Geng, S., Hao, S.Y., Li, W.H., & Zhang, X. (2024). The impacts of app violation notification on companies' market value. In Li, E.Y. *et al.* (Eds.) *Proceedings of The International Conference on Electronic Business, Volume 23* (pp. 458-468). ICEB'24, *Zhuhai, China, October 24-28,* 2024

The Impacts of App Violation Notification on Companies' Market Value

Shuo Geng [1]
Shiyun Hao [2]
Weihua Li [3]
Xiong Zhang [4,*]

*Corresponding author
[1] Beijing Jiaotong University, Beijing, China, 23120617@bjtu.edu.cn
[2] Beijing Jiaotong University, Beijing, China, 21120609@bjtu.edu.cn
[3] Beijing Daxing No.1 Vocational School, Beijing, China, liweihua_011@163.com
[4] Beijing Jiaotong University, Beijing, China, xiongzhang@bjtu.edu.cn

ABSTRACT

With rapid development of Information Technology (IT), mobile devices and Apps are commonly adopted. Some Apps have been notified for violating the rights and interests of users, which inevitably causing negative impacts on companies. In this study, we quantify such impact in China through the event study approach, and the results show that App violation has brought significant negative impacts (-0.15%) to companies. The violations of collecting and using of personal information have larger negative impact on companies among different violations. Meanwhile, the study also finds that after the implementation of the Personal Information Protection Law of the People's Republic of China, such negative impacts of App violation problems on companies increases. Research contributes to information management yield. These findings can help companies and governments during their decision making.

Keywords: App violation, event study, company market value.

INTRODUCTION

As technology continues to evolve, mobile devices and mobile applications (Apps) are being adopted worldwide at an unprecedented rate. It has become common for users to own multiple mobile devices. The number of Apps has also grown significantly. Their use has become an integral part of our daily work and life. The daily active user (DAU) of mobile devices had exceeded 1.1 billion in 2021, and active hours of Apps in a single day had reached 5.26 hours, up 2.7% year-on-year. As of December 2021, the number of Apps in China's App shops was 2.52 million, and annual distribution volume of Apps had exceeded 2.1 trillion times, with a 31% increase in distribution scale (Avery.com, 2022). In this context, violation problems related to Apps inevitably pose security and privacy risks to users and affect associated companies. For example, JD Finance failed to apply for privacy permissions in accordance with its privacy statement. It was notified for alleged over-scope collection of users' private information. This caused hot debates among netizens and brought large negative impacts to JD.com.

App Violation Problems refer to Apps violating laws and regulations by collecting, using, leaking, tampering with or destroying users' personal information without users' consent or beyond the scope of users' authorisation, as well as using users' personal information for commercial promotion, financial fraud and other unlawful behaviours (Cyberspace Administration of China, 2019). In terms of personal information, the violation problems include private or excessive collection of personal information, using and sharing it privately with third parties. In terms of App permissions, some Apps have behaviours such as mandatory, frequent and excessive requests for permissions, or cannot be used without such permissions. In terms of App usage, some Apps force people to use targeted push functions, use personal information for automated decision-making, or are difficult in account cancellation. Unlike data security incidents and data breaches, app violation incidents usually focus on the improper collection, use or processing of personal information by applications. They emphasize the interaction between enterprises and users. Compared with uncertain data leaks, app violation incidents can be prevented and punished. At the same time, the government's privacy policies and laws and regulations are more binding. Therefore, China's Ministry of Industry and Information Technology (MIIT) has organised third-party testing agencies to inspect mobile phone applications and focus on App/SDK violations.

Once violation problems exist in mobile applications, users would have concerns about personal information, leading to users' dissatisfaction, disappointment or even loss, which will have a negative impact on the production and operation in companies. Nowadays, governments have started to investigate such violation according to laws, and would notify or punish associated companies if necessary. Such notification and severe punishment have significant impacts on companies. Existing research has analyzed the impact of different IT operational failure events on wealth effects and whether a company's stock returns respond to announcements of data theft. (Goldstein et al., 2011; Hinz et al., 2014), At the same time, the literature on APP permissions analyzes users' privacy concerns and trade-offs when accepting application permission requests during the download phase. (Verena et al., 2017; Gu et al., 2016). However, detailed investigation on such impacts is lacking in current research, which is

mainly conducted from two aspects: users (Liu et al., 2018; Wang et al., 2020) and companies (Wui et al., 2022; Zhen et al., 2020). Existing literature focuses on the influencing factors and psychological changes of users' decision-making on personal information disclosure, etc. (Liu & Sun, 2021); companies' optional strategies to reduce concerns of users and impacts of investment in information security on companies, etc. (Zhen., 2020). However, the impacts of mobile Apps on companies due to violation problems, especially in China context, has not been well measured and discussed. This study will quantify and analyse the impact of App violation on associated companies. In this study, we collect notifications related to App violation problems in China and analyse its impact on market value of companies through event study method. We found that App violation problems have negative impact (-0.15%) on companies' market value, and different types of violation problems have different degrees of impacts. Violation of collecting and using of personal information has a larger negative impact among all types. In addition, since app violations are more affected by factors such as laws, the impact will be even greater after the country promulgates relevant laws. the notification of App violations caused larger losses to companies after the enactment and implementation of Personal Information Protection Law.

LITERATURE REVIEW

After combing through existing literature, The literature primarily focuses on data security incidents, such as hacking of consumer electronics companies, showing that announcements of data breaches lead to stock price declines for both affected and similar companies (Oliver et al., 2014). In IT operational risk, studies on U.S. financial service firms over a 25-year period reveal that function-related failures have a greater negative impact on firm value than data-related incidents (Goldstein et al., 2011). While data breaches negatively affect market value, taking countermeasures can have positive effects, with related announcements increasing short-term market value by an average of 0.63% (Indranil et al., 2013). Regarding app privacy, users disclose personal information based on a cost-benefit analysis, reflecting the privacy calculus in mobile app contexts (Wottrich et al., 2017), with factors such as perceived permission sensitivity and app popularity influencing user decisions (Gu et al., 2016).There are also literature studies that show the impact of data security breaches on corporate responses and provide countermeasures and suggestions(Zhang et al., 2015,2020,2021; Zhu et al.2020). (Dong et al.,2024) built a knowledge graph about data security vulnerabilities. We found that most of studies analysed from both user and enterprise perspectives. They study the influence of both parties' perception and attitude during make decision in the face of information security problems. From the user's perspective, the researchers expect to find the influencing factors affecting users' personal information disclosure decisions. The studies help to targeted alleviate the phenomenon of user's worry and increase users' willingness to use Apps. (Xie et al., 2013) proposed to involve users in the process of corporate's information security management. They integrate information security awareness of use into business processes to construct a multiple mediator model. The results proved that user participation influences the effectiveness of information security management, with a significant positive effect. However, different attitudes towards mobile Apps still influence users' final decisions on personal information disclosure. Existing literature on behavioural security suggests that one of the main influences on users' perception of security is their perceived privacy concerns(Wu et al., 2020). Some scholars have studied users' disclosure decisions based on the communicative privacy management theory (CPM) framework in the context of the existence of data privacy paradox (Liu & Sun, 2021) divided users' decision-making process into three stages based on CPM framework: cognitive factors, cognitive trade-offs and disclosure decisions. They study the role of two different attitudes, trust and worry, on users' willingness to disclose personal information by building a disclosure decision model. The study found that cognitive factors of user disclosure framework have a significant impact on cognitive trade-offs, which in turn generate two different attitudes towards disclosure. (Balapour et al., 2020) found that perception of user privacy risk has a negative impact on mobile application security.

Users' perceptions influence their decision to disclose privacy to some extent. But the pursuit of App personalisation inevitably comes at the cost of personal information disclosure. The mobile Apps' rich functionality has led many users to engage in exchange behaviours between functionality and privacy. Facing this phenomenon that users are unwilling to disclose information because they perceive their personal privacy information is uncontrollable, (Liu et al., 2018) propose a new privacy protection method based on theory of fairness and theory of planned behaviour. The method is expected to be used to improve user experience of m-commerce services. In addition, (Tripathi & Mukhopadhyay, 2022) found a strong negative relationship between privacy violations and users' self-disclosure willingness. This poses new requirements for information security governance in companies. There are more studies from the user's perspective. The above studies aim to help manager better understand users' attitudes and behaviours towards security problems during use of mobile Apps through empirical research or modelling.

Relatively a few studies have addressed the relationship between personal information protection and companies from a corporate perspective. (Zhen et al., 2020) demonstrated the potential relationship between information security governance and companies' performance by conducting a survey on information security management carried out by Chinese companies. The study shows that there is a significant positive moderating effect of information security governance on companies' performance. Information security integration capability mediates positive moderation between them. When companies have security problems, such as privacy breaches, cybersecurity issues, etc., the impact on performance is enormous (Wu et al., 2020). Strong user privacy concerns pose a serious challenge to company social responsibility. In order to use valuable data of consumer and transactional on mobile Apps appropriately, companies should adopt ethical decisions and strategies that reduce privacy risk concerns of users. (Libaque-Sáenz et al., 2021) tested the effects of different intervention strategies, fair information practices and data collection methods, on privacy-related decision. The results show that both intervention

strategies have a significant effect on perception of data control and risk, which in turn affects behavioural intention. However, there is a shortcoming in exploring impact of mobile App violation problems on companies' market value using China as the research scenario. This paper conducts this research by using the event study methodology to fill this gap. The study aims to quantify the impact of mobile application violations on companies.

RESEARCH HYPOTHESES

Announcements about a company provide useful information to the market. They generally have an impact on its stock price and market value.The market generally reacts positively when the disclosed announcements contain positive factors. Similarly, the market generally reacts negatively when newly disclosed announcements contain negative factors, such as losses and bankruptcies. For example, self-disclosed privacy breaches by firms have a significant negative impact on companies' market value and cause economic losses (Tripathi & Mukhopadhyay, 2022). We can gain that psychological and behavioural characteristics of investor, such as overconfidence, risk appetite, herd effect, etc., will affect investment decisions and development of financial market from behavioural financial theory. Investors will fell disappointed and crisis when companies being notified for App Violation. For this reason we propose following hypothesis:

H1: Notification of mobile Apps that infringe on users' rights and interests negatively affects companies' market value.

App infringement on users' rights and interests refers to Apps violate relevant laws and regulations. For instance, Apps may collect users' personal information privately or excessively without users' consent or without informing the purpose, manner and scope of collecting personal information. Apps may violate the safety and security obligations of network operators, resulting in the leakage, destruction, or loss of users' personal information (MIIT, 2020). In reality, App violations of users' rights and interests include: forcing users to use targeted push functions, privately collecting personal information, privately sharing to third parties, frequently applying for permissions and so on. According to the “Scope of Personal Information Necessary for Common Types of Mobile Internet applications” issued by the State Internet Information Office, collection of users' personal information account for 86.6% of App violation problems (General Office of the MIIT, 2021). In the process of collecting personal information, Apps did not comply with the requirement of "disclosing the rules of collection and use, indicating the purpose, manner and scope of collection and use, and obtaining the consent of collected person". The lack of users’ consent was one of the most common violations. The collection and use of personal information by Apps in violation of laws is an infringement of users' privacy.The illegal collection and use of personal information brings more harm to companies compared to other violation problems. For example, the sale of users’ personal information to third parties without their consent may result in abuse for fraud, harassment, etc., causing financial loss and emotional distress. In addition,we believe that different types of violations are mutually inclusive. For example, in the process of using personal information in violation of regulations, it is very likely that the illegal collection of personal information has also been carried out.Therefore, we propose following hypothesis:

H2: Violations of collecting and using personal information have a larger negative impact on companies among all types.

The regulatory environment in China has improved significantly with the formation of legal framework for protection of personal information. The State has accelerated the process of building relevant laws and regulations. Regulators have adopted the strategy of "improving while governing", improving relevant regulations and standards in course of the specialised governance of App violations. Personal Information Protection Law of the People's Republic of China (PIPLPPC) was enacted and came into force on 1 November 2021. The law provides guidance to handle, use, store, and transmit personal information in order to protect the safety and lawful use of personal information (China National People's Congress, 2021). This is a milestone in protection of personal information rights and interests in China. The enactment and implementation of Personal Information Protection Law (PIPL) has greatly increased sensitivity of whole society to the use of personal information. Thus, we speculate that the negative impact on companies due to App violation problems will be even higher after enactment and implementation of the law. Meanwhile, enterprises' investment in information security governance increases over time. Several studies have shown a positive relationship between a company's investment in information security and its performance (Zhen et al., 2020). Companies need more resources to secure their information as cyber attacks and threats increase. The MIIT released Three-Year Action Plan for High-Quality Development of Cybersecurity Industry (2021-2023) in 2021. The plan proposes that by 2023, the proportion of network security investment in key industries, such as telecommunications, to information technology investment will reach 10% (MIIT, 2021). Under the background of improved policies, strict regulation and increased investment by companies, users' knowledge of personal privacy information is also increasing, and the degree of importance is also gradually increasing. So that the impact of App violation problems to companies will become larger. Therefore, we propose the following hypothesis:

H3(a): The notifications of App violation problems have a larger negative impact on companies over time.
H3(b): The notifications of App violation problems have a larger negative impact on companies after the implementation of Personal Information Protection Law.

DATA

This study collects data about App violation published in news, characteristics of such violation and listed companies to build a unique dataset .

Collection and Screening of App/SDK Violation

First, we collect data on mobile internet applications (Apps) and third-party software development kits (SDKs) which infringing on users' rights and interests based on announcements published on official websites. The MIIT organised a special rectification for App infringement, and notified App/SDKs for such infringement. For example, the Tentacle Live software downloaded from official website of Hangzhou Kaixun Technology Co. was notified for such violations on 19 December 2019. This App (version 5.6.0) asked users for excessive permissions, collected personal information privately and shared it with third parties, causing serious damages to users. Battle of the Balls (version 12.1.2), downloaded from the Xiaomi App Store, was notified for asking for excessive permissions and privately collecting personal information. This App was developed by Giant Interactive Group Inc. Each event in the dataset includes App name, company name, version, App source, violation problem, and notification time. The company name is the company associated with the App; App source is the platform on which the App is downloaded, including official website, Application Treasure, Wandoujia, AppGallery and so on; The violation problem is non-compliance behavior that exist in App, including private collection, use and sharing of user data; The notification time is time when the press release was issued. In the end, we collected in total 4032 nofitication of App violation problems, with 2203 associated companies.

This research aims to focus on the impact of non-compliant Apps' notification on the firms, so we only choose listed companies. We first obtain all listed companiess in the Choice database for A-share, Hong Kong and US stocks. Then, we use Levenshtein Distance algorithm to match the companies' name in dataset with the company name and stock abbreviation of listed companies. We manually identify, confirm and screen for the matching results to improve accuracy. Finally, we get 131 events in three stock markets. In this paper, we only consider 60 notifications of App violation problem that occurred in A-share market.

A company may have multiple Apps with violations on the same date. For this, we keep only one event to remove confounding effects. In additional, we need to ensure that company does not have recurring App violation notification events throughout event window (estimation window, time interval and event window). For events that are repeated two or more times, we keep only the first occurrence. We exclude events of dislisted companies. Events like M&A, restructuring, etc. in event window is are also removed.

The stock data for associated companies was obtained from Choice Financial database. We exclude companies with missing stock data. Finally, the dataset contains 47 valid data samples and involves 38 companies from different industries. The notification time of events is between 2020 and 2023. There were 14 App violation events in 2020 and 2021, 8 App violation events in 2022, 9 App violation events in 2023, and 1 App violation events in 2024

Type of App/SDK Violation

The reasons for App violation problems are various and inconsistently described in raw data. We standardised the violation problems into five categories after a detailed analysis, as shown in Table 1.

Table 1: Classification of App/SDK Violation Type

Violated Type	Violation Problem
App forced, frequent, and excessive permission requests	Excessive Permission Requests
	Do not allow to use without permission
	App forced, frequent, excessive permission requests
	Unauthorised access to address book and geolocation
Violation of using personal information	Private sharing personal information with third parties
	Violation of using personal information
Violation of collecting personal information	Collection of personal information beyond the scope
	Private collection of personal information
	Violation of collecting personal information
	Violation of collecting personal information by SDK (device MAC address)
	Forced collection of non-essential personal information
	Violation of collecting personal information, etc.
	Collecting personal information beyond the scope.
Deceive, mislead and force users	Forcing users to use targeted push functions
	Deceive, mislead and force users

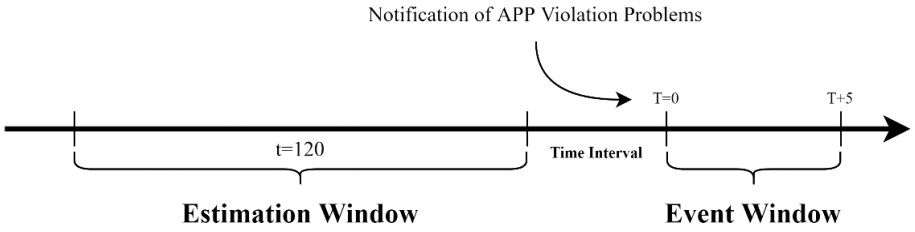
	Inadequate disclosure and notification of collected personal information
Difficulty in cancelling accounts	Difficulty in cancelling accounts

Source: This study

Among five types of events, there are 20 samples with violations of App forced, frequent, and excessive permission requests, 32samples with violations of unauthorised collection of personal information, 9 samples with violations of deceive, mislead and force user behaviours, 8 samples with violations of unauthorised use of personal information, and 2 samples with violations of difficulty in cancelling accounts. One sample may have multiple violation problems.

METHOD

This paper use the event study method to analyze data and test the proposed hypotheses. The time of App violation notification is the event day, refered to as day 0. Event window usually consists of three parts: event window, estimation window and time interval. The event window is a time period during which stock prices fluctuate after an event occurs. The length of event window can be set autonomously for research purposes. During this time period, the impact of events on companys' stock value is usually measured by abnormal returns. Abnormal return is the difference between actual stock return and average market return. This study considers the short-term impact of App violation events. We set the event window as five effective trading days from the event day. (i.e., (0, 1), (0, 2)...(0, 5)). The estimation window is set to 120 trading days based on existing literature. We also set a time interval (5 trading days) in order to avoid the impact of early leakage of event-related information on the company's cumulative returns. Figure 1 shows structure of event window.



Source: This study
Figure 1: Event Window Distribution

This study uses market model to estimate normal return. The CSI 300 index is chosen as market index. Abnormal returns are calculated as follows:

$$AR_{it}=R_{it}-NR_{it} \tag{1}$$

where R_{it} is real return of firm i at time t. NR_{it} is normal return of firm i at time t (calculated from expected return model). AR_{it} is the abnormal return of firm i at time t. The firm's real return, R_{it}, is the ratio of the difference between closing price of stock on event day (If the event day is non-trading day, we choose the stock price on later trading day) and closing price of stock on previous trading day, to closing price of stock on previous trading day. The relationship between predicted normal stock return NR_{it} and market return R_{mt} is as follows:

$$NR_{it}=\beta iR_{mt}+\varepsilon_{it}+\alpha i \tag{2}$$

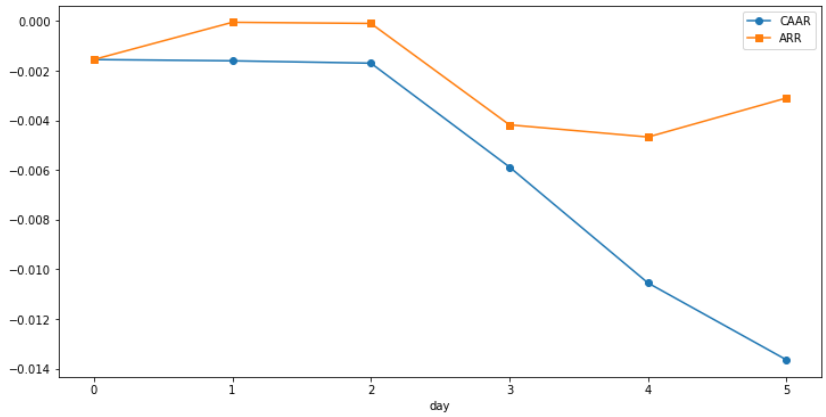
where m represents the market. α, β are OLS estimation parameters. ε_{it} is disturbance term.

After obtaining abnormal return for a single day, cumulative abnormal returns can be obtained by summing abnormal return for a time window. Then, we average all events to obtain average abnormal return (AAR) and cumulative average abnormal return (CAAR), respectively.

RESULT

In this section we analyse and interpret the results.

Abnormal Return (Market Model)



Source: This study
Figure 2: AAR and CAAR During Event Window

Figure 2 shows average abnormal returns and cumulative average abnormal returns in different windows. We find that in (0, 5) the average abnormal return is negative at all times. Overall, cumulative average abnormal return values are negative in different event windows. We validated the results using standard two-tailed t test and Z test, as shown in Table 2. The results are significantly negative at 0.10 and 0.05 levels for day 0 and day 1, respectively.

Table 2: Average Abnormal Return in Event Window

	AAR	*t test*	*Z test*
day 0	-0.001550	-0.414912	-0.414912
day 1	-0.000051	-0.012219	-0.012219
day 2	-0.000096	-0.022004	-0.022004
day 3	-0.004180	**-1.249867***	**-1.249867***
day 4	-0.004670	**-1.305809***	**-1.305809***
day 5	-0.003098	-0.924095	-0.924095

Source: This study
Note: ***, **, * denote significance levels of 1%, 5% and 10% respectively.

Similarly, results of t test and Z test for CAAR are shown in Table 3. We can find that CAAR in window (0, 1) is significantly negative at 0.05 level.

Table 3: Cumulative Average Abnormal Return in Event Window

Event Window	*CAAR*	*t test*	*Z test*
(0, 0)	-0.001550	-0.414912	-0.414912
(0, 1)	-0.001602	-0.25404	-0.25404
(0, 2)	-0.001697	-0.226443	-0.226443
(0, 3)	-0.005878	-0.646024	-0.646024
(0, 4)	-0.010548	-0.959595	-0.959595
(0, 5)	-0.013646	**-1.328676***	**-1.328676***

Source: This study
Note: ***, **, * denote significance levels of 1%, 5% and 10% respectively.

The results support H1. When a company was notified due to App/SDK violations, such as infringement of users' rights and interests, its market value would react negatively in short term. The extent of stock price loss is approximately 0.15% on day 0. The cumulative average abnormal returns show an overall continuous downward trend during (0, 5) event window. The public or investors will have distrust towards the companies when they are notified to the society because of its App violation problems. This distrust will affect the public's choice, causing damage to the enterprise's reputation, etc., and leading to a decline in companies' market value.

Abnormal Return (Fama-French Three-Factor Model)

We use Fama-French three-factor model to recalculate abnormal returns to assess stability and reliability of the above results. The three-factor model suggests that the excess return of a portfolio (including individual stock) can be explained by three factors: market portfolio (Rm-Rf), market value factor (SMB, Small Minus Big), and book-to-market ratio factor (HML, High Minus Low). As shown in Table 4, the average abnormal returns are negative on day 0 and day 1, and they are statistically

significant. Similarly in Table 5, cumulative average abnormal returns are negative on day 0 and in (0, 1), and they are statistically significant.
These results are qualitatively consistent with those from market model, but overall the degree of impact is relatively lower.

Table 4: Average Abnormal Return in Event Window
(Three-Factor Model)

	AAR	*t test*	*Z test*
day 0	-0.002020	-0.504084	-0.504084
day 1	-0.000667	-0.166875	-0.166875
day 2	-0.000346	-0.078264	-0.078264
day 3	-0.002675	**-0.87307**	**-0.87307**
day 4	-0.001954	-0.514091	-0.514091
day 5	-0.003616	**-1.06108**	**-1.06108**

Source: This study
Note: ***, **, * denote significance levels of 1%, 5% and 10% respectively.

Table 5: Cumulative Average Abnormal Return in Event Window
(Three-Factor Model)

Event Window	*CAAR*	*t test*	*Z test*
(0, 0)	-0.002020	-0.504084	-0.504084
(0, 1)	-0.002687	-0.423199	-0.423199
(0, 2)	-0.003032	-0.406246	-0.406246
(0, 3)	-0.005707	-0.662609	-0.662609
(0, 4)	-0.007661	**-0.707175**	**-0.707175**
(0, 5)	-0.011277	**-1.146519**	**-1.146519**

Source: This study
Note: ***, **, * denote significance levels of 1%, 5% and 10% respectively.

Sub-Sample Analysis
Table 6 shows the impacts of different violation problems on companies' market value.

Table 6: Abnormal Return for Different App/SDK Violation Event Types

App forced, frequent, and excessive permission requests (N=20)	AR0	AR1	AR2	CAR [0,1]	CAR [0,2]
AAR/CAAR	-0.004713	-0.001361	-0.001936	-0.004713	-0.006074
t test	-0.873311	-0.257913	-0.446951	-0.873311	-0.903402
Z test	-0.873311	-0.257913	-0.446951	-0.873311	-0.903402
Violation of collecting personal information (N=32)	AR0	AR1	AR2	CAR [0,1]	CAR [0,2]
AAR/CAAR	-0.010555	-0.007845	0.003657	-0.018400	-0.014743
t test	**-1.93914***	**-1.370317**	0.440967	**-1.93914***	**-2.014622***
Z test	**-1.93914***	**-1.370317**	0.440967	**-1.93914***	**-2.014622***
Violation of using personal information (N=8)	AR0	AR1	AR2	CAR [0,1]	CAR [0,2]
AAR/CAAR	-0.012986	-0.010889	0.006253	-0.012986	-0.023875
t test	-2.077994	-0.697161	**2.935809***	-2.077994	-2.056236
Z test	-2.077994	-0.697161	**2.935809***	-2.077994	-2.056236
Deceive, mislead and force users (N=9)	AR0	AR1	AR2	CAR [0,1]	CAR [0,2]
AAR/CAAR	0.001533	-0.008362	0.007821	-0.006829	0.000992
t test	0.257414	**-2.109186***	1.196378	-0.91599	0.154605
Z test	0.257414	**-2.109186***	1.196378	-0.91599	0.154605
Difficulty in cancelling accounts (N=2)	AR0	AR1	AR2	CAR [0,1]	CAR [0,2]
AAR/CAAR	-0.005525	0.006396	-0.00081	0.000871	0.000061

t test	-0.463249	0.628245	-0.27867	0.498622	0.052786
Z test	-0.463249	0.628245	-0.27867	0.498622	0.052786

Source: This study
Note: ***, **, * denote significance levels of 1%, 5% and 10% respectively.

As shown in Table 6, different App violation problems have different degrees of impacts on companies. Violation of collecting personal information and violation of using personal information have smaller abnormal returns, i.e., notifications of above two type of violation events have a larger impact on companies, the results suppert H2. he average abnormal return of violation of collecting personal information is -1.05% on day 0 and is significant at 0.10 level. It is also significantly negative at 0.10 level on day 1, and the level of loss is almost equal to that on day 0. The abnormal return on day 2 becomes positive. The CAAR in (0,1) is significantly negative at 0.05 level, reaching -1.84%. Violation of using personal information is not significant on day 0 and day 1, but is significantly positive on day 2. The reason for this observation may be the small sample size. Although the result of violation of using personal information is not significant, the damage is more serious than that in the violation of collecting personal information, with a CAAR of -2.39% in (0,2). Overall App's violation of collecting and using of personal information has a larger impact on companies. These two type of violations may cause serious impacts on individuals, such as personal privacy leakage. Privacy leakage leads to personal information being used illegally and being subjected to a lot of harassment, e.g., receiving a lot of advertisements, sales messages, and phone calls. Personal information is illegally provided to the third parties, resulting in financial loss. Companies might lose trust of their users or investors, which is reflected as a decline in stock price in the stock market.

The impacts of other types of App violation problems are not significant on day 0. Events of difficulty in cancelling accounts are not discussed due to small sample size. Events of App forced, frequent, and excessive permission requests are not significant, but AAR is negative on day 0 and day 1, and CAAR is negative in (0, 1) and (0, 2). Events of deceive, mislead and force users is positive on day 0 and significantly negative at the 0.10 level on day 1. These three types of App violation problems also have negative impacts on the production and operation of companies. However, they cause relatively little harm compared to those in the violation of collecting and using personal information, the results confirm H2.

Time
This section analyses impacts of App violation problems on companies in different years.

Table 7: Abnormal Return for Different Years During Event Window

2020 (N=14)	AR0	AR1	AR2	CAR [0,1]	CAR [0,2]
AAR/CAAR	-0.01278	-0.01206	-0.00684	-0.02484	-0.03168
t test	-1.07446	-1.20084	-1.39932	-1.28748	-1.49604
Z test	-1.07446	-1.20084	-1.39932	-1.28748	-1.49604
Negative Percentage	0.7	0.6	0.6	0.7	0.7
2021 (N=14)	AR0	AR1	AR2	CAR [0,1]	CAR [0,2]
AAR/CAAR	-0.00902	-0.00293	0.010138	-0.01194	-0.00181
t test	**-3.99146****	-0.82134	**2.049924***	**-3.90605****	-0.32909
Z test	**-3.99146****	-0.82134	**2.049924***	**-3.90605****	-0.32909
Negative Percentage	0.9	0.7	0.4	0.9	0.5
2022 (N=8)	AR0	AR1	AR2	CAR [0,1]	CAR [0,2]
AAR/CAAR	-0.00564	-0.01982	-0.016	-0.02546	-0.04146
t test	-0.29076	-1.68202	-2.62154	-1.21898	-2.08527
Z test	-0.29076	-1.68202	-2.62154	-1.21898	-2.08527
Negative Percentage	0.5	0.75	1	0.5	0.75
2023 (N=9)	AR0	AR1	AR2	CAR [0,1]	CAR [0,2]
AAR/CAAR	-0.005147	-0.002527	0.02074	-0.005147	-0.007674
t test	-1.865829	-0.233745	0.716428	-1.865829	-0.814306
Z test	-1.865829	-0.233745	0.716428	-1.865829	-0.814306
Negative Percentage	0.833333	0.5	0.333333	0.833333	0.5

Source: This study
Note: ***, **, * denote significance levels of 1%, 5% and 10% respectively.

From Table 7, we find that abnormal returns are increasing from 2020 to 2023, i.e., the losses caused to the companies are decreasing from 2020 to 2023. It changes from -1.28% in 2020 to -0.5 % in 2023. However, this result is significant only in 2021. Events occurring in 2021 are significantly negative at 0.05 and 0.01 levels on day 0 and day 2, respectively. The

cumulative average abnormal return in (0, 1) are significantly negative at 0.05 level, the results confirm H3(a). China increased its regulation on personal information protection in 2021. The much-anticipated PIPLPPC was passed by the 30th meeting of the Standing Committee of the 13th National People's Congress (NPC) on 20 August and has come into effect on 1 November 2021. The next section of this paper will focus on analysing whether there is a significant difference in impact of App violation problems notifications on companies before and after the implementation of PIPL.

Personal Information Protection Law

We compare the abnormal returns before and after the implementation of PIPL to further explore whether the state regulation of personal information protection has a significant impact on our previous findings.

Table 8: Abnormal Return Before and After Implementation of Personal Information Protection Law

Before Implementation (N=27)	AR0	AR1	AR2	CAR [0,1]	CAR [0,2]
AAR/CAAR	-0.01171	-0.00671	0.001827	-0.011712	-0.018417
t test	**-1.89864***	-1.21589	0.444269	**-1.898643***	**-1.815977***
Z test	**-1.89864***	-1.21589	0.444269	**-1.898643***	**-1.815977***
Negative Percentage	0.84	0.63	0.47	0.84	0.78
After Implementation (N=19)	AR0	AR1	AR2	CAR [0,1]	CAR [0,2]
AAR/CAAR	-0.00329	-0.010679	-0.000799	-0.00329	-0.013969
t test	-0.5338	0.187581	-0.091631	-0.5338	**-1.708017***
Z test	-0.5338	0.187581	-0.091631	-0.5338	**-1.708017***
Negative Percentage	0.583333	0.78	0.56	0.67	0.67

Source: This study

Note: ***, **, * denote significance levels of 1%, 5% and 10% respectively.

From Table 8, we find that before the implementation of Law, AR is significant at -1.17% at 0.10 level on day 0, and cumulative average abnormal return is significant at -1.84% at 0.10 level in event window (0, 2). In contrast, it is negative but insignificant on day 0 after the implementation of Law, and significant at -1.06% at 0.10 level on day 1. The cumulative average abnormal return for event window (0, 2) is significant at -1.39 % at 0.10 level, with relatively larger losses after implementation of the Law, the results support H3(b). The enactment and implementation of PIPL has a significant impact on companies whose App has violation problems. The Law details and improves the principles that should be followed in protection of personal information, such as the principle of "minimal access" and "openness and transparency" to information of obligee. It clarifies the boundaries of rights and obligations in handling of personal information, improves the institutional mechanism for personal information protection, and builds a "protection network" for personal information, which will maximise the protection of citizens' rights and interests. Studies have shown that perceived privacy risk has a negative impact on perceived security of mobile phone applications (Balapour et al., 2020). The soundness of law raises awareness for the whole society about the protection of personal information, which influences users' decision-making about disclosure of personal information. The notification of companies' App violation problems will lead to a decrease in the trust of users or investors, etc., This leads them to question their ability to produce and operate, thus bringing larger losses to companies.

CONCLUSIONS

Previous studies have focused on the impact of privacy breach on affiliated companies, users' attitudes on personal information disclosure decisions in face of App breaches, and so on. In the era of mobile internet, the impact of Apps being notified for violation problems on the market operation and market value of companies has been less discussed. In this study, we collect notifications of App violation problems for listed companies, quantify the question using event study method. The market model is used to calculate the abnormal returns of companies, and the results are evaluated and discussed.

The results suggest that events of companies being notified for App violation problems have a significant negative impact on companies' market value. This result is consistent when calculated using both market model and Fama-French three-factor model. This suggests that when a company's App is notified for infringing on users' rights and interests, the event might cause the public to distrust it and make it's reputation damaged, but will actually affect it's stock market. The investors may feel a breakdown in trust when an App is found to be in violation. They will perceive the App as not complying with rules and regulations and be unethical. This distrust may lead investors to doubt the future of companies and reduce their interest in investing. In addition, among different types of violation problems, violations of collecting and using of personal information can have larger negative impact on companies. Both of those behaviours are violations of users' privacy. The illegal use of personal information without user's consent may lead to abuse for fraud, harassment, etc., causing financial loss and mental distress to user, and thus causing even more damage to compamies. If users uninstall the app in large numbers or use it for fewer hours due to privacy violations, the companies' business may suffer. This could result in the company losing customers, market share and revenue. We therefore analysed the event from perspective of time. The result shows that over time the negative impact on market value on the day of notification is decreasing. However, the results are significant only in 2021. Furthermore, we explore whether there is a significant difference in impact of notification on companies before and after the

implementation of Personal Information Protection Law. We found that the negative impact of App violation notification on companies became larger after implementation of the Law. The Act states clear provisions on various types of situations, including the use of sensitive personal information and the handling of personal information in violation of law. Violations of the Personal Information Protection Act will be severely punished. Besides, the Act increases the compliance costs for companies, so that user information security is better protected. This warns that companies should conduct App development and information collection within the scope of law. In the era of digital economy and mobile IoT, the quantitative analyses of this study can provide auxiliary support to companies and government in decision making when facing information and privacy protection.

The study still has some limitations. The data collected in this study is mainly from the Chinese market. The result might nor be applicable to other country. The other researchers can explore other datasets for advance work. Besides, there are other App infringements that were not included. Subsequent research could expand the categories and investigate the impact of them on companies. The findings focus on the short-term impact of App violations on companies, and we do not estimate the various period for long-term valuation.

ACKNOWLEGEMENTS

This research is supported by grants from Beijing Social Science Foundation (Grant 23GLB012). Xiong Zhang (xiongzhang@bjtu.edu.cn) is the corresponding author.

REFERENCES

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, *52*, 102063. https://doi.org/10.1016/j.ijinfomgt.2019.102063

Cyberspace Administration of China. (2019, December 30). *Notification on the Publication of the Method for Determining the Acts of Illegal and Illegal Collection and Use of Personal Information by Apps*. Https://Wap.Miit.Gov.Cn/Jgsj/Waj/Wjfb/Art/2020/Art_8663d2afe61b40c3beb7c65bf6ec2a64.Html.

Libaque-Sáenz, C. F., Wong, S. F., Chang, Y., & Bravo, E. R. (2021). The effect of Fair information practices and data collection methods on privacy-related behaviors: A study of Mobile apps. *Information & Management*, *58*(1), 103284. https://doi.org/10.1016/j.im.2020.103284

Tripathi, M., & Mukhopadhyay, A. (2022). Does privacy breach affect firm performance? An analysis incorporating event-induced changes and event clustering. *Information & Management*, *59*(8), 103707. https://doi.org/10.1016/j.im.2022.103707

Wu, D., Moody, G. D., Zhang, J., & Lowry, P. B. (2020). Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention. *Information & Management*, 57(5), 103235. https://doi.org/10.1016/j.im.2019.103235

China National People's Congress. (2021, August 20). Law of the People's Republic of China on the protection of personal information. Retrieved from China National People's Congress website.

Liu, B. L. & Sun, W.-J. (2021). A process study of mobile users' information disclosure decision making from a holistic perspective of communication privacy management theory. *Management Science*, *34*(6), 76–87. https://doi.org/10.3969/j.issn.1672

Liu, B.L. Yang, S. L., & Li, Y. H. (2018). An empirical study on the influence and interaction of privacy preference setting and privacy feedback on mobile commerce users' behavioural intention. *China Management Science*, *26*(8), 164–178.

Wui Y. L. Zhang J. R. Wang F. J. & Cheng M. Y. (2022). A study on the relationship between data asset disclosure and analysts' surplus forecasts - Empirical evidence based on textual analysis. *Journal of Management Engineering*., *36*(5), 130–140.

Ministry of Industry and Information Technology. (2021). Publicly soliciting opinions on the three-year action plan for high-quality development of the cybersecurity industry (2021-2023) (Draft). Retrieved from Cyber Security Administration website.

Ministry of Industry and Information Technology. (2020). Notice of the ministry of industry and information technology on the deepening of special remedial actions for app infringement of users' rights and interests. Retrieved from Ministry of Industry and Information Technology website.

Wang, L. Wang, L. Y. & Sun, Z. (2020). Mechanisms of privacy violation experiences on internet users' self-disclosure. *Systems Engineering Theory and Practice*, *40*(1), 79–93.

Zhen, J., Xie, Z. X. Li, K. H. & Lin, R. H. (2020). Information security governance and firm performance: A moderated mediation model. *Nankai Management Review*, *23*(1), 158–168.

General Office of the Ministry of Industry and Information Technology. (2021). Notice on the issuance of provisions on the scope of necessary personal information for common types of mobile internet applications. Retrieved from the Office of Internet Information Technology website.

Mobile app trend insights white paper. Retrieved March, 2022, from Avery website, https://report.iresearch.cn/report_pdf.aspx?id=3955

Xie, Z. X. Lin, R. H. & Wang, X. Q. (2013). The effect of user participation on the effectiveness of information security management - A multiple mediation approach. *Management Science*, *26*(3), 65–76.

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management, 52*(3), 337-347. https://doi.org/10.1016/j.im.2014.12.006

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An event study analysis of the economic impact of IT operational risk and its subcategories. *Journal of the Association for Information Systems*, *12*(9), 1. 10.17705/1jais.00275

Bose, I., & Leung, A. C. M. (2013). The impact of adoption of identity theft countermeasures on firm value. *Decision Support Systems*, *55*(3), 753-763. https://doi.org/10.1016/j.dss.2013.03.001

Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19-28. https://doi.org/10.1016/j.dss.2016.10.002

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision support systems*, 106, 44-52. https://doi.org/10.1016/j.dss.2017.12.003

Zhang, X., Xie, H., Yang, H., Shao, H., & Zhu, M. (2020). A general framework to understand vulnerabilities in information systems. *IEEE Access*, 8, 121858-121873. 10.1109/ACCESS.2020.3006361

Zhang, X., Tsang, A., Yue, W. T., & Chau, M. (2015). The classification of hackers by knowledge exchange behaviors. *Information Systems Frontiers*, 17, 1239-1251. https://doi.org/10.1007/s10796-015-9567-0

Zhang, X., Shao, H., Zhu, M., & Zhang, R. (2020). Towards understanding vulnerability in information systems: The topic modeling perspective. Retrieved from https://aisel.aisnet.org/pacis2020/242

Yang, H., Zhang, J., & Zhang, X. (2021). Network vulnerability and enterprises' response: The preliminary analysis. In *AMCIS*. Retrieved from https://aisel.aisnet.org/amcis2021/info_security/info_security/22

Junzhe Dong., Shuo Geng., Xiong Zhang.(2024) An intelligent retrieval system for similar information system vulnerabilities based on knowledge graph. *IEEE International Conference on Data Science in Cyberspace* (IEEE DSC 2024), Jinan, China, August 26-28, 2024.