamental multiples, leaving little marginal information in the search

¹¹Zang et al. (2015) document that Android applications transmit significantly more sensitive user data to third parties than iOS apps, illustrating the broader security externality investors likely have in mind.

¹²For detailed information about this database, please refer to the company's [website](#).

index at the time of the shock.

Columns (3) and (4) turn from firm-specific attributes to the competitive landscape in which the breach occurs. The coefficient on the industry Herfindahl–Hirschman Index (HHI) is positive: a one-standard-deviation increase in concentration—signalling weaker product-market rivalry—dampens the announcement loss. The mechanism is rooted by the classic study of [Porter \(1980\)](#). When consumers face few close substitutes, the elasticity of demand is low; a trust shock therefore translates into smaller revenue defections, and the disciplining role of future competitive pressure is muted. In effect, market power acts as an imperfect insurance policy against reputational damage, cushioning the equity hit.

In contrast, membership in a data-driven sector (as classified by the National Bureau of Statistics, 2021) magnifies the valuation penalty. For these businesses personal data are a first-order production input—fuel for recommendation algorithms, targeted advertising, and dynamic pricing. A privacy citation thus threatens not merely a temporary fine but the firm’s ability to harvest and monetise user information going forward, impairing the very cash-flow engine that supports its valuation. Put differently, the shadow price of trust is higher when data sit at the core of the revenue model; losing that trust triggers a disproportionately large downward revision in expected future earnings relative to tangibles-oriented industries.

4.3 Spillovers to Industry Peers

Whether a privacy citation reverberates beyond the focal firm hinges on the signal investors extract from the news. In a Bayesian framework with imperfect monitoring, a single enforcement action updates beliefs not only about the target’s compliance but also about the latent distribution of

misconduct across technologically similar firms. If the update is purely idiosyncratic (“bad apple”), peer prices should be flat or even rise as competitive pressure eases. If, instead, the Notice is interpreted as evidence of an industry-wide hazard (“rotten barrel”), valuations of uninvolved firms fall because expected future enforcement and remediation costs are revised upward.

4.3.1 Average spillover effect

Panel A of Table 5 indicates that investors treat a privacy citation as an industry-wide warning rather than a firm-specific mishap. For the 5,091 peer-firm observations in our sample, average cumulative abnormal returns are materially negative—roughly -0.30% over the $(-1, +1)$ window and between -0.40 and -0.96% across the broader $(-5, +5)$ span—no matter which return-generation model we employ.¹³ Median reactions are even more severe, revealing a left-skew in the cross-section. The pattern implies that a single MIIT notice resets investors’ beliefs about sector-wide compliance risk, in line with Bayesian “common-shock” learning models such as [Veldkamp \(2006\)](#): one public enforcement action is enough to raise the posterior that technologically similar firms are skating just as close to the regulatory edge.

4.3.2 What shapes the spillover?

Column (1) shows that the spillover is more severe for large peers and for those with higher return volatility. Larger firms have more to lose if data-governance costs escalate, while high-beta stocks are mechanically more sensitive to any rise in systematic risk. Interestingly, peers with larger boards are penalised more, suggesting that investors view extensive governance structures as a costly signal that serious compliance programmes will now have to scale further, eroding future

¹³Peers are defined as listed firms that share the cited company’s two-digit industry code.

cash flows. The effect is dampened for older and more highly levered firms, plausibly because such organisations have longer compliance track records and tighter creditor monitoring, reducing the incremental information content of a rival’s citation.

Column (2) interacts peer returns with the magnitude of the focal firm’s abnormal loss, our proxy for perceived misconduct severity.¹⁴ The coefficient is negative and economically large: a one-standard-deviation increase in severity (1.56%) deepens peer losses by roughly 6.7 basis points, or 22% of the average spillover. This is textbook Bayesian updating—the stronger the signal that the regulator uncovered a serious breach, the more investors extrapolate elevated enforcement risk to the rest of the industry.

Column (3) introduces an indicator for whether the cited firm sits in the top 5 % of industry sales. The sign flips: when a leader is caught, peers enjoy a modest positive CAR of +0.40% relative to the –0.30% baseline. Two forces are at play: (i) direct contagion raises risk premia, but (ii) a business-stealing effect reallocates future sales toward rivals (Bloom et al., 2013; Cao et al., 2021). For dominant targets, the second channel overwhelms the first, so net spillovers turn favourable—echoing standard IO predictions where a fall in a dominant player’s quality shifts residual demand toward fringe firms.

Column (4) shows that the negative spillover is markedly worse—about –0.50%—in NBSC-classified “data-driven” industries. In these sectors, personal data are a critical production input; hence, any hint of tighter regulation or user backlash is capitalised as a larger expected hit to future cash flows. Put differently, the option value of continued data access is highest where algorithms are core to value creation, so the loss of reputational trust carries a bigger price tag.

¹⁴We measure misconduct severity using $CAR(-1,1) \times -100$ of misconduct firms, assuming that larger negative abnormal returns reflect greater perceived misconduct severity from investors’ viewpoints.

Finally, Column (5) interacts leader status with market structure. Where rivalry is intense (low HHI), leader misconduct boosts peers even more, because customers can switch suppliers quickly, amplifying the business-stealing channel. Conversely, in concentrated markets the contagion component dominates and the net effect reverts to zero. Within data-driven sectors, however, even leader misconduct generates a strongly negative net spillover (−1.96%). Here, investors evidently believe that the regulatory spotlight will widen to all firms relying on similar data architectures, swamping any competitive windfall.

4.3.3 Discussion

The spillover findings can be reconciled with standard theory once one recognises that a data-privacy citation is simultaneously a signal about industry-wide risk and a shock to relative competitive strength. In conceptual terms, investors form beliefs about the underlying regulatory environment—specifically, the likelihood and severity of future enforcement actions against firms that share similar data architectures. When the regulator cites one firm, Bayesian updating à la [Veldkamp \(2006\)](#) leads investors to revise upward the probability that the broader industry operates in a “high-enforcement” regime. This shift increases discount rates and expected compliance costs for peers whose technological exposure resembles that of the cited firm. The magnitude of this common-risk update grows with both the strength of the regulatory signal (proxied empirically by the cited firm’s own CAR) and the degree of technological similarity across firms, which is greatest in data-centric industries where personal information is a core production input.

Concurrently, classic oligopoly models with horizontally differentiated products (e.g., Hotelling-Bertrand competition) imply that a negative quality shock to one supplier reallocates some demand

to its rivals, raising their incremental cash flows.¹⁵ Whether the net spillover is positive or negative therefore depends on which of these two forces dominates. In asset-heavy, low-information industries, technological similarity is low, so the business-stealing channel can outweigh a modest common-risk update—hence leader misconduct may benefit rivals. In contrast, in digital sectors the underlying technological exposure is highly correlated: once the enforcement bar is revealed to be higher, every firm that monetises user data must invest in parallel remediation, so the increase in systematic compliance cost more than offsets any market-share windfall. This logic also explains why concentration (high HHI) dampens the negative shock: when alternatives are scarce, the elasticity of substitution is low, muting both the competitive exodus from the cited firm and the perceived threat of industry-wide churn.

Put differently, the event induces a joint shift in both the expected mean and variance of future cash flows. Where data are peripheral, the variance channel is weak and the mean shift for rivals can be positive; where data are central, the variance channel is strong and becomes dominant. Under either regime, investors act as rational learners, and the observed cross-section of peer CARs aligns with the comparative-static predictions of Bayesian common-shock updating married to standard product-market rivalry.

4.4 Misconduct and cost of debt

The equity-market evidence shows that a privacy citation destroys shareholder wealth and, in competitive industries, hands a relative advantage to rivals. Creditors, however, are loss-averse claimants who focus on downside risk and cash-flow stability. If a breach elevates the likelihood of regulatory fines, customer churn, or costly remediation, lenders should price that incremental

¹⁵See, inter alia, [Berry et al. \(1995\)](#) on demand substitution and [Porter \(1980\)](#) for the managerial analogue.

default risk ex-ante. This follows directly from structural credit-risk theory, where the spread compensates for the option value of default (Merton, 1974; Leland, 1998). In line with the loan-pricing results for financial misstatements and external cyberattacks documented by Chava et al. (2018) and Huang and Wang (2021), we test whether an MIIT notice translates into higher debt costs.

4.4.1 Identification

For each firm that appears in an MIIT notice we pin down a unique “event year,” τ , defined as the fiscal year that contains the first disclosure. A firm-level treatment indicator, $Treat_i$, equals one for the 79 non-financial A-share companies that receive at least one notice during 2019–2022 and zero otherwise. The time-varying variable $Post_{it}$ switches from zero to one in fiscal year τ and stays at one thereafter; for never-cited firms it remains zero throughout. The interaction $Treat_i \times Post_{it}$ therefore captures the incremental change in borrowing costs after the initial citation, relative to (i) the firm’s own pre-notice path and (ii) a control group of observationally similar peers that are never cited.

To construct that control group we implement propensity-score matching (PSM) within the same two-digit SIC code and fiscal year, a design that holds constant both industry credit conditions and macro shocks. Beginning with the full population of Shanghai- and Shenzhen-listed firms from 2016-2022, we drop financial institutions, observations with missing variables, and potential controls that have data gaps around any treatment year; all continuous variables are winsorised at the 1st and 99th percentiles. We then estimate a probit model in which the dependent variable is an indicator for being cited in year t , and the covariates are those that theory and earlier results show predict both data misconduct and loan pricing: the logarithm of total assets, firm age, asset tangibility, leverage, state-ownership status, institutional block ownership, board size (log of di-

rectors), and the proportion of independent directors. The fitted value of this regression is each firm’s propensity score. Inside every industry–year cell the cited firm is paired with the non-cited firm whose score is numerically closest, using 1:1 nearest-neighbour matching without replacement. This procedure yields 79 treated firms and 79 matched controls—158 firms in total—for the subsequent difference-in-differences (DiD) panel.

Panel A of Table 6 reports mean and median values of all eight matching variables for the two groups; none of the differences is statistically significant, confirming that the PSM removes observable selection bias. Consequently, the coefficient on $Treat_i \times Post_{it}$ in the DiD regressions isolates the causal effect of an MIIT citation on the cost of debt, net of pre-treatment heterogeneity in size, governance, leverage, or industry conditions.

4.4.2 Difference-in-differences tests

We estimate a firm–year difference-in-differences (DiD) model that compares guilty firms with propensity-score-matched controls from the same two-digit SIC industry and fiscal year. The estimation equation is

$$COD_{it} = \alpha + \beta_1 Post_{i,t} \times Treat_i + \beta_2 X_{i,t-1} + \delta_t + \omega_i + \varepsilon_{i,t} \quad (1)$$

where COD is measured (i) as interest expense divided by total liabilities (COD1) and, for robustness, (ii) by the same numerator over the average of beginning- and end-of-year liabilities (COD2). Year dummies absorb macro credit-cycle swings; firm fixed effects control for time-invariant risk factors. Financial firms are excluded because their liabilities are operational and their privacy

notices—often KYC-related—carry a different risk interpretation.¹⁶

Panel B of Table 6 reports a β_1 of 0.42 percentage points for COD1—an economically large jump given a pre-event mean cost of 1.49%. The increase remains at 0.34–0.42% when we alter the cost-of-debt denominator or add time-varying controls, implying an average 28% rise in interest burden. Because event timing is staggered, we re-estimate using the Callaway and Sant’Anna (2021) estimator. Figure 3 and Table 7 show flat, insignificant pre-trends and a monotone post-notice escalation, validating the parallel-trends assumption.

Three non-mutually-exclusive channels can rationalise the spread widening. First, a breach increases *cash-flow volatility*: regulatory audits and loss of user trust amplify earnings variance, and in a Merton framework higher asset volatility widens credit spreads. Second, it lowers the *expected recoverable asset value*: the cost of rebuilding compliant data architecture and potential user attrition push the firm closer to the default boundary. Third, the notice provides a *governance signal*: lenders infer that latent control problems extend beyond data management, raising the subjective probability of future negative shocks. Each mechanism increases the priced probability of distress, so rational creditors compensate by charging a higher coupon.

In short, privacy overreach imposes a dual capital-market penalty. Equity investors suffer an immediate valuation hit, while debt investors reprice risk more gradually, producing a persistent increase in the cost of external finance even in the absence of formal monetary fines.

4.5 Cross-sectional tests

The baseline DiD results establish that an MIIT privacy citation lifts a firm’s borrowing cost by roughly 30 bps. We now explore which firms are hit hardest. Classical credit-risk theory predicts

¹⁶Including financial companies leaves the coefficients qualitatively unchanged; results are available upon request.

that the marginal spread increase should be larger when a notice either (i) compounds pre-existing concerns about the borrower’s integrity or (ii) threatens the future cash-flow path that serviceability depends upon. We operationalise those ideas with six ex-ante characteristics—prior misconduct, product-market rivalry, financial slack, and three measures of innovative capacity—and re-estimate equation (1) within subsamples split on the median (Table 8). All regressions retain the same covariates, year dummies, and firm fixed effects used in Table 6. Results are summarised below.

4.5.1 Violation history

Firms with a history of misconduct are more likely to face severe financial penalties, which can imply higher debt costs when new violations occur. Roychowdhury and Srinivasan (2019) show that prior violations lead to harsher credit ratings, which typically result in increased borrowing costs. Egan et al. (2019) find that repeat offenders are significantly more likely to engage in further misconduct, suggesting compounded financial risks. In a similar vein, financial advisors with a history of infractions are more likely to face future complaints and settlements, highlighting the persistent financial risks associated with past misconduct (Law and Mills, 2019).

In dynamic moral-hazard models, a lender observing a second infraction updates the posterior that the borrower is a “bad” type, raising the perceived hazard rate of future default. This lowers the borrower’s reputation capital and increases the spread required to satisfy incentive compatibility.¹⁷

We group firms into two sub-samples based on whether they experienced financial misconduct in the three years preceding the app citation. Panel A of Table 8 confirms the prediction: coefficients in the “Yes” columns (prior offences) are significantly larger, implying that app mis-

¹⁷For example, in the model of Diamond (1989), borrowers are of unobservable quality; each period’s performance (or misconduct) updates the lender’s posterior belief. A second infraction therefore shifts the borrower’s perceived type toward the “bad” state, raising the probability of future default and, in equilibrium, the promised spread.

conduct adds roughly twice as many basis points to the cost of debt when the borrower is already a recidivist. Creditors therefore treat an MIIT notice as an incremental blow to an already-damaged credibility stock.

4.5.2 Industry competition

Product-market rivalry sharpens the way creditors respond to a privacy citation. In a competitive industry a loss of reputation quickly translates into customer defections, price cuts, and lower future cash flows; lenders therefore perceive a larger jump in default risk. This mechanism is well documented for accounting fraud and operational failures (see, e.g., the event-study evidence in [Cao et al. \(2021\)](#), [Chen et al. \(2024\)](#), and [Von Meyerinck et al. \(2024\)](#)). We test whether the same logic applies to data-governance breaches.

Using the inverse of the Herfindahl index as our rivalry measure, we classify industries below the sample-median HHI as “highly competitive.” Panel B of Table 8 shows that an MIIT notice raises the cost of debt by roughly 51 bp in these arenas, yet by only 15 bp where concentration is greater. The differential is economically large and statistically significant. Two forces likely drive the pattern: (i) cash-flow sensitivity—with many substitutes, customers can switch away from the tainted platform at low cost, shrinking the borrower’s revenue base; and (ii) strategic retaliation—alert competitors step up marketing and compliance signalling, further eroding the violator’s margins. Anticipating both channels, creditors charge a steeper spread when misconduct is revealed in a competitive setting.

The finding extends prior results on traditional misconduct to the digital realm: even when penalties are purely reputational, competitive pressure magnifies the financing consequences, underscoring how data-privacy lapses have become a salient component of operational risk in modern

product markets.

4.5.3 Financial constraints

Financially constrained firms enter the data economy with thinner cash buffers and a heavier reliance on external finance. When an MIIT notice removes illicit data advantages and forces costly remediation, these firms take a double hit: liquidity tightens just as revenues become more uncertain. Under the peck-ordering logic of [Rajan and Zingales \(1998\)](#), their shadow cost of finance should climb sharply. Field evidence supports the asymmetry: easing constraints boosts innovation ([McKenzie, 2017](#)), whereas bad news triggers especially large penalties for cash-strapped firms ([Eaglin, 2023](#)).

Consistent with this view, we split the sample at the median Kaplan–Zingales (KZ) index. Panel C of Table 8 shows that an MIIT citation widens credit spreads by about 55 basis points in the high-KZ group—over ten times the 7 bp increase for their low-KZ counterparts. Lenders evidently conclude that constrained borrowers face both greater near-term cash-flow volatility and limited capacity to fund compliance upgrades, and they price the notice as a material jump in default risk.

4.5.4 R&D and digital adoption

Innovation capacity alters the way creditors price a privacy citation. In a data-intensive economy, firms with deep R&D pipelines and advanced analytics can (i) substitute proprietary algorithms for raw personal data, and (ii) re-engineer compliance architectures at lower marginal cost. Both channels dampen the expected cash-flow shock and, in standard structural models of credit risk, translate into a smaller jump in spreads. By contrast, firms that lag on technological capability are

doubly exposed: the notice both curtails a key growth input and forces costly remediation, pushing the asset–liability process closer to the default boundary. A growing empirical literature documents this asymmetry—low-R&D firms recover more slowly from macro shocks (Dukes et al., 1980), while leaders in AI and data analytics convert digital capital into higher productivity and more resilient cash flows (Brynjolfsson and McElheran, 2016; Farboodi and Veldkamp, 2020; Babina et al., 2024). Consistent with those insights, we split the sample along three technology margins.

First, R&D effort. Using the median ratio of R&D expense to sales, we classify firms into high- and low-intensity groups. Panel D of Table 8 shows that a privacy notice raises borrowing costs by roughly 45 bp for the low-R&D group but by only 10 bp for the high-R&D group.

Second, codified digital know-how. The count of digital-technology patent applications provides an orthogonal proxy for data-related inventive output. Panel E reveals the same pattern: firms below the median patent stock face a spread increase of about 70 bp, versus 17 bp for patent-rich peers.

Third, organisational big-data infrastructure. We use text-mine annual reports for keywords such as “data mining,” “visualisation,” or “heterogeneous data,” and scale by total word count. Firms in the bottom half of this distribution incur a 74 bp post-notice penalty; top-half adopters about 23 bp (Panel F).

Taken together, the evidence matches theoretical priors: where technological slack is greatest, a data-privacy citation threatens both current earnings and future growth options, so creditors demand a markedly higher risk premium. Conversely, firms at the digital frontier—notwithstanding the same legal violation—retain the flexibility to pivot away from raw-data dependence, contain remediation costs, and thus convince lenders that default risk has risen by far less.

In short, the price of governance failure is not uniform. It is amplified for borrowers that

combine weak innovation capacity with heavy reliance on user data, and muted for those that possess the R&D depth and digital assets needed to absorb the shock. This heterogeneity underscores how reputational enforcement can widen pre-existing dispersion in the cost of capital, reallocating financial resources toward technologically adaptable firms in the modern data economy.

4.6 Economic outcome tests

The evidence so far shows that an MIIT “naming-and-shaming” notice raises both equity and debt costs. Two channels are theoretically salient. First, public censure erodes the firm’s reputation capital, thereby depressing sales and profitability. Second, the shock heightens cash-flow volatility, pushing the firm closer to the default boundary in a Merton-style capital-structure model. We test each mechanism in turn.

4.6.1 Reputation and operating performance

Loss of stakeholder trust is the canonical penalty for misconduct.¹⁸ In data-intensive businesses that rely on continuous consumer consent, reputational capital is even more valuable ([Brynjolfsson and McElheran, 2016](#); [Goldfarb and Que, 2023](#)). A privacy citation, by threatening future data access, should therefore cut directly into revenue and margins.

To operationalise firm reputation we adopt the latent-factor technique of [Agarwal et al. \(2015\)](#). Each year we gather twelve observable measures that various stakeholders monitor: three market-facing indicators (a firm’s industry rank in sales, total assets, and brand value); three creditor-oriented ratios (current ratio, long-term-debt ratio, and overall leverage); three equity-holder signals (earnings per share, cash dividend per share, and an indicator for engagement of a Big-Four

¹⁸See the early fraud studies of [Fich and Shivdasani \(2007\)](#) and [Karpoff et al. \(2008a,b\)](#).

auditor); and three governance proxies (the sustainable-growth rate and the proportion of independent directors). After standardising these variables we run a principal-component analysis and use the first component—which explains the largest share of common variation—as our composite reputation score. Firms are then sorted into deciles each year, with 1 denoting the lowest and 10 the highest reputational standing.

Panel A of Table 9 shows that the DiD interaction ($Treat \times Post$) reduces the reputation score by roughly one decile and, consistent with that loss of goodwill, lowers sales-growth by 12%, ROA by 3.6%, and ROE by 11%. The magnitudes dwarf those reported for one-off cyber intrusions in [Kamiya et al. \(2021\)](#) or external data breaches in [Huang and Wang \(2021\)](#), suggesting that internal privacy abuse is perceived as a deeper organisational failing. Because both the level and stability of operating cash flow enter credit-spread models, these results provide a direct link between the notice and the subsequent jump in borrowing costs.

4.6.2 Operational risk

Higher earnings volatility increases the uncertainty surrounding a firm's future cash flows and, by extension, its capacity to meet fixed debt-service obligations. In Merton's structural framework, greater cash-flow volatility raises the probability that asset values will dip below the face value of liabilities before maturity, triggering default ([Merton, 1974](#)). Creditors therefore charge a risk premium whenever a borrower's earnings become more erratic. In the context of app misconduct, two mechanisms naturally lift volatility: (i) the abrupt withdrawal or redesign of data-driven revenue engines (e.g. personalised ads, recommendation algorithms) once illicit data practices are curtailed, and (ii) the costly experimentation with alternative growth strategies while compliance systems are overhauled. Either channel makes quarterly profits less predictable, inducing lenders

to reassess downside risk.

To quantify this effect, we follow [John et al. \(2008\)](#) and [Faccio et al. \(2011\)](#), computing the standard deviation of ROA and ROE over rolling five-year windows that end in the disclosure year. We then regress these volatility measures on the DiD term $Treat_i \times Post_{i,t}$. Columns (1)–(4) of Panel B in [Table 9](#) show positive, statistically significant coefficients at the 5% level for both σ_{ROA} and σ_{ROE} . Relative to their own pre-notice history and to matched controls, cited firms experience an economically meaningful uptick in earnings variance.

This post-notice rise in operating risk offers a direct channel linking data-privacy lapses to the 40-basis-point increase in borrowing costs documented earlier. From a creditor’s perspective, the sanction signals that the firm’s data assets—central to customer acquisition and retention—are now less reliable sources of cash flow. Absent those stabilising data streams, the firm’s payoff distribution widens, moving it closer to the default boundary outlined by Merton. The market consequently prices a higher probability of financial distress, reinforcing the view that data governance failures propagate through both the reputation and risk-taking dimensions of corporate finance.

5 Conclusions

This study investigates the impact of data privacy misconduct by firms in the mobile application industry on firm performance, focusing on debt financing costs and market reactions to data privacy violations. Exploiting the unique regulatory environment in China, where the Ministry of Industry and Information Technology publicly identifies but does not fine firms engaged in unlawful data practices, we provide robust empirical evidence on the economic consequences of such misconduct.

Our findings reveal several insights. First, the announcement of data misconduct leads to significant negative abnormal returns, implying substantial shareholder wealth loss as investors perceive these events as detrimental to firm value. The market's reaction is particularly severe for firms with high media attention and those operating in competitive, data-driven sectors. Also, we observe significant negative spillover effects on industry peers, indicating that data misconduct by one firm adversely affects the market value of other firms within the same industry. This suggests that such misconduct is perceived as indicative of broader industry-wide issues, amplifying the negative impact across the sector.

Second, using a difference-in-difference analysis, we identify the causal relationship between borrowing costs and data misconduct. Firms found guilty of app misconduct experience a substantial rise in borrowing costs. This increase is more pronounced for firms with a history of violations, those operating in competitive sectors, firms under financial constraints, and those with limited digital innovation, highlighting the compounded risk perceived by creditors.

Third, we provide a channel test to explore the economic mechanism for the raised debt financing for infringing firms. The rise in debt costs is primarily driven by increased risk-taking and reputation loss. Our analysis shows that firms guilty of data misconduct suffer reputation loss, reflected by declines in sales growth, ROA, and ROE. Moreover, these firms engage in higher risk-taking, as evidenced by greater earnings volatility.

In summary, our study offers implications for both China and the broader international community regarding data regulation. From an economic and corporate finance perspective, when a firm's data practices are called into question by regulators, lenders anticipate higher default risk due to potential legal penalties, remediation costs, and the loss of consumer trust, which directly impacts the firm's cash flows and profitability. This heightened risk perception necessitates a risk

premium, thus increasing the cost of debt. Additionally, firms embroiled in data privacy scandals may face more stringent borrowing terms, reduced access to capital, and higher interest rates, reflecting the lenders' demand for compensation for the increased risk of lending to a compromised entity. It also shows that the Chinese approach of "naming and shaming" those guilty of misconduct has significant impact, even in the absence of fines or restrictions on the activities of guilty firms.

References

- Agarwal, J., Osiyevskyy, O., and Feldman, P. M. (2015). Corporate reputation measurement: Alternative factor structures, nomological validity, and organizational outcomes. *Journal of Business Ethics*, 130:485–506.
- Amiram, D., Bozanic, Z., Cox, J. D., Dupont, Q., Karpoff, J. M., and Sloan, R. (2018). Financial reporting fraud and other forms of misconduct: a multidisciplinary review of the literature. *Review of Accounting Studies*, 23:732–783.
- Anderson, R. C., Mansi, S. A., and Reeb, D. M. (2004). Board characteristics, accounting report integrity, and the cost of debt. *Journal of Accounting and Economics*, 37(3):315–342.
- Aridor, G., Che, Y.-K., and Salz, T. (2023). The effect of privacy regulation on the data industry: Empirical evidence from gdpr. *RAND Journal of Economics*, 54:695–730.
- Ashraf, M. (2022). The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review*, 97(2):1–24.
- Ashraf, M. and Sunder, J. (2023). Can shareholders benefit from consumer protection disclosure mandates? evidence from data breach disclosure laws. *The Accounting Review*, 98(4):1–32.
- Babina, T., Fedyk, A., He, A., and Hodson, J. (2024). Artificial intelligence, firm growth, and product innovation. *Journal of Financial Economics*, 151:103745.
- Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, 76(2):169–217.

- Berry, S. T., Levinsohn, J. A., and Pakes, A. (1995). Automobile prices in market equilibrium: Part i and ii.
- Bessen, J. E., Impink, S. M., Reichensperger, L., and Seamans, R. (2020). Gdpr and the importance of data to ai startups. *Working paper, NYU Stern School of Business*.
- Bian, B., Ma, X., and Tang, H. (2021). The supply and demand for data privacy: Evidence from mobile apps. *Available at SSRN 3987541*.
- Bloom, N., Schankerman, M., and Van Reenen, J. (2013). Identifying technology spillovers and product market rivalry. *Econometrica*, 81(4):1347–1393.
- Brynjolfsson, E. and McElheran, K. (2016). The rapid adoption of data-driven decision-making. *American Economic Review*, 106(5):133–139.
- Cabral, L. (2016). Living up to expectations: Corporate reputation and persistence of firm performance. *Strategy Science*, 1(1):2–11.
- Callaway, B. and Sant’Anna, P. H. (2021). Difference-in-differences with multiple time periods. *Journal of Econometrics*, 225(2):200–230.
- Cao, S. S., Fang, V. W., and Lei, L. G. (2021). Negative peer disclosure. *Journal of Financial Economics*, 140(3):815–837.
- Chava, S., Huang, K., and Johnson, S. A. (2018). The dynamics of borrower reputation following financial misreporting. *Management Science*, 64(10):4775–4797.
- Chen, J., Su, X., Tian, X., Xu, B., and Zhang, X. (2024). Do product market threats discipline corporate misconduct? *Leeds University Business School Working Paper*.

- Chen, L., Huang, Y., Ouyang, S., and Xiong, W. (2021). The data privacy paradox and digital demand. Technical report, National Bureau of Economic Research.
- Demirer, M., Hernández, D. J. J., Li, D., and Peng, S. (2024). Data, privacy laws and firm production: Evidence from the gdpr. Technical report, National Bureau of Economic Research.
- Diamond, D. W. (1989). Reputation acquisition in debt markets. *Journal of Political Economy*, 97(4):828–862.
- Dukes, R. E., Dyckman, T. R., and Elliott, J. A. (1980). Accounting for research and development costs: The impact on research and development expenditures. *Journal of Accounting Research*, pages 1–26.
- Dyck, A., Morse, A., and Zingales, L. (2024). How pervasive is corporate fraud? *Review of Accounting Studies*, 29(1):736–769.
- Eaglin, F. C. (2023). The need for speed: The impact of capital constraints on strategic misconduct. Available at SSRN 4703027.
- Egan, M., Matvos, G., and Seru, A. (2019). The market for financial adviser misconduct. *Journal of Political Economy*, 127(1):233–295.
- Faccio, M., Marchica, M.-T., and Mura, R. (2011). Large shareholder diversification and corporate risk-taking. *The Review of Financial Studies*, 24(11):3601–3641.
- Farboodi, M. and Veldkamp, L. (2020). Long-run growth of financial data technology. *American Economic Review*, 110(8):2485–2523.

- Fich, E. M. and Shivdasani, A. (2007). Financial fraud, director reputation, and shareholder wealth. *Journal of Financial Economics*, 86(2):306–336.
- Gande, A. and Lewis, C. M. (2009). Shareholder-initiated class action lawsuits: Shareholder wealth effects and industry spillovers. *Journal of Financial and Quantitative Analysis*, 44(4):823–850.
- Goldberg, S., Johnson, G., and Shriver, S. (2019). Regulating privacy online: The early impact of the gdpr on european web traffic & e-commerce outcomes. *Available at SSRN*, 3421731.
- Goldfarb, A. and Que, V. F. (2023). The economics of digital privacy. *Annual Review of Economics*, 15(1):267–286.
- Goldfarb, A. and Tucker, C. (2019). Digital economics. *Journal of Economic Literature*, 57(1):3–43.
- Goldfarb, A. and Tucker, C. E. (2024). *The Economics of Privacy*. University of Chicago Press.
- Hart, O. D. and Moore, J. (1995). Debt and seniority: An analysis of the role of hard claims in constraining management.
- Haslem, B., Hutton, I., and Smith, A. H. (2017). How much do corporate defendants really lose? a new verdict on the reputation loss induced by corporate litigation. *Financial Management*, 46(2):323–358.
- Heese, J., Pérez-Cavazos, G., and Peter, C. D. (2022). When the local newspaper leaves town: The effects of local newspaper closures on corporate misconduct. *Journal of Financial Economics*, 145(2):445–463.

- Hennes, K. M., Leone, A. J., and Miller, B. P. (2008). The importance of distinguishing errors from irregularities in restatement research: The case of restatements and ceo/cfo turnover. *The Accounting Review*, 83(6):1487–1519.
- Huang, H. H. and Wang, C. (2021). Do banks price firms' data breaches? *The Accounting Review*, 96(3):261–286.
- Jensen, M. C. (1986). Agency costs of free cash flow, corporate finance, and takeovers. *The American Economic Review*, 76(2):323–329.
- Jiang, J. (2008). Beating earnings benchmarks and the cost of debt. *The Accounting Review*, 83(2):377–416.
- John, K., Litov, L., and Yeung, B. (2008). Corporate governance and risk-taking. *The Journal of Finance*, 63(4):1679–1728.
- Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., and Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 139(3):719–749.
- Kaplan, S. N. and Zingales, L. (1997). Do investment-cash flow sensitivities provide useful measures of financing constraints? *The Quarterly Journal of Economics*, 112(1):169–215.
- Karpoff, J. M., Koester, A., Lee, D. S., and Martin, G. S. (2017). Proxies and databases in financial misconduct research. *The Accounting Review*, 92(6):129–163.
- Karpoff, J. M., Lee, D. S., and Martin, G. S. (2008a). The consequences to managers for cooking the books. *Journal of Financial Economics*, 88(88):193–215.

- Karpoff, J. M., Lee, D. S., and Martin, G. S. (2008b). The consequences to managers for financial misrepresentation. *Journal of Financial Economics*, 88(2):193–215.
- Kedia, S. and Rajgopal, S. (2011). Do the sec’s enforcement preferences affect corporate misconduct? *Journal of Accounting and Economics*, 51(3):259–278.
- Law, K. K. and Mills, L. F. (2019). Financial gatekeepers and investor protection: Evidence from criminal background checks. *Journal of Accounting Research*, 57(2):491–543.
- Leland, H. E. (1998). Agency costs, risk management, and capital structure. *The Journal of Finance*, 53(4):1213–1243.
- Liu, X. (2016). Corruption culture and corporate misconduct. *Journal of Financial Economics*, 122(2):307–327.
- Mansi, S. A., Maxwell, W. F., and Miller, D. P. (2011). Analyst forecast characteristics and the cost of debt. *Review of Accounting Studies*, 16:116–142.
- McKenzie, D. (2017). Identifying and spurring high-growth entrepreneurship: Experimental evidence from a business plan competition. *American Economic Review*, 107(8):2278–2307.
- Merton, R. C. (1974). On the pricing of corporate debt: The risk structure of interest rates. *The Journal of Finance*, 29(2):449–470.
- Peukert, C., Bechtold, S., Batikas, M., and Kretschmer, T. (2022). Regulatory spillovers and data governance: Evidence from the gdpr. *Marketing Science*, 41(4):746–768.
- Porter, M. E. (1980). *Competitive Strategy: Techniques for analyzing industries and competitors*, volume 1.

- Qi, Y., Roth, L., and Wald, J. K. (2010). Political rights and the cost of debt. *Journal of Financial Economics*, 95(2):202–226.
- Rajan, R. and Zingales, L. (1998). Financial dependence and growth. *American Economic Review*, 88(3):559–586.
- Roychowdhury, S. and Srinivasan, S. (2019). The role of gatekeepers in capital markets. *Journal of Accounting Research*, 57(2):295–322.
- Schmitt, J., Miller, K. M., and Skiera, B. (2022). The impact of privacy laws on online user behavior. *HEC Paris Research Paper*.
- Sun, T., Yuan, Z., Li, C., Zhang, K., and Xu, J. (2024). The value of personal data in internet commerce: A high-stakes field experiment on data regulation policy. *Management Science*, 70(4):2645–2660.
- Tambe, P., Hitt, L., Rock, D., and Brynjolfsson, E. (2020). Digital capital and superstar firms. Technical report, National Bureau of Economic Research.
- Valta, P. (2012). Competition and the cost of debt. *Journal of Financial Economics*, 105(3):661–682.
- Van Binsbergen, J. H., Graham, J. R., and Yang, J. (2010). The cost of debt. *The Journal of Finance*, 65(6):2089–2136.
- Veldkamp, L. L. (2006). Information markets and the comovement of asset prices. *The Review of Economic Studies*, 73(3):823–845.

Velte, P. (2023). The link between corporate governance and corporate financial misconduct. a review of archival studies and implications for future research. *Management Review Quarterly*, 73(1):353–411.

Von Meyerinck, F., Pursiainen, V., and Schmid, M. (2024). Competition and the reputational costs of litigation. *University of St. Gallen, School of Finance Research Paper*, (2024/07).

Zang, J., Dummit, K., Graves, J., Lisker, P., and Sweeney, L. (2015). Who knows what about me? a survey of behind the scenes personal data sharing to third parties by mobile apps. *Technology Science*, 30:2–1.

A Variable Descriptions

A.1 This appendix provides detailed descriptions of all the variables used in the tables.

- **Total assets:** The logarithm of total assets. *Source: CSMAR*
- **Firm age:** The logarithm of the years since company establishment. *Source: CSMAR*
- **Asset tangibility:** Fixed assets divided by total assets. *Source: CSMAR*
- **Leverage:** Total debt divided by total assets. *Source: CSMAR*
- **State-owned enterprise:** One for state-owned enterprises, and zero otherwise. *Source: CN-RDS*
- **Institutional block ownership:** The fraction of shares held by the institutional shareholder. *Source: CSMAR*
- **Log(directors number):** The logarithm of the number of total directors. *Source: CSMAR*
- **Independent directors (%):** Number of independent directors divided by total directors. *Source: CSMAR*
- **Stock return volatility:** Standard deviation of a firm's daily stock returns during a year. *Source: CSMAR*
- **Violation History:** 0-1 variable, equal to 1 if the firm had a fraud experience in the past 3 year, and 0 otherwise. *Source: RESSET*

- **CSR performance:** One if voluntarily released corporate social responsibility reports, and zero otherwise. *Source: CSMAR*
- **High ESG rating:** One if the misconduct companies' ESG rating is above BB, and zero otherwise. ESG rating data is derived from the Huazheng Index, which divides the ESG performance of enterprises into nine levels: low to high C, CC, CCC, B, BB, BBB, A, AA, AAA. *Source: WIND*
- **Industry's Herfindahl index:** Index computed as the sum of squared market shares of firms' sales at the industry level. *Source: CSMAR*
- **Data-driven industry:** According to the "Statistical Classification of the Digital Economy and its Core Industries (2021)", categories 04 are classified as data-driven industries in the digital economy. *Source: Manually collected*
- **non-iPhone:** 0-1 variable, equal to 1 if the app is only available on non-iOS systems.
- **APP search index:** The logarithm of the misconduct app's average search index for the 5 days before the event date. The search index is derived from the "QiMai Data" official website, calculated from search results, download volume, associated keywords, and other metrics based on the app Store. *Source: Manually collected*
- **Misconducts' Severity:** The opposite number of misconduct events' CAR (-1, 1) based on the market model. *Source: Manually calculation*
- **Industry leader misconduct:** Denoted as D_{ILM} . One if the misconduct firms' total sales rank among the top 1% in the industry, and zero otherwise. *Source: Manually calculation*

- **COD1:** (Interest expense/total liabilities)*100 *Source: CSMAR*
- **COD2:** (Interest expense/average liabilities)*100 *Source: CSMAR*
- **Treat:** 0-1 variable, equal to 1 if the sample is a treatment group firm, and 0 otherwise.
Source: Manually calculation
- **Post:** 0-1 variable, equal to 1 if the sample is from the post-treatment period, and 0 otherwise.
Source: Manually calculation
- **Financing constraints:** Measured by KZ index ([Kaplan and Zingales, 1997](#)). *Source: CS-MAR*
- **R&D intensity:** R&D expenditure/revenue. *Source: CNRDS*
- **Digital Technology Innovation :** Number of digital technology patent applications. *Source: CNRDS*
- **Big Data Technology:** Frequency of big data technology-related terms in the annual report/total word count of the annual report. *Source: CSMAR*
- **Firm reputation:** The firm reputation score was calculated using factor analysis based on 12 indicators from different stakeholder perspectives. Enterprises were then ranked by their scores from lowest to highest and divided into ten groups, with scores assigned sequentially from 1 to 10. *Source: CSMAR*
- **Sales growth:** $(Sales_t - Sales_{t-1}) / Sales_{t-1}$ *Source: CSMAR*
- **ROA:** Net income divided by total assets. *Source: CSMAR*

- **ROE**: Net income divided by shareholders' equity. Source: CSMAR
- **Firmrisk1**: The standard deviation of ROA for past 5 years (i.e., $t - 4$ to t) Source: CSMAR
- **Firmrisk2**: The standard deviation of ROE for past 5 years (i.e., $t - 4$ to t) Source: CSMAR

B Data Protection and Privacy Regulations

B.1 This appendix provides brief descriptions of major data protection and digital privacy regulations around th world.

- **European Union (EU) - General Data Protection Regulation (GDPR):** The GDPR, enacted on May 25, 2018, has served as a benchmark for data privacy laws globally. The policy is characterized by its stringent consent requirements, rights for data subjects, including the right to be forgotten, and significant penalties for non-compliance. GDPR also stresses the policy applies to member states and any organization that deals with EU data.¹⁹
- **United States - California Consumer Privacy Act (CCPA):** Effective from January 2020, the CCPA introduced data privacy measures similar to the GDPR but with a focus on California residents' rights and transparency regarding their personal data. The act mandates enterprises to disclose their data collection and sharing practices and provides consumers the right to opt out of data selling.
- **Canada - Personal Information Protection and Electronic Documents Act (PIPEDA):** The PIPEDA was effective in 2000. The act governs collecting, using, and disclosing personal data in commercial activities across Canada. The PIPEDA strengthens the protection of the privacy rights of individuals, which is aligned with trust promotion in e-commerce.
- **Japan - The Japan Act on the Protection of Personal Information (APPI):** The APPI was adopted in 2003. The act safeguards the personal data of Japanese citizens. It mandates that

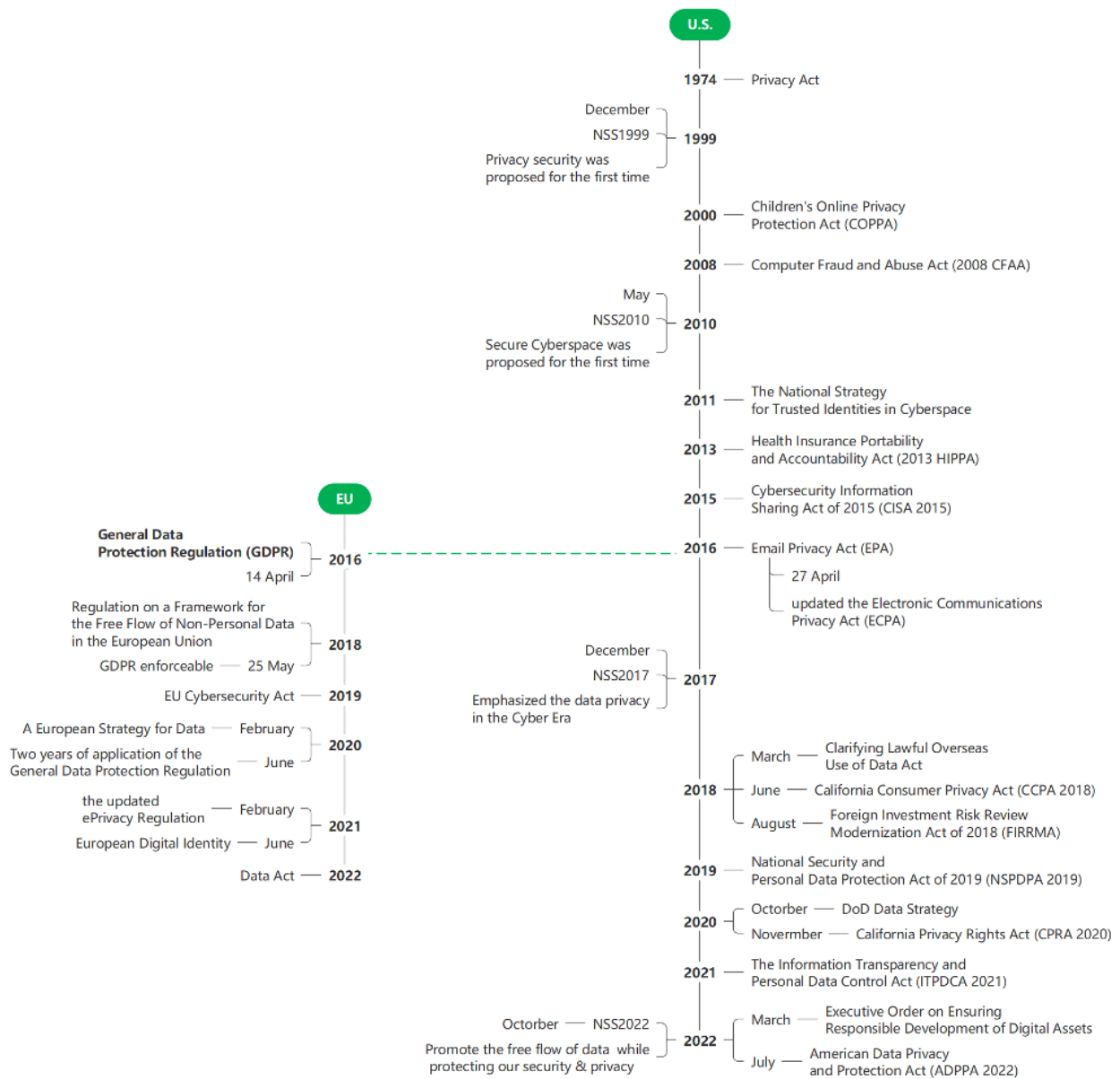
¹⁹For financial institutions, the GDPR not only regulates the handling of personal data within the EU but also affects any global financial transactions involving EU citizens' data.

any entity handling this data must comply with its provisions to avoid legal repercussions. The law outlines a clear framework for proper data management, specifying the obligations of business operators to ensure robust privacy and data protection standards. This regulation is critical for maintaining data integrity and security within Japan's digital economy.

- **India - Personal Data Protection Bill (PDPB):** In December 2019, India introduced the PDPB, setting a precedent for data privacy legislation in South Asia. This law aims to modernize India's legal framework for data privacy, establish cross-border data transfer standards, define data processors' responsibilities, and remedy unauthorized or harmful data processing.

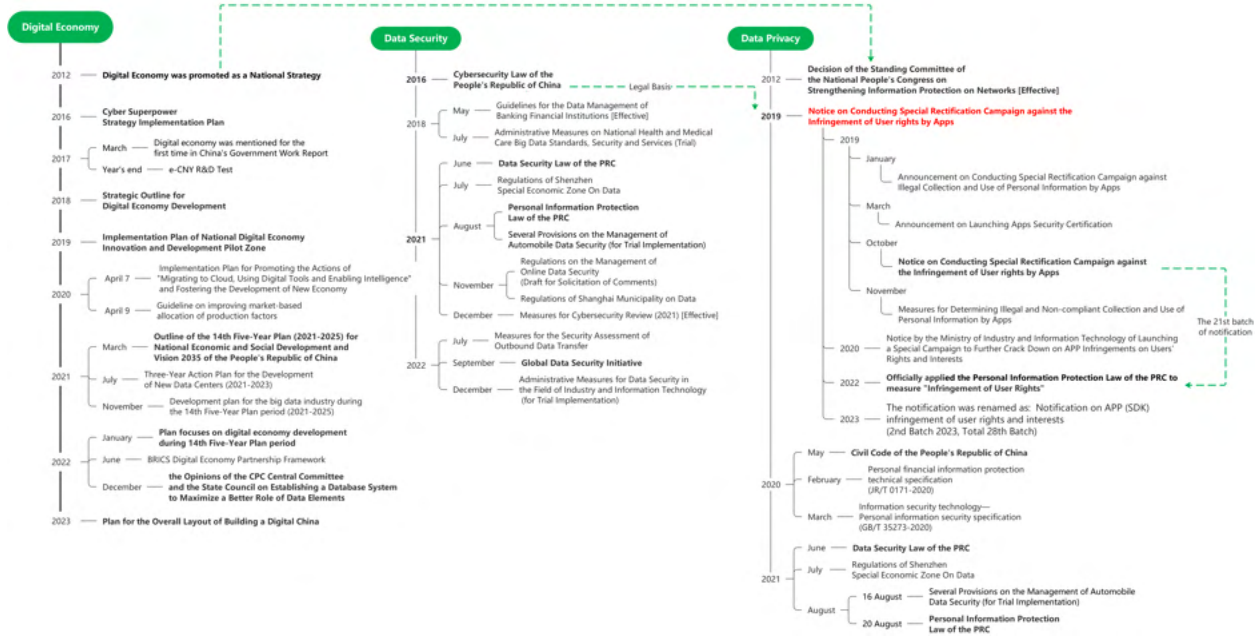
B.2 Timelines of Data Privacy Regulations in EU and US

Figure 1: Timeline of Data Privacy Regulations in the EU and US.



B.3 Timeline of Development in Digital Economy and Data Privacy Regulations in China.

Figure 2: Timeline of Data Privacy Regulations in China.



C Examples of Penalties

1. APP forcefully, frequently, and excessively requests permissions.

Subject of Punishment: Shadowy Heroes Dungeon Survival, Forest Fire and Ice Man, etc.

2. Collecting and using personal information beyond the necessary scope.

Subject of Punishment: 360 Mobile Security, Lily Marriage, Express 100, etc.

3. Illegally collecting and using personal information.

Subject of Punishment: Happy Life, Car Headlines, Xunyou Mobile Game Accelerator, Fun Life, etc.

4. Illegally utilizing personal information for automated decision-making.

Subject of Punishment: Adview Advertising SDK, etc.

5. Deceiving, misleading, and coercing users.

Subject of Punishment: Play More, Draw a Yarn Rescue, Save Little Brothers, etc.

6. Deceiving and misleading users into using products or services.

Subject of Punishment: Play More, Draw a Yarn Rescue, Save Little Brothers, etc.

7. Deceiving and misleading users into downloading the APP.

Subject of Punishment: Super Cleaning King, Love Diary, etc.

8. Inadequate disclosure of APP information on application distribution platforms.

Subject of Punishment: Tom Cat Run, Fun Shopping Life, etc.

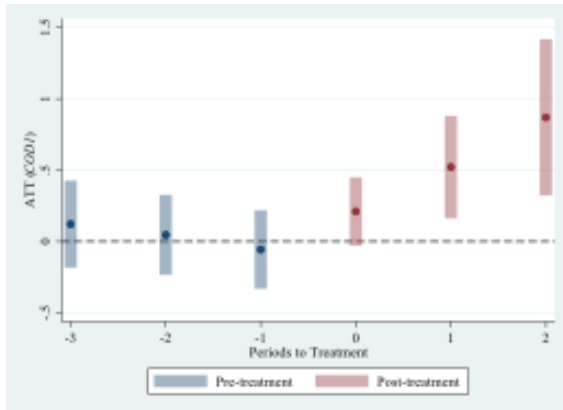
9. Forcing users to use targeted push functions.

Subject of Punishment: Mei Guo, SimCity: I am the Mayor, etc.

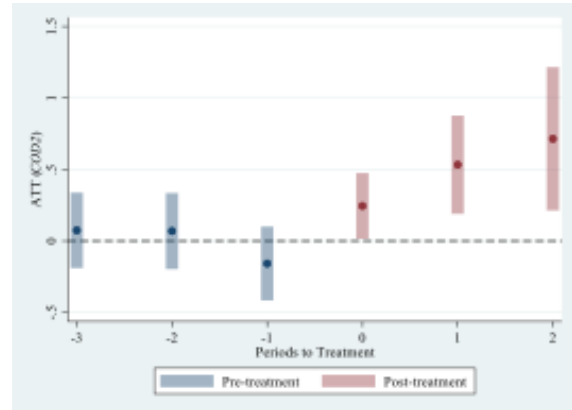
10. Pop-up message harassment of users.

Subject of Punishment: Oxygen Voice, Dou Dou Free Novels, etc.

Figure 3: Dynamic Coefficients of Cost of Debt from CSDID



(a) COD1



(b) COD2

Table 1: Distribution of Corporate Data misconduct Events by Year and Industry

Industry	2019	2020	2021	2022	2023	Total
Information, Software and IT Services	1	13	31	8	13	66
Manufacturing	0	6	10	2	2	20
Culture, Sports, and Entertainment	0	3	6	2	1	12
Wholesale and Retail Trade	0	2	7	1	1	11
Financial Industry	0	1	5	2	2	10
Transportation	0	2	3	0	0	5
Education	0	0	1	2	1	4
Business Services	0	0	1	0	0	1
Real Estate	0	1	0	0	0	1
Scientific Research	0	0	0	1	0	1
Total	1	28	64	18	20	131

Notes: The table presents the distribution of 131 corporate data misconduct events against 95 distinct firms over the period 2019 to 2023 by year and industry.

Table 2: Summary Statistics

The table shows summary statistics for a sample of 106 firm-year observations that experienced misconduct (84 distinct firms) and the remaining 19976 firm-year observations (4,799 distinct firms) that did *not* experience misconduct from 2019 to 2023. All variables are measured at the beginning of the year in which the data-misconduct event occurred. The Appendix provides detailed descriptions of the construction of the variables. ***, **, and * denote that tests of mean (median) differences in firm and industry characteristics between misconduct and non-misconduct firms are significant at the 1 %, 5 %, and 10 % levels, respectively.

	Firm-years for misconduct (N = 106): A		Firm-years for non-misconduct (N = 19,976): B		Test of difference (A – B)	
	Mean	Median	Mean	Median	Mean	Median
Total assets	23.180	23.018	22.388	22.127	0.792***	0.891***
Firm age	2.964	2.996	2.971	2.996	-0.007	0.000
Asset tangibility	0.098	0.067	0.188	0.157	-0.091***	-0.090***
Leverage	0.426	0.414	0.428	0.415	-0.001	-0.001
State-owned enterprise	0.255	0.000	0.287	0.000	-0.032	0.000
Institutional block ownership	0.414	0.382	0.429	0.433	-0.015	-0.051
Log(directors number)	2.048	2.079	2.105	2.197	-0.056***	-0.118
Independent directors (%)	0.393	0.375	0.379	0.364	0.014***	0.011
Stock return volatility	0.028	0.027	0.033	0.029	-0.005**	-0.002*
Violation history	0.896	1.000	0.696	1.000	0.200***	0.000
CSR performance	0.651	1.000	0.886	1.000	-0.235***	0.000
High ESG rating	0.434	0.000	0.393	0.000	0.041	0.000
Industry's Herfindahl index	0.116	0.074	0.081	0.055	0.035***	0.019***
Data-driven industry	0.104	0.000	0.015	0.000	0.089***	0.000***

Table 3: Probit Regression Estimates

The table presents estimates of probit regressions in which the dependent variable is an indicator that takes the value one if a firm experiences data misconduct in a given year and zero otherwise. All explanatory variables are measured one year before the data misconduct, so the sample consists of all firm-year observations over the period 2018 to 2022 for explanatory variables, and 2019 to 2023 for the explained variable. The appendix provides detailed descriptions of the construction of the variables. t-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

	Misconduct				
	(1)	(2)	(3)	(4)	(5)
Violation History		0.333*** (2.98)			
CSR performance			-0.511*** (-3.29)		
High ESG rating			-0.234*** (-2.68)		
Industry's Herfindahl index				1.404*** (4.44)	
I_{Data}					0.698*** (3.93)
Total assets	0.321*** (7.07)	0.309*** (6.80)	0.266*** (5.47)	0.248*** (6.28)	0.255*** (6.24)
Firm age	0.023 (0.15)	-0.032 (-0.20)	-0.044 (-0.26)	-0.089 (-0.64)	-0.063 (-0.44)
Asset tangibility	-1.003*** (-2.61)	-1.033*** (-2.60)	-1.044*** (-2.63)	-2.072*** (-5.28)	-1.751*** (-4.41)
Leverage	-0.489* (-1.81)	-0.518* (-1.89)	-0.421 (-1.53)	-0.825*** (-2.91)	-0.793*** (-2.63)
State-owned enterprise	-0.145 (-1.11)	-0.138 (-1.08)	-0.157 (-1.12)	-0.104 (-0.87)	-0.075 (-0.62)
Institutional block ownership	-0.323 (-1.44)	-0.216 (-0.97)	-0.458* (-1.90)	-0.470** (-2.29)	-0.455** (-2.19)
Log(directors number)	-0.871*** (-3.07)	-0.879*** (-3.10)	-0.970*** (-3.48)	-0.729*** (-2.58)	-0.726** (-2.53)
Independent directors (%)	-0.368 (-0.35)	-0.402 (-0.38)	-0.422 (-0.39)	-0.235 (-0.24)	0.040 (0.04)
Stock return volatility	-3.724 (-1.06)	-2.543 (-0.76)	-14.653*** (-2.75)	-3.970 (-1.40)	-3.676 (-1.32)
i Year fixed effects	Y	Y	Y	Y	Y
Industry fixed effects	Y	Y	Y	N	N
Observations	18,790	18,789	17,535	21,041	20,358
Pseudo R ²	0.263	0.270	0.282	0.151	0.149

Table 4: Univariate and Multivariate Analysis of CARs

This table presents the mean and median cumulative abnormal returns (CARs) for firms around the data misconduct event dates (Panel A), and estimates of ordinary least squares (OLS) regressions (Panel B). The sample contains 122 data misconduct events (91 distinct firms) from 2019 to 2023. The abnormal stock returns are calculated using the market-adjusted and market models, respectively. The market model parameters are estimated using 255 trading days of return data beginning 300 days before and ending 46 days before the data misconduct events dates, using the equal-weighted return as a proxy for the market return. In Panel A, the numbers in parentheses are t-values for t-tests and z-values for Wilcoxon signed-rank tests that the mean CAR and the median CAR are equal to zero, respectively. In Panel B, the dependent variable is the CAR within the (-1, 1) window based on the market model, z-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the industry level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A. Univariate Analysis of CARs				
CARs (%)	Market-adjusted (122 obs)		Market model (122 obs)	
	Mean	Median	Mean	Median
CAR (-1, 1)	-1.19*** (-3.33)	-1.39*** (-3.63)	-1.11*** (-2.82)	-0.96*** (-3.14)
CAR (-2, 2)	-1.25*** (-2.66)	-1.74*** (-3.34)	-1.16** (-2.16)	-1.45*** (-2.88)
CAR (-5, 5)	-2.22*** (-3.50)	-2.53*** (-3.44)	-1.80** (-2.39)	-1.25** (-2.20)
Panel B. OLS Regressions of CARs				
	(1)	(2)	(3)	(4)
non-IPHONE		-1.909*** (-11.28)		
APP search index		-0.474 (-1.46)		
Industry Herfindahl			4.630** (2.76)	
I_{Data}				-1.943** (-2.58)
Total assets	-0.267 (-0.55)	0.085 (0.18)	-0.220 (-0.51)	-0.133 (-0.38)
Firm age	0.332 (0.22)	-1.427 (-0.75)	-0.259 (-0.21)	-0.191 (-0.15)
Asset tangibility	4.127 (1.36)	-2.077 (-0.94)	2.790 (1.38)	4.254*** (3.90)
Leverage	2.687 (0.57)	1.746 (0.41)	2.394 (0.82)	1.895 (0.57)
SOE	1.136 (1.08)	2.749*** (7.65)	0.801 (0.95)	1.376 (1.79)
Institutional block ownership	-5.429** (-2.99)	-6.647** (-2.99)	-5.597*** (-4.46)	-5.800** (-3.38)
Log(directors number)	0.033 (0.01)	0.197 (0.07)	-0.125 (-0.05)	-0.250 (-0.13)
Independent directors (%)	-3.078 (-0.27)	-6.313 (-0.65)	-1.438 (-0.15)	-3.238 (-0.37)
Return volatility	-59.891 (-0.58)	-64.946 (-0.57)	-80.790 (-1.47)	-58.749 (-0.70)
Year FE	Y	Y	Y	Y
Industry FE	Y	Y	N	N
Observations	108	95	108	106
R ²	0.146	0.240	0.156	0.151

Table 5: Cumulative Abnormal Returns (CARs) for Industry Competitors

This table presents the mean and median cumulative abnormal returns (CARs) for industry peer firms around the data misconduct events dates (Panel A) and estimates of ordinary least squares (OLS) regressions in which the dependent variable is the CAR within the (-1, 1) window based on the market model (Panel B). Industry peer firms are those that share the same industry code as the data misconduct firm. We only keep the first data misconduct event in an industry-year and finally get 5091 observations from 2019 to 2023. The abnormal stock returns are calculated using the market-adjusted and market models, respectively. The market model parameters are estimated using 255 trading days of return data beginning 300 days before and ending 46 days before the event, using the equal-weighted return as a proxy for the market return. In Panel A, the numbers in parentheses are t-values for t-tests and z-values for Wilcoxon signed-rank tests that the mean CAR and the median CAR are equal to zero, respectively. In Panel B, z-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the industry level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A: Univariate Analysis of CARs				
CARs (%)	Market-adjusted model (5091 obs)		Market model (5091 obs)	
	Mean	Median	Mean	Median
CAR (-1, 1)	-0.30*** (-4.82)	-0.79*** (-11.95)	-0.33*** (-4.95)	-0.61*** (-10.49)
CAR (-2, 2)	-0.44*** (-5.21)	-1.19*** (-12.24)	-0.63*** (-7.02)	-1.09*** (-12.30)
CAR (-5, 5)	-0.42*** (-3.50)	-1.13*** (-8.58)	-0.96*** (-7.01)	-1.04*** (-8.87)

Panel B: OLS Regressions of CARs					
	CAR				
	(1)	(2)	(3)	(4)	(5)
Misconducts' Severity		-0.043** (-2.98)			
D_{ILM}			0.402** (2.61)		0.414** (2.48)
Industry's Herfindahl Index				-0.565 (-0.33)	1.843 (1.53)
I_{Data}				-0.495** (-2.36)	1.052* (2.20)
$D_{ILM} \times$ Industry's Herfindahl Index					-4.074*** (-5.51)
$D_{ILM} \times I_{Data}$					-1.961*** (-3.86)
Total Assets	-0.204*** (-6.72)	-0.204*** (-6.39)	-0.208*** (-6.46)	-0.198*** (-5.65)	-0.180*** (-5.45)
Firm Age	0.602*** (6.54)	0.606*** (6.81)	0.582*** (6.80)	0.637*** (3.97)	0.659*** (7.09)
Asset Tangibility	0.786 (0.75)	0.787 (0.69)	0.862 (0.82)	1.371 (1.13)	0.781 (0.73)
Leverage	1.686*** (3.89)	1.718*** (4.05)	1.624** (3.24)	1.155* (1.88)	1.339 (1.82)
SOE	-0.023 (-0.14)	-0.028 (-0.16)	0.011 (0.06)	-0.071 (-0.36)	0.055 (0.33)
Institutional Block Ownership	-1.098 (-1.23)	-1.113 (-1.25)	-1.092 (-1.23)	-1.406 (-1.50)	-1.099 (-1.38)
Log(Directors Number)	-0.503* (-2.15)	-0.507* (-2.16)	-0.523* (-2.29)	-0.818** (-2.98)	-0.931** (-2.89)
Independent Directors (%)	-0.559 (-0.48)	-0.614 (-0.51)	-0.516 (-0.45)	-1.333 (-1.16)	-1.480 (-1.30)
Stock Return Volatility	-33.376*** (-5.83)	-33.586*** (-5.96)	-33.634*** (-5.83)	-32.839*** (-5.50)	-33.976*** (-5.49)
Year Fixed Effects	Y	Y	Y	Y	Y
Industry Fixed Effects	Y	Y	Y	N	Y
Observations	4715	4699	4715	4559	4559
R ²	0.095	0.096	0.096	0.088	0.102

Table 6: Corporate Data Misconduct and Cost of Debt

Panel A reports descriptive statistics for treated firms (misconduct) and matched controls during 2019–2022. Panel B reports PSM–DID estimates where the dependent variable is the cost of debt (COD). Treated and control firms are matched within industry–year. Standard errors are clustered at the firm level. ***, **, * denote 1%, 5%, 10% significance, respectively.

Panel A: Descriptive Statistics for PSM-Matched Sample						
	Treated (N = 79)		Control (N = 79)		Test of Difference (A–B)	
	Mean	Median	Mean	Median	Mean Diff (p-val)	Median Diff (p-val)
Total assets	23.075	22.935	23.026	22.693	0.050 (0.847)	0.242 (0.426)
Firm age	2.991	2.996	2.976	2.996	0.015 (0.751)	0.000 (0.750)
Asset tangibility	0.120	0.077	0.110	0.085	0.011 (0.547)	-0.008 (0.426)
Leverage	0.459	0.431	0.483	0.504	-0.024 (0.499)	-0.073 (0.265)
SOE	0.304	0.000	0.367	0.000	-0.063 (0.403)	0.000 (0.400)
Block ownership	0.446	0.454	0.489	0.495	-0.043 (0.276)	-0.041 (0.265)
Log(directors number)	2.046	2.079	2.083	2.079	-0.038 (0.257)	0.000 (0.631)
Independent directors (%)	0.395	0.375	0.402	0.400	-0.008 (0.468)	-0.025 (0.749)
Panel B: PSM–DID Estimates of Cost of Debt						
	Dependent Variable: COD					
	(1) COD1	(2) COD2	(3) COD1	(4) COD2		
<i>Treat × Post</i>	0.418*** (2.93)	0.371*** (2.71)	0.356*** (2.78)	0.338*** (2.66)		
Total assets			0.373** (2.04)	0.275* (1.74)		
Firm age			0.326 (0.37)	0.012 (0.01)		
Asset tangibility			-0.573 (-0.47)	-0.651 (-0.66)		
Leverage			2.706*** (4.16)	1.622*** (2.83)		
SOE			-0.274 (-0.94)	-0.173 (-0.58)		
Block ownership			-0.251 (-0.48)	-0.153 (-0.31)		
Log(directors number)			0.047 (0.14)	0.082 (0.31)		
Independent directors (%)			0.013 (0.02)	-0.137 (-0.18)		
Year fixed effects	Y	Y	Y	Y		
Firm fixed effects	Y	Y	Y	Y		
Obs.	952	952	952	952		
R ²	0.068	0.057	0.192	0.116		

Table 7: CSDID Estimation Results

This table reports the CSDID estimation results to address potential bias in multi-period DID models due to heterogeneous treatment effects (Callaway and Sant’Anna, 2021). Following from the study by Denes et al. (2023), the CSDID method is used to solve this estimation problem. The results show the average treatment effect (Overall ATT) of COD1 and COD2 is 0.437 and 0.432, respectively, both significant at the 1% level. The attention variables before the regulation (Pre_avg, Tm1–Tm5) are not significant, while the key attention variables after the regulation (Post_avg, Tp0–Tp2) are significant at the 5% level. Figure 3 further illustrates the trends of each relative year’s ATT estimates and their 95% confidence intervals.

Variable	COD1			COD2		
	Coefficient	Z-value	P-value	Coefficient	Z-value	P-value
Overall ATT	0.437***	2.93	0.003	0.432***	3.15	0.002
Pre_avg	-0.030	-0.29	0.771	-0.075	-0.72	0.474
Post_avg	0.533***	3.21	0.001	0.497***	3.23	0.001
Tm5	-0.202	-0.52	0.604	-0.291	-0.67	0.500
Tm4	-0.056	-0.29	0.772	-0.069	-0.30	0.762
Tm3	0.121	0.78	0.438	0.074	0.55	0.581
Tm2	0.045	0.32	0.752	0.069	0.51	0.611
Tm1	-0.057	-0.40	0.686	-0.158	-1.20	0.231
Tp0	0.209*	1.71	0.087	0.245**	2.09	0.037
Tp1	0.521***	2.84	0.004	0.533***	3.04	0.002
Tp2	0.869***	3.11	0.002	0.714***	2.79	0.005

Table 8: Corporate Data Misconduct and Cost of Debt: Cross-Sectional Tests

In this table, we conduct a series of cross-sectional analyses to provide additional evidence on the impact of data privacy misconduct via apps on firms' debt costs. Specifically, we investigate how this impact varies based on six key financial characteristics: history of misconduct, industry competition, financial constraints, R&D intensity, digital innovation, and big data technology adoption. Violation History is a 0-1 variable, equal to 1 if the firm had a fraud experience in the past 3 years, and 0 otherwise. Financing constraints is measured by KZ index (Kaplan and Zingales, 1997). R&D intensity is measured by R&D expenditure/revenue. Digital Technology Innovation is measured by the number of digital technology patent applications. Big Data Technology is measured by the frequency of big data technology-related terms in the annual report/total word count of the annual report. Grouping is performed based on the 0-1 variable or the sample median of the above continuous variables. The appendix provides detailed descriptions of the construction of the variables. Standard errors are adjusted for clustering at the firm level.

	COD1		COD2	
	(1)	(2)	(3)	(4)
Panel A: Violation History	NO	YES	NO	YES
Treat×Post	-0.253 (-1.03)	0.447*** (3.18)	-0.255 (-0.97)	0.419*** (2.94)
Empirical p-values		0.006		0.010
Observations	253	699	253	699
R ²	0.305	0.219	0.217	0.133
Panel B: Industry Competition	Low	High	Low	High
Treat×Post	0.149 (0.84)	0.511** (2.60)	0.088 (0.52)	0.537*** (2.68)
Empirical p-values		0.090		0.049
Observations	476	476	476	476
R ²	0.150	0.273	0.097	0.194
Panel C: Financing Constraints	Low	High	Low	High
Treat×Post	0.065 (0.36)	0.546*** (2.88)	-0.021 (-0.12)	0.563*** (3.09)
Empirical p-values		0.069		0.033
Observations	472	473	472	473
R ²	0.175	0.228	0.091	0.178
Panel D: R&D Intensity	Low	High	Low	High
Treat×Post	0.454*** (2.86)	0.103 (0.60)	0.475*** (2.99)	0.074 (0.43)
Empirical p-values		0.071		0.047
Observations	436	437	436	437
R ²	0.204	0.225	0.137	0.141
Panel E: Digital Technology Innovation	Low	High	Low	High
Treat×Post	0.699*** (3.81)	0.167 (1.12)	0.670*** (3.81)	0.184 (1.34)
Empirical p-values		0.052		0.080
Observations	386	386	386	386
R ²	0.289	0.164	0.219	0.121
Panel F: Big Data Technology	Low	High	Low	High
Treat×Post	0.736** (2.49)	0.230 (1.32)	0.696** (2.13)	0.262 (1.53)
Empirical p-values		0.043		0.075
Observations	472	472	472	472
R ²	0.180	0.217	0.103	0.131

Note: All regressions include control variables, firm fixed effects, and year fixed effects. “Empirical p-values” test differences in Treat×Post across groups via 1,000 bootstrap iterations. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively. t-statistics in parentheses.

Table 9: Effects of Data Misconduct on Reputation Loss, Operational Performance and Operational Risk-Taking

This table examines the mechanism by which corporate data misconduct affects the cost of debt, including two mechanisms: decreased operational performance due to reputational damage and increased operational risk reflected in more volatile earnings. Firm reputation is calculated using factor analysis based on 12 indicators from different stakeholder perspectives. Operational performance measures include sales growth defined as $(Sales_t - Sales_{t-1}) / Sales_{t-1}$, return on assets (ROA) and return on equity (ROE). Corporate operational risk-taking is measured using σ_{ROA} and σ_{ROE} , while reputation risk is measured using Sales growth. σ_{ROA} is defined as the standard deviation of ROA for the past 5 years (i.e., $t - 4$ to t), σ_{ROE} is defined as the standard deviation of ROE for the past 5 years (i.e., $t - 4$ to t). The Appendix A provides detailed descriptions of the construction of the variables. Standard errors are adjusted for clustering at the firm level.

Panel A: Reputation Loss and Operational Performance								
	Firm Reputation		Sales Growth		ROA		ROE	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
<i>Treat</i> × <i>Post</i>	-1.004***	-0.947***	-0.118*	-0.128**	-0.036**	-0.036**	-0.109***	-0.103***
	(-3.26)	(-3.06)	(-2.29)	(-2.30)	(-3.17)	(-3.09)	(-3.13)	(-3.08)
Total assets		0.094		-0.307***		-0.046***		-0.045
		(0.39)		(-3.67)		(-4.03)		(-1.25)
Firm age		2.708		0.828*		0.032		0.300*
		(1.52)		(1.91)		(0.60)		(1.76)
Asset tangibility		2.666*		0.328		-0.042		-0.016
		(1.86)		(0.86)		(-0.67)		(-0.09)
Leverage		-0.771		-0.471*		0.052**		-0.009
		(-1.04)		(-1.86)		(2.05)		(-0.11)
State-owned enterprise		-0.015		-0.084		-0.009		-0.092
		(-0.04)		(-0.77)		(-0.47)		(-1.25)
Institutional block ownership		1.845*		-0.165		0.109**		0.168*
		(1.71)		(-0.54)		(3.00)		(1.82)
Log(directors number)		-0.677		-0.188		-0.028		-0.038
		(-1.01)		(-0.96)		(-0.94)		(-0.57)
Independent directors (%)		-0.262		0.227		0.063		0.192
		(-0.14)		(0.49)		(0.79)		(1.04)
Year fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Firm fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Observations	799	799	1045	1045	1044	1044	1044	1044
R ²	0.083	0.104	0.050	0.125	0.082	0.127	0.077	0.093

Panel B: Operational Risk-Taking

	σ_{ROA}		σ_{ROE}	
	(1)	(2)	(3)	(4)
<i>Treat</i> × <i>Post</i>	0.013** (2.48)	0.035** (2.45)	0.010* (2.23)	0.025** (2.26)
Total assets		-0.018*** (-4.05)		-0.062*** (-4.60)
Firm age		0.005 (0.16)		-0.020 (-0.24)
Asset tangibility		-0.080*** (-3.84)		-0.196*** (-3.24)
Leverage		0.064*** (4.20)		0.258*** (6.34)
State-owned enterprise		-0.001 (-0.17)		0.016 (0.93)
Institutional block ownership		-0.041** (-2.18)		-0.041 (-0.93)
Log(directors number)		-0.004 (-0.34)		-0.010 (-0.40)
Independent directors (%)		-0.029 (-0.88)		-0.106 (-1.39)
Year fixed effects	Y	Y	Y	Y
Firm fixed effects	Y	Y	Y	Y
Observations	1046	1046	1046	1046
R ²	0.134	0.145	0.231	0.303