Research on Privacy Policy Compliance of Third-Party Payment Platforms

Zhi Ye(✉) and Shanshan Li

School of Information Management, Wuhan University, Wuhan 430072, China
yz_whu@whu.edu.cn

Abstract. [Significance] To investigate the compliance of the content clauses of the privacy policies of third-party payment platforms based on the laws, regulations, and standards related to personal financial information. [Methods] Based on 21 laws, regulations, and standards related to personal financial information, we constructed the compliance evaluation index system by using the grounded theory and analyzed the privacy policies of mainstream third-party payment platforms using the content analysis method. [Conclusions] The compliance of third-party payment platforms is high; the privacy policies of third-party payment platforms for corporate-side customers are not perfect; and compliance is poor in terms of individual rights.

Keywords: third-party payments · privacy policy · compliance

1 Introduction

In December 2020, the scale of China's online payment users reached 854 million. However, since 2021, "violation of credit information collection, provision, and inquiry" has become a common type of violation in the administrative penalties issued by the People's Bank of China against banks.

Under strong regulation, how well do third-party payment platforms protect personal information? The purpose of this paper is to explore whether the privacy policies of third-party payment platforms comply with the laws and regulations, which helps to understand the current situation of self-regulation in China's third-party payment industry, identify problems in the formulation and implementation of privacy policies.

2 Related Research

Tu clearly defined third-party payment as an online payment model in which independent institutions with certain strengths and credibility are contracted with major banks to facilitate transactions between two parties by interfacing with the banks' payment and settlement systems [1] Tu studied the business practices, products, services, and privacy terms of some typical third-party payment enterprises to analyze the risks and reasons for the existence of personal information of third-party payment users. Zhuo [2]

V. Gaikar et al. (Eds.): ECIT 2023, AHE 18, pp. 297–305, 2023.
https://doi.org/10.2991/978-94-6463-210-1_39

investigated the compliance of service agreements and privacy policies of 10 third-party payment platforms using the Information Security Technology Personal Information Security Specification as the judgment standard. Gong [3] defined the scope and content of consumer personal information and rights in third-party payments by analyzing consumer personal information protection cases.

A privacy policy is a self-regulatory document in which Internet service providers describe and make commitments to the lawful collection and usage of personal information based on their service functions. Privacy policy compliance refers to the extent to which the privacy policy complies with relevant national laws and regulations and industry standards. In the study of privacy policy compliance, various types are covered, including websites, mobile reading, healthcare, and social applications. In the meantime, a series of methods are used, including machine learning, text analysis, comparative analysis method, and content analysis method.

Valentine [4] used content analysis to code the ALA privacy policy guidelines. Javed [5] evaluated website privacy statements from 10 sectors in three South Asian countries, and found low accessibility and privacy compliance, particularly in the education, healthcare, and government sectors. Some scholars used content analysis to evaluate privacy policy. Ma [6] constructed a comprehensive evaluation index system to evaluate 104 mobile health apps. Ni [7] constructed an evaluation scale based on the Personal Information Security Specification and assessed the compliance of 45 popular chronic diseases from the perspective of information life cycle management application.

Li [8] constructed core indicators based mainly on users' rights, application operators' obligations, and regulators' responsibilities as the key to determining whether a privacy policy is compliant. Fu [9] found leading Chinese Internet and information service providers privacy policies to be generally compliant with China's personal information protection provisions, but their Fair Information Practices need improvement. Mohan [10] found that many cloud services claiming compliance did not have clear and concise privacy policies and found "GDPR dark patterns" (areas of non-compliance) in ten large cloud services. Xiao [11] extracted and summarized the scope of regulations and standards related to personal information protection, constructed a compliance evaluation index system, and conducted an empirical study on social applications. Lu [12] tested 100 banking apps, using download and installation as the test criteria, and found that privacy policy was a prominent issue.

In summary, privacy policy evaluation has gained extensive attention from scholars all around the world. However, most of the research were published before the implementation of the Data Security Law and the Personal Information Protection Law of the People's Republic of China and evaluated based on standards. There is no relevant research on the evaluation of current privacy policies based on laws and regulations, and the types involved are mostly websites, mobile reading apps, and healthcare, while there is less research on privacy policies for third-party payments.

3 Study Design

3.1 Study Materials

As there are many third-party payment platforms, we selected the top 10 platforms in terms of market share and influence according to the China Third-Party Payment Industry Research Report 2021. This is a list of the collection: Alipay, TenPay, One Wallet, UMF, 99bill, UnionPay, YeePay, ResPay, Jingdong Finance, and DxmPay. The privacy policies (including the list of third-party information sharing, personal information protection rules for children, list of device permissions, etc.) were obtained from the companies' official websites, and the privacy policies were collected until 15 October 2022.

3.2 Research Methodology

The evaluation indexes were constructed based on existing laws, regulations, and standards, drawing on the existing indexes. We used keywords, such as "information", "confidentiality", "privacy" and "security", to search the national laws and regulations from the PKU Law database. And we browsed the government's official websites to search for laws, regulations, and standards that we may miss. Many papers constructed evaluation systems based on the Information Security Technology Personal Information Security Specification", which is widely used in privacy policy evaluation, including other highly related standards. Finally, we got 21 laws, regulations and standards. Then, we used a text coding approach to construct an index system for evaluating the privacy policy compliance of third-party payment platforms.

Based on the idea of grounded theory, each category of the compliance indicator system was formed following the steps of open coding and axial coding. Firstly, the Personal Information Protection Law of the People's Republic of China was coded openly, and the substantive content of the relevant articles was extracted and conceptualized. The 29 subject areas were conceptualized by extracting the substantive content of the relevant articles. The remaining laws, regulations, and standards were then coded in the same way, with new codes added to those that could not be covered by the previous codes until they were saturated, resulting in 9 new categories. The 38 categories were coded in a correlational way to explore the potential relationships and connections between them, to discover the main categories, and to summarize them into 7 main categories, which were used as first-level indicators. The 38 thematic categories formed by open coding were used as secondary indicators, resulting in a compliance evaluation indicator system (see Fig. 1).

3.3 Content Analysis Implementation Process and Reliability Test

According to the compliance evaluation index system, we assigned values to the second level indicator. There is no distinction of importance, and the completeness of evaluation indicators is used as the judgment criterion. The number of secondary indicators included in the privacy policy is counted and then aggregated to obtain a compliance score.

First-level indicators	Second-level indicators	First-level indicators	Second-level indicators
Privacy Policy Basics	Personal Information Processor Information	Information entrusment、sharing、transfer	Information about the recipient of personal information
	Scope of application		Rights and obligations of the parties
	Effective time frame		Purpose, manner of information processing
	Basic principles of personal information security		Third-party access management
	Policy Updates	Sensitive information	Sensitive personal information
Collection and usage of personal information	Types of personal information		Minors' information
	Authorization and device permissions		Children's information
	Indicate the purpose, manner, and scope of collection and usage of information	Individual rights	Access to copy personal information
	Data classification and grading		Correction of additional personal information
	Re-authorization following changes in the purpose, manner, and scope of collection and usage of information		Delete personal information
	Circumstances in which consent is not required		Information transfer
	Circumstances in which collection will cease		Get a copy of your personal information
	Automated decision making		Cancellation of accounts
	Cross-border provision of personal information		Consent, refusal, or withdrawal of authorization
	The usage of cookies and similar technologies		Request Response
Information storage	Information storage period		Deceased users
	Information storage locations	Obligations of personal information Processors	Safety and protection measures
	Information storage protection measures		The way to report complaints about personal information security
			Informing the user of the situation
			Security incident planning and remedial measures

Fig. 1. Third-party payment platform privacy policy compliance evaluation index system

4 Results

4.1 Overall Compliance Analysis

The overall average compliance score of third-party payments was 32.8 (see Fig. 2), with a good degree of compliance. The pull-down in the overall average compliance score was mainly influenced by UMF and Yeepay. Among them, DxmPay scored the highest, with the best compliance; UMF and Yeepay got worst results, and their compliance scores were lower in terms of individual rights.

Each platform scored full marks in the areas of information storage, entrustment, sharing and transfer, and obligations of personal information processors, indicating a good level of compliance. The scores of collection and usage of personal information and individual rights varied widely, with many shortcomings. For example, only a few

Platform name	Privacy Policy Basics	Collection and usage of personal information	Information storage	Information entrusment、sharing、transfer	Sensitive information	Individual rights	Obligations of personal information processors	Total (38 items in total)	Ranking
Alipay	5	9	3	4	3	7	4	35	2
TenPay	4	9	3	4	3	7	4	34	6
One Wallet	4	9	3	4	3	7	4	34	6
UMF	4	7	3	4	3	2	4	27	9
99bill	4	8	3	4	3	5	4	31	8
UnionPay	4	8	3	4	3	9	4	35	2
YeePay	4	9	3	4	2	0	4	26	10
ResPay	5	10	3	4	3	6	4	35	2
Jingdong Finance	5	9	3	4	3	7	4	35	2
DxmPay	5	10	3	4	3	7	4	36	1
Average score	4.4	8.8	3	4	2.9	5.7	4	32.8	

Fig. 2. Total average compliance of third-party payment platforms

platforms clearly stated that data is classified and graded, and processed according to classification; most platforms did not state the rights to transfer their information or how to exercise their rights over the personal information of deceased users. The pull-down of the overall average compliance score is mainly influenced by two aspects: the collection and usage of personal information and individual rights.

4.2 Analysis of Secondary Indicator Results

1) Privacy Policy Basics

Four platforms received full marks for excellent compliance, while the remaining platforms had varying degrees of deficiencies. UMF and YeePay did not state the time limit for the effective date, and no corresponding announcement could be found in their APPs or official websites; the remaining platforms left some time between the adjusted date and the effective date, allowing users to consider whether to re-agree to the privacy policy. Tenpay, One Wallet, 99bill, and UnionPay did not state the basic principles followed by the platforms in processing personal information.

2) Sensitive Information

Except for Yeepay, which did not state how children's information would be processed, all platforms gave definition or examples of sensitive personal information and included authorized consent from parents or guardians of minors before obtaining personal information, as well as mechanisms for processing and protecting personal information. Each platform stated that it will adopt encryption technology to encrypt and store users' personal sensitive information, and will adopt physical approaches, security technology, management systems, and other measures to protect information security under the current level of technology.

As for biometric information, such as fingerprints and facial features, most platforms explicitly stated that they will not collect biometric information from users, and fingerprints and facial information will be stored on the device, and extraction and verification of biometric information will be completed at the device, with the platform receiving only the verification results. In contrast, UnionPay stated that it will store biometric information separately from personal identification information, will not store the original biometric information in principle, but only the summary information of the biometric information, and will not keep personal financial identification information. In addition, UMF, 99bill, and Yeepay did not state how the platforms will collect and process biometric information. It is worth mentioning that UnionPay stated that it is not available to children under the age of 14; UMF stated that minors should stop using it; and DxmPay did not provide services to those under the age of 18 and may provide limited browsing services.

3) Collection and Usage of Personal Information

All platforms specified the type, purpose, manner, and scope of the information collected and used, the circumstances under which user authorization and re-authorization are required. And they listed the device permissions required to be obtained to provide each function, the impact of the platform's usage of automated decision-making on users, and how the platform uses cookies and similar technologies. Upon investigation and analysis, the following issues were found: (1) none of the platforms mentioned that they would classify and grade the data collected, except for UnionPay, ResPay, and

DxmPay; (2) UnionPay did not state the circumstances under which information could be collected and used without the user's consent, and did not cite the original law, and the description was not comprehensive; (3) UMF, 99bill and UnionPay did not state the Circumstances in which consent is not required (4) UMF did not describe the cross-border provision of personal information.

4) Individual Rights

In terms of individual rights, most platforms performed well overall in terms of general rights protection and poorly in terms of specific rights, with average compliance scores mainly pulled down by two platforms, UMF and YeePay. In terms of general rights protection, most platforms (70%) provided users with the access rights to copy, correct, delete, obtain a copy of personal information, cancel their accounts, consent, refuse or withdraw authorization and request a response. As for special rights protection, except for UnionPay, which provided a statement and means of exercising rights over deceased users' information, none of the platforms mentioned this, and many platforms have to improve their practices in terms of information transfer and management of deceased users' information.

Two platforms, UMF and YeePay, scored very low on personal rights, with YeePay scoring 0. We did not find users' rights description in its apps or official website, and we did not obtain the information protection text by calling the Information Protection Office; UMF only scored on two second level indicators, consent, refusal or withdrawal of authorization, and cancellation of accounts, this also means UMF got Poor performance in other indicators.

5) Information Storage, Information Entrustment, Sharing, Transfer, and Obligations of Personal Information Processors

All selected third-party payment platforms received full marks, indicating that these platforms state (1) the location, duration, and storage protection measures of information storage; (2) disclosure of the type and manner of information collected by third parties, information about the recipient of the information and the rights, obligations purpose and manner of both parties when entrusting the processing of personal information; 70% of the platforms provided links or attachments similar to the Third Party Information Sharing List, while the remaining 30% stated that they had obtained users' consent before the third party collected information; (3) the specific protection measures for personal information security, the way to report complaints about personal information security, the circumstances in which users are explicitly required to be informed, as well as the security incident plans and remedial measures, comply with the requirements of laws, regulations, and norms.

5 Conclusion

The 10 third-party payment platforms have a high market share and influence and are subject to strong government regulation due to the specific industry they operate in. Therefore, the compliance of the privacy policies of the 10 selected third-party payment platforms is relatively high, but there are also some shortcomings and room for improvement of the privacy policies.

First, the content completeness of the privacy policies needs to be improved, especially for third-party payment platforms targeting corporate users. The study found that

the content of some platforms is incomplete; in addition, for third-party payment platforms targeting corporate users, the privacy policy does not list the effective date of updates and lacks a description of individual rights. Drawing on the policy templates provided in the Information Security Technology Personal Information Security Specification, enterprises should improve their privacy policies by comparing the content with the compliance evaluation index system.

Second, in response to the potential for over-scope collection of non-essential information, platforms need to reconsider the way they identify users. Except for 99bill and UnionPay, all platforms require verification and retention of copies or photocopies of valid identity documents and other information that can prove users' identities. According to terms 5 and 14 of the Supervision and Administration of Anti-Money Laundering and Anti-Terrorist Financing of Financial Institutions, financial institutions may obtain customer identification information to fulfill their anti-money laundering and anti-terrorist financing duties or obligations. In 2017, the People's Bank of China issued a notice to strengthen anti-money laundering customer identification, which is based on the "Measures on Customer Identification and Customer Identification of Financial Institutions" issued in June 2007. According to Measures for the Administration of Retention of Information and Transaction Records, the institution shall identify the customer if a single transaction exceeds RMB10,000 or USD1,000. Third-party payment platforms can use other ways to cross-check and identify users to balance the convenience and security.

Third, the government should continue ongoing policy regulation. In 2017, the Office of the Internet Trustee, together with three other departments, launched a special work on privacy policy and continued in the following years, effectively promoting APPs to improve their privacy policies. The study found that most third-party payment platforms have updated their privacy policies relatively quickly. The high level of compliance with the obligations of personal information processors, the storage, entrustment, sharing, and transfer of personal financial information and sensitive information is inextricably linked to the ongoing review and regulation by the regulator, so this work should also continue and be combined with credit rating and reward and punishment methods to achieve greater regulatory effectiveness.

Fourth, we will continue to promote the certification of "personal financial information protection capability". Personal financial information protection capability certification refers to the assessment of conformity with standards in terms of personal financial information collection, storage, transmission, processing, classification, and grading. Personal financial information contains a large amount of sensitive information, and once it is leaked or viewed without authorization, it will cause harm, or even serious harm, to information security and property safety. This will help protect the rights and interests of financial consumers, and it is a recognition of the full process of protection, which will enable users to use it with confidence.

Finally, the protection of users' rights should be strengthened. The third-party payment platforms distinguish essential and non-essential user information based on different functions, and provide explanations of the scope and manner in which information is collected, stored, processed, and used. However, they do not pay enough attention to individual rights, especially the right to transfer information and the deceased users. And

the platforms do not provide instructions on how to exercise their rights; some platforms do not provide ways for users to obtain copies of their personal information. Platforms should comply with the requirements of regulations and standards, enrich the content of users' rights, and balance the rights of users and platforms.

References

1. Tu Meng, Zhang Mianwei. Research on the risk of personal information security of third-party payment users and countermeasures [J]. Intelligence Theory and Practice,2018,41(12): 70-75.
2. Zhuo Xia Ting. Research on the compliance of personal information clauses in third-party payment platform agreements [D]. Xiangtan University, 2019.
3. Gong Binbin. An empirical study on the protection of consumers' personal information in third-party payment [D]. Zhengzhou University, 2020.
4. Valentine G, Barron K. An Examination of Academic Library Privacy Policy Compliance with Professional Guidelines[J]. Evidence-Based Library and Information Practice,2022,17(3):77-96.
5. Javed Y, Salehin K M, Shehab M. A study of South Asian websites on privacy compliance[J]. IEEE Access, 2020, 8: 156067-156083.
6. Ma Zhangyu, Liu Qiankun. Evaluation and empirical study of privacy policies of mobile health apps[J]. Library intelligence work,2020,64(07):46-55.
7. Ni Z, Wang Y, Qian Y. Privacy Policy Compliance of Chronic Disease Management Apps in China: Scale Development and Content Evaluation[J]. JMIR mHealth and uHealth,2021,9(1):e23409.
8. Li Yanshun. Compliance review and improvement of mobile application software privacy policy in China - a textual examination based on 49 cases of privacy policy[J]. Legal Business Re-search,2019,36(05):26-39.
9. Fu T. China's personal information protection in a data-driven economy: a privacy policy study of Alibaba, Baidu and Tencent[J]. Global Media and Communication,2019,15(2):195-213.
10. Mohan J, Wasserman M, Chidambaram V. Analyzing GDPR compliance through the lens of privacy policy[M]//Heterogeneous Data Management, Polystores, and Analytics for Healthcare. Springer, Cham, 2019: 82-95.
11. Xiao Xue, Cao Yufei. Compliance study of personal information protection policies for social applications in China[J]. Intelligence Theory and Practice, 2021, 44(03):91-100.
12. Lu, Zhi-Rui. The protection and utilization of financial consumer information from the evaluation results of 100 banking apps: On the occasion of the consultation on the Draft Law on the Protection of Personal Information[J]. Credit, 2021,39(03):38-46.