The Impact of the Personal Information Protection Law on App Privacy Policies (Postprint)

Authors: Han Shuo

Date: 2023-10-08T00:00:00+00:00

Abstract

[Purpose/Significance] Comparing changes in APP privacy policies before and after the implementation of the Personal Information Protection Law can effectively evaluate its impact and limitations, providing reference for the formulation or revision of subsequent relevant laws, regulations, and policies. [Method/Process] Collected privacy policy changes of the top 30 APPs by user activity in the first half of 2021, analyzed whether they were influenced by the Personal Information Protection Law, and for those APP privacy policies that changed due to such influence, conducted coding and analysis using the coding approach of constructivist grounded theory, compared them with the content of the Personal Information Protection Law, and verified the conclusions using the privacy policies of APPs that remained unchanged. [Results/Conclusion] The study indicates that with the implementation of the Personal Information Protection Law, a substantial number of APPs have modified their privacy policies, notably adding rights such as the right to information duplication and separate consent for sensitive information. However, not all provisions have exerted significant influence; certain provisions lack enforceability and detailed standards, and have not manifested noticeable changes in privacy policies. Accordingly, optimization strategies and priority areas for subsequent laws and regulations are proposed.

Full Text

Preamble

Research on the Impact of the Personal Information Protection Law on APP Privacy Policies

Han Shuo[1,2]

[1]School of Information Management, Wuhan University, Wuhan 430072
[2]Advanced Study Center for Intellectual Property Rights of Wuhan University,

Wuhan 430072

Abstract

[**Purpose/Significance**] Comparing changes in APP privacy policies before and after the implementation of the Personal Information Protection Law can effectively evaluate its impact and limitations, providing valuable reference for subsequent formulation or revision of relevant laws, regulations, and policies. [**Method/Process**] This study collected privacy policy changes for the top 30 APPs by user activity in the first half of 2021, analyzing whether they were influenced by the Personal Information Protection Law. For those APPs whose privacy policies changed due to this influence, we employed constructivist grounded theory coding methods for encoding and analysis, compared these changes with the content of the Personal Information Protection Law, and validated our conclusions using privacy policies that remained unchanged. [**Result/Conclusion**] The research demonstrates that with the implementation of the Personal Information Protection Law, numerous APPs revised their privacy policies, significantly adding rights such as the right to information copying and separate consent for sensitive information. However, not all provisions produced substantial impact—some lacked enforceability and detailed standards, showing no significant changes in privacy policies. Based on these findings, we propose optimization strategies and priority areas for subsequent legislation.

Keywords: personal information protection; APP; privacy policy; grounded theory

Classification Numbers: G203; G920

Citation Format: Han S. Research on the Impact of the Personal Information Protection Law on APP Privacy Policies [J/OL]. Knowledge Management Forum, 2022, 7(6): 662-673 [citation date]. http://www.kmf.ac.cn/p/323/.

Introduction

In recent years, with the rapid development of new-generation information technologies, particularly mobile internet, personal information protection in APPs has become a critical issue of high concern to the Party Central Committee and the State Council, widespread public interest, urgent economic development needs, and universal international advancement [1]. On August 20, 2021, the 30th session of the Standing Committee of the 13th National People’ s Congress passed the Personal Information Protection Law of the People’ s Republic of China [2] (hereinafter referred to as the “Personal Information Protection Law”). China’ s personal information protection framework has gradually improved, evolving from the 2012 Decision of the Standing Committee of the National People’ s Congress on Strengthening Network Information Protection to the Cybersecurity Law and Consumer Protection Law, and finally to the specialized Personal Information Protection Law.

The Personal Information Protection Law took effect on November 1, 2021. During late October and early November, many APPs updated their privacy policies and sought renewed consent from users, clearly responding to the law' s effective date. The update notices or changelogs explicitly mentioned the Personal Information Protection Law. For example, Taobao' s privacy policy update notice stated, "To better protect the legitimate rights and interests of Taobao platform members and in accordance with the latest regulatory requirements, we have updated the Taobao Privacy Policy" [3]. Weibo announced that to fully implement the requirements of the Personal Information Protection Law, it updated its Weibo Personal Information Protection Policy [4]. Both JD.com' s Privacy Policy [5] and Tencent Video' s Privacy Protection Guidelines [6] directly cited relevant definitions from the Personal Information Protection Law.

Privacy policies, also known as "personal information protection policies," represent the primary mechanism through which personal information controllers follow the principle of openness and transparency to inform users about the scope and rules of personal information collection and use. They serve as an important mechanism for self-regulation and cooperation with supervisory management, and as a crucial means to guarantee the right to information of personal information subjects [7]. Therefore, changes in privacy policies constitute one of the most visible and rapid manifestations of APP operators' compliance with the Personal Information Protection Law. Studying these changes can reveal the law' s implementation effectiveness and existing problems, providing important reference for subsequent updates to the law, implementation rules, and related policies.

Literature Review

Personal information protection has been extensively studied across management, law, computer science, and other fields. As early as 2005, legal scholar Qi Aimin researched Personal Information Protection Law legislation and proposed a draft [8-9]. Since its enactment, scholars have widely discussed various aspects of the law, including its relationship with the Civil Code [10], rules for damages compensation for personal information violations [11], and regulations on cross-border data flows [12]. Implementation of the law has also attracted attention, primarily through theoretical analyses [13-14] and news reports [15], as well as industry-specific studies examining its impact on sectors such as healthcare [16] and finance [17]. However, no studies have specifically measured its actual implementation.

Privacy policies are closely linked to the Personal Information Protection Law and have long been a research subject. Studies have examined the interpretation and optimization strategies of the "notice-consent principle" [18], corporate privacy policy regulation [19], and in the library and information science field, numerous scholars have conducted textual analyses of APP privacy policies. These include framework optimization and compliance assessments for mobile reading and healthcare software [20], user-friendliness measurements [21], and analyses of user reading behavior regarding privacy policies [22]. Comparative studies of typical domestic and international privacy policy changes have also been conducted [23-24]. Grounded theory and its coding methods are widely used in privacy policy analysis. For instance, Wen Yuheng et al. [25] encoded text related to "data" in privacy policies of China's top internet companies to understand and correct data property rights concepts in the digital market. Zhang Yue et al. [26] used grounded theory to construct a framework of factors influencing medical consultation APP privacy policy cognition through interviews with 23 university students, offering relevant recommendations. These studies provide methodological references for this research.

Through analysis of relevant research, we find that studies on the Personal Information Protection Law have focused on content and theoretical discussions, with few measuring its implementation effectiveness. Privacy policy comparison studies have typically examined single policies rather than patterns across multiple policies. As a critical application of the Personal Information Protection Law, no research has yet measured the law's implementation through privacy policy changes.

Research Design and Methodology

First, we selected APP samples, queried their privacy policies, determined revision dates, and assessed whether changes were related to the Personal Information Protection Law's implementation. We then applied constructivist grounded theory coding methods to encode the samples, completing open coding and focused coding. The extracted focused codes were compared with provisions in the Personal Information Protection Law to ultimately determine the law's impact on APP privacy policies.

Constructivist grounded theory represents one of three mainstream grounded theory schools, developed by K. C. Charmaz by integrating B. G. Glaser's "classic grounded theory" and A. L. Strauss's "programmatic" grounded theory with constructivist theory [27]. Its coding methods and theory generation are highly open, viewing coding as merely a tool that should remain flexible rather than rigid [28]. For instance, it approves of coding units at the line, sentence, or event level, and does not exclude either the 18 theoretical models of classic grounded theory or the "6C" model of programmatic grounded theory [29]. Domestic examples also exist of modifying and optimizing coding methods based on constructivist grounded theory [30].

Since this research examines the impact of the Personal Information Protection Law on privacy policies, the influencing factors and affected concepts of the constructed theory are predetermined and separate. Therefore, our category extraction and theory construction differ from typical coding processes: we first conducted substantive coding of privacy policy changes, then summarized each provision of the Personal Information Protection Law, then corresponded the privacy policy change codes with these provisions, and finally extracted key indicators of the law' s impact on privacy policies, validated using privacy policies not included in the coding sample.

Research Sample and Data Sources

We selected the top 30 APPs from the "APP User Scale Ranking"in QuestMobile' s "China Mobile Internet 2021 Half-Year Report" [31] published in July 2021 as our research sample. We collected current and historical versions of these APPs' privacy policies, with a cutoff date of December 1, 2021. We screened for privacy policies updated within three days before or after November 1, 2021, and those updated between August 20 and December 1, 2021 with other evidence of being influenced by the Personal Information Protection Law, using these as coding samples. Historical versions were obtained primarily through publicly available historical versions provided by APP operators and versions archived by web snapshot services. Modified content was identified through update notices when new privacy policy versions were released, using text comparison software such as Word and Beyond Compare 4 to identify differences between old and new versions, supplemented by manual screening.

Among the research samples, 18 APPs updated their privacy policies within three days of November 1, 2021. Historical versions could not be found for 5 APPs, and 3 others updated outside this timeframe but with evidence of being influenced by the Personal Information Protection Law. Ultimately, 16 versions that could be confirmed as influenced by the law and for which both old and new versions were available were used as the basis for coding. Eight APPs whose latest privacy policy updates occurred before August 2021 could not have been influenced by the law. Six privacy policies updated around November 1, 2021, clearly influenced by the law but without available historical versions, were used to validate the coding results after completion. The update timelines and usage methods for each APP' s privacy policy are shown in Table 1 .

Coding Process

Open Coding

Based on text comparison results, we used Nvivo software for coding to obtain open coding results. During coding, we employed a substantive change coding approach, coding each modification once. If a change was limited to one sentence, that sentence served as the coding unit; if the change was substantial and involved multiple sentences, the smallest paragraph containing the single change served as the coding unit. Some changes might entail multiple substantive content changes, potentially resulting in multiple codes for one location. Modifications that only involved position changes without substantive content changes were not coded; modifications that changed wording for more accurate expression but without substantive content changes were not coded; obvious terminology changes were coded. After open coding, we performed 882 codes across 16 files. Due to space limitations, these are not listed here; the raw data has been uploaded to the Science Data Bank for hosting [32].

Focused Coding

Focused coding represents the second major coding process. It involves using the most important or most frequently occurring initial codes to filter codes with substantial data, making them more directed, selective, and conceptual than initial codes. The transition from initial to focused coding is not entirely linear; comparison, modification, and merging of later open codes with earlier ones essentially begin the focused coding process [28]. In our focused coding, we considered not only frequency but also substantive content changes, such as newly added user privacy-related rights and new data controller obligations.

Some changes followed functional modifications and did not affect the core content of privacy policies, nor were they changes influenced by the Personal Information Protection Law, so they were omitted during focused coding. The primary basis for judging functional changes was the APP' s version update notes from the relevant period. Our complete focused coding is available in reference [32], where parenthetical content indicates the number of files and reference points in Nvivo—that is, the number of privacy policies modified and the frequency of code occurrence across all samples. The table contains 133 primary codes (denoted by "a"), 53 secondary codes (denoted by "A"), and 6 tertiary codes (denoted by "B").

Analysis of Coding Results

Analyzing the coding results from the tertiary code level, the richest content appears in B1 Notice-Consent, followed by B5 User Rights and B4 Information Sharing. Detailed provisions on the notice-consent principle, strengthening individual rights, and clarifying obligations of personal information processors are universally recognized as the most important enhancements brought by the Personal Information Protection Law [32]. Within B1 Notice-Consent, the most frequent modifications were expanding the content and conditions notified to users, such as detailed explanations of information collection content, processing purposes, usage methods, privacy policy applicability scope, etc., and adding conditions for notifying users about policy changes and system permission usage. The second most frequent was adding situations requiring separate consent, such as processing sensitive personal information, children' s information, and changing processing purposes, which require separate user consent, enhancing protection for sensitive information and minors. The code also standardized exceptions to notice-consent, clarifying conditions under which personal information can be processed without notifying users.

In B5 User Rights, the main modifications were adding legal rights such as the right to copy, right to modify (manage personal information), right to withdraw consent, right to deletion (account cancellation), and rights of close relatives, as well as management rights including system permission management, personalized recommendation management, function disabling, and restricting automated information system decision-making. In B4 Information Sharing, constraints were added for both personal information users themselves and those sharing the information, with more detailed explanations of sharing purposes, content, conditions, and objects, including integration of sharing object lists and clarification of conditions for information transfer, including notification of the recipient' s name and contact information.

In B3 Information Security, the most modifications concerned information storage, primarily adding time and location restrictions on information storage, with more detailed explanations of conditions and responsibilities for cross-border transmission. Next were personal security incident response and security risk contact information, enhancing the emergency response capabilities of controllers and individuals regarding sudden security incidents. Changes in B2 involved privacy policy terminology modifications based on the Personal Information Protection Law' s definitions, such as changing the term "personal sensitive information" in old versions to "sensitive personal information" and aligning definitions with the law.

Notably, privacy policies contain substantial content related to cookies (data stored on user local terminals). The coding reveals that cookie-related provisions also underwent numerous changes, forming a separate tertiary category. However, the Personal Information Protection Law does not specifically regulate cookies and related technologies, indicating that even privacy policies released on the law' s implementation date were not entirely influenced by it. Therefore, we correspond the coding results with each provision of the Personal Information Protection Law below to better identify privacy policy changes specifically attributable to the law.

Correspondence with Personal Information Protection Law

This section analyzes each provision of the Personal Information Protection Law, extracts its main content, and then selects relevant codes from the focused coding above for correspondence, primarily using secondary and primary codes as units. Since the Personal Information Protection Law covers extensive content and is not specialized legislation for privacy policies, our analysis only extracts provisions related to privacy policies. The extraction of provision content primarily references interpretations by the Legislative Affairs Commission of the Standing Committee of the National People' s Congress [33], the Supreme People' s Court [34], and legal scholars [35]. Table 2 details the correspondence, where suffixes in the "Corresponding Privacy Policy Changes" column indicate the number of privacy policies modified.

Table 2 shows that most relevant provisions of the Personal Information Protection Law have impacted APP privacy policies. Based on the quantity and content of impact, provisions can be divided into three categories:

First Category: Provisions with obvious and broad impact, characterized by numerous corresponding code types and high impact quantities. These include Articles 4, 14-16, 19, 22-25, 28, 29, 31, 38, 44-51, 53, 57, 59, and 73. Articles 4, 28, and 73 define relevant concepts, and privacy policies correspondingly modified their definitions. Article 15 stipulates the right to withdraw consent, with privacy policies adding this right—impacted by this single provision. Article 16 prohibits denying services for refusing information processing, leading privacy policies to add a "basic function" mode allowing product use without providing personal information. Other provisions like Article 19 on information retention periods, Article 23 on separate consent for sharing personal information, Article 29 on separate consent for processing sensitive personal information, Article 31 on minors' information, Article 45 on the right to copy, Article 46 on modifying information, Article 47 on deleting personal information, Article 49 on rights of close relatives, and Article 53 on specialized responsible institutions all follow this pattern.

Second Category: Provisions with relatively obvious but concentrated impact, characterized by high numbers of affected privacy policies but fewer code types, mostly general statements with low consistency in impacted content and likely different manifestations across privacy policies. These include Articles 13, 17, and 21. Article 13 specifies conditions for processing personal information, including six situations besides user consent, manifested in privacy policies as exceptions where personal information can be processed without consent. In old privacy policies and standards [7], exceptions were generally divided into two categories: exceptions for collection and use consent, and exceptions for sharing and transferring personal information without consent. After the Personal Information Protection Law, privacy policies interpreted Article 13 differently: some integrated both exception types (e.g., iQiyi), some retained only collection/use exceptions (e.g., WiFi Master Key), some applied them only to sharing (e.g., JD.com), some repeated identical exception conditions twice (e.g., Tencent Video), and some selectively extracted them separately (e.g., Toutiao, Meituan), or even applied them to cross-border transmission without consent (e.g., UC Browser). Article 17 specifies items requiring notification, a general provision of the notice-consent principle, manifested in privacy policies as improvements to information processing purposes, usage methods, collection content, applicability scope, and processor identity. Article 21 concerns entrusting personal information processing, manifested in privacy policies as enriched information on sharing purposes, conditions, content, and objects.

Third Category: Provisions with minimal impact, characterized by no corresponding codes or very few affected codes, such as Articles 20, 52, and 58 with no corresponding changes, and Articles 23 and 59 with minimal impact. The reasons include restrictive conditions without specific content, such as Article 52 stipulating that "personal information processors reaching the quantity specified by the national cyberspace administration shall designate a personal information protection 负责人," though the administration has yet to issue the specified quantity. Article 58 requires "personal information processors providing important internet platform services, with huge user numbers and complex business types" to fulfill special obligations, but without defining specific conditions. Another reason may be unclear applicability scope and relationships between provisions, such as Articles 20 and 23. Article 20 concerns joint processing by two or more personal information processors, while Article 23 concerns providing processed information to other personal information processors. Though similar to Articles 21 and 22 in content, their impact is far smaller. From privacy policy obligations, APPs attribute most behaviors to entrusted processing under Article 21 and transfer behaviors under Article 23, with fewer behaviors falling under Articles 20 and 23.

Impact Verification of Personal Information Protection Law

To verify the typical impacts identified above, we extracted key compliance items from the Personal Information Protection Law' s impact on privacy policies, primarily based on second-category provisions from Section 4.2 that affected numerous privacy policies. We identified several compliance indicators and compared them against collected unmodified privacy policies and those modified around November 1, 2021 without available old versions—that is, comparing privacy policies deemed unaffected versus those confirmed as affected by the law—to assess compliance status and validate our findings. The selected compliance indicators ultimately included 12 items: basic function mode, right to information copying, right to data portability, automated decision-making constraints (disabling personalized recommendations), rights of close relatives, specialized protection teams, etc. Table 3 details the comparison between the two types of privacy policies.

Overall, the Personal Information Protection Law' s implementation has had significant effects, with updated privacy policies showing more compliance items and clearly trending toward green (compliant). Notably, the Tencent News APP met all indicators. However, Table 3 also shows that some APPs' failure to update privacy policies does not mean they already meet the law's requirements. Although some privacy policies achieved relatively high protection levels before the law, the most compliant APP (Baidu) only met 4 requirements, far below the law' s standards.

By compliance item, the most obvious change is the constraint on automated decision-making, primarily manifested as users' ability to disable personalized recommendations, considered one of the law' s biggest highlights. Next are prohibitions on denying services for refusing information collection (basic function mode) and users' right to information copying. However, items such as rights of deceased subjects' close relatives, data portability, and notification content for personal information transfer remain unprovided in half of the modified privacy policies, indicating limited influence that aligns with our focused coding results.

Discussion

Overview of Personal Information Protection Law' s Impact

Among the 30 research samples, 18 privacy policies were updated within three days of the implementation date, and 4 were updated after its promulgation, affecting over two-thirds of samples, all stating compliance with recent laws and regulations, some explicitly citing the Personal Information Protection Law. Analysis of modified content found most changes traceable to the law, such as clarifying personal information collection content, usage methods, and processor identities; requiring separate consent and special notices for sensitive personal information; adding individuals' right to copy information; and establishing specialized departments for personal information protection. Definitions of personal information, sensitive personal information, anonymization, and de-identification were highly consistent with the law. The validation in Section 4.3 using the remaining 14 privacy policies also shows significantly higher compliance ratios in updated policies.

However, although over two-thirds of APPs updated their privacy policies, not all updates occurred before November 1. Some APPs only updated their policies in early December, one month after implementation, and nearly one-third have yet to make changes in response to the Personal Information Protection Law. As Section 4.3 demonstrates, failure to update does not indicate existing compliance, revealing insufficient enforceability of the law.

Problems with Personal Information Protection Law

Although the law prompted numerous APPs to update privacy policies, the updated policies do not fully comply with new requirements. For instance, Article 45 stipulates that users can copy personal information and transfer it to designated processors, yet most privacy policies only state that users can copy their personal information, with few providing transfer methods. Article 49 grants close relatives rights to access, copy, correct, and delete information after the subject' s death, but only a minority of updated privacy policies grant users this right for their close relatives. Provisions such as joint information processing (Article 20) and special notices for sensitive personal information processing (Article 30) are absent from privacy policies.

Additionally, several provisions have minimal impact due to lack of specific standards, such as Articles 52 and 58. Some APP privacy policy changes lack corresponding provisions in the law (e.g., cookie-related provisions), leading to non-uniform standards and simplified practices. Some provisions lack clear applicability scope interpretations, resulting in absent impact, such as Article 22 requiring separate consent when providing personal information to other processors, which privacy policies have not applied to any of their behaviors. Some provisions receive different or even contradictory interpretations across privacy policies, such as Article 13' s conditions for processing personal information without consent, which appear in various forms across privacy policy exception provisions.

Recommendations for Supporting Measures for Personal Information Protection Law

The identified problems do not reflect legislative inadequacy but rather the inherent limitations of a foundational law requiring supporting policies for effective implementation. Based on privacy policy modifications, we propose priority areas for supporting policies to inform subsequent legislation and regulations.

Standards for Special Processors Provisions such as Article 45(3) requiring personal information processors "meeting conditions specified by the national cyberspace administration" to provide personal information transfer pathways, Article 52 regarding processors "reaching quantities specified by the national cyberspace administration,"and Article 58 concerning processors "providing important internet platform services, with huge user numbers and complex business types" have not been accompanied by the administration' s "relevant regulations" [36], resulting in almost no APP privacy policies proactively complying. Therefore, standards and identification procedures for special processors should be promptly issued to implement these provisions.

Conditions for Information Sharing Articles 20-23 address non-single-processor personal information handling: joint processing, entrusted processing, information transfer, and providing information to other processors. While these impose different requirements, unclear applicability scope and relationships, particularly among joint processing, entrusted processing, and provision to others, have led privacy policies to extensively use entrusted processing and "affiliate company sharing" without requiring separate consent. This "affiliate company sharing"model, which shares personal information with other processors without separate consent, does not comply with any of Articles 20-23. Therefore, further clarification is needed on scope and limitations under different sharing models, particularly regarding the legal nature of frequently used "affiliate company" sharing models to prevent gray areas in APP privacy practices.

Exceptions to Consent Requirements Article 13 specifies six situations besides consent where personal information can be processed. However, collection, storage, transmission, and deletion pose different privacy risks, as Chapter 3 specially regulates cross-border transmission conditions and obligations as special requirements that clearly supersede Article 13' s general provisions. As Section 4.2 analysis shows, privacy policies interpret Article 13 differently, not universally treating cross-border transmission as a special condition. Therefore, supporting regulations should detail exceptions to consent requirements, specifying that special circumstances like cross-border transmission must meet particular conditions before Article 13' s general "no-consent" provisions can apply.

Cookies and Similar Technologies Cookies are small text files created by web browsers and stored on users' computers to identify users and improve server interaction efficiency [37]. As cookies contain user identity information and behavioral preferences controllable by website providers, they pose significant privacy risks [38] warranting regulatory attention. The EU' s Electronic Privacy Directive [39] is even called the "Cookie Law" due to its focus on cookies [40]. Although the Personal Information Protection Law addresses the notice-consent principle and user rights, it does not cover all privacy policy content, such as cookie-related provisions, leading many privacy policies to simplify cookie disclosures. Therefore, further regulations on cookies and related technologies are needed to ensure personal information protection when APPs use these technologies.

Conclusion

Evaluating law implementation effects helps assess whether legislative goals are achieved and identify problems [41]. Privacy policies represent a primary manifestation of China' s Personal Information Protection Law' s implementation effects. By studying privacy policy changes, we can evaluate the law' s impact and identify shortcomings. To avoid scholar interpretation bias and personal subjectivity, we conducted coding without detailed prior analysis of the law, then compared results provision by provision to trace privacy policy changes to their sources, assess the law' s impact, and identify problems such as inadequate implementation, lack of specific provisions leading to inconsistent interpretations, and propose optimization directions for supporting laws and regulations. These problems do not reflect flaws in the Personal Information Protection Law itself but rather its limitations as foundational legislation requiring implementation rules and related regulations. Our findings can inform the Personal Information Protection Law Implementation Rules, national cyberspace administration regulations, and the Ministry of Industry and Information Technology' s Interim Provisions on APP Personal Information Protection. However, this study has limitations: it only examines APPs' self-published privacy policies, whose legal nature and validity require further study as they are not recommended to be considered standard contracts under the Personal Information Protection Law. Moreover, the Personal Information Protection Law' s impact extends beyond APP privacy policies, which only reflect partial effectiveness of some provisions; comprehensive assessment of the law' s implementation effects can draw from other aspects.

References

[1] China Academy of Information and Communications Technology. White Paper on Personal Information Protection Governance of Mobile Internet Applications (APP) [R]. Beijing: China Academy of Information and Communications Technology, 2021.
[2] NPC Website. Order of the President of the People' s Republic of China

[EB/OL]. [2022-03-19]. http://www.npc.gov.cn/npc/c30834/202108/5891377866c04fd78df8d76d9b76338e.shtm
[3] Taobao. Taobao Rules Center - Notice of Changes to "Taobao Privacy Policy" [EB/OL]. [2021-11-27]. https://rulechannel.taobao.com/#/rule/detail?ruleId=11004810&cId=176.
[4] Weibo Administrator. Weibo Community Announcement [EB/OL]. [2021-12-17]. https://m.weibo.cn/status/4700169407565686?.
[5] JD.com. JD Privacy Policy [EB/OL]. [2021-11-27]. https://about.jd.com/privacy/.
[6] Tencent Video. Tencent Video Privacy Protection Guidelines [EB/OL]. [2021-12-17]. https://privacy.qq.com/document/preview/3fab9c7fc1424ebda42c3ce488322c8a.
[7] National Information Security Standardization Technical Committee. Information Security Technology - Personal Information Security Specification: GB/T 35273-2020[S]. Beijing: State Administration for Market Regulation, Standardization Administration of China, 2020.
[8] Qi Aimin. Research on Personal Information Protection Law [J]. Hebei Law Science, 2008(4): 14-32.
[9] Qi Aimin. Scholar' s Draft Proposal for the Personal Information Protection Law of the People' s Republic of China [J]. Hebei Law Science, 2005(6): 2-5.
[10] Shi Jiayou. The Private Law Dimension of Personal Information Protection—Also on the Relationship Between the Civil Code and the Personal Information Protection Law [J]. Journal of Comparative Law, 2021(5): 14-32.
[11] Yang Lixin. Rules and Application of Damages for Infringement of Personal Information Rights—Interpretation of Key Terms in Article 69 of the Personal Information Protection Law [J]. Journal of Shanghai University of Political Science and Law (Law Review), 2022, 37(1): 1-15.
[12] Liu Xiaochun, Hu Jia. The Personal Information Protection Law Provides an Institutional Foundation for China' s Cross-Border Data Flow [J]. China Foreign Trade, 2021(12): 42-45.
[13] Guo Feng, Chen Longye, Jia Yuhui. Discussion on Several Issues in the Specific Application of the Personal Information Protection Law—From the Perspective of the Relationship Between the Civil Code and the Personal Information Protection Law [J]. Law Application, 2022(1): 12-22.
[14] Wang Liming, Ding Xiaodong. On the Highlights, Characteristics, and Application of the Personal Information Protection Law [J]. Jurist, 2021(6): 1-16.
[15] Gao Xiaoping, Ye Dan. Are Internet Companies Ready for Personal Information Protection? [N]. Southern Daily, 2021-01-01(B02).
[16] Wu Lingfang. Discussion on Medical Data Management and Application Under the Implementation of the Personal Information Protection Law [J]. Soft Science of Health, 2022, 36(1): 5-7.
[17] Zhang Kun. Impact of the Personal Information Protection Law on the Insurance Industry and Recommendations [J]. Tsinghua Financial Review, 2021(12): 88-92.
[18] Wan Fang. The Notice-Consent Principle in Privacy Policies and Its Alienation [J]. Science of Law (Journal of Northwest University of Political Science and Law), 2019, 37(2): 61-68.
[19] Gao Qinwei. Corporate Privacy Policies and Government Regulation in Personal Information Protection [J]. Studies in Law and Business, 2019, 36(2):

16-27.
[20] Zhao Yang, Yan Zhouzhou, Shen Qiqi, et al. Research on Compliance of Healthcare APP Privacy Policies Based on Machine Learning [J]. Data Analysis and Knowledge Discovery, 2022, 6(5): 112-126.
[21] Yao Shengyi, Wu Dan. Research on User-Friendliness Evaluation of APP Privacy Policies [J]. Journal of Information Resources Management, 2021, 11(1): 30-39.
[22] Zhu Hou, Zhang Mingxin, Lu Yonghe. Empirical Research on Social Media Users' Willingness to Read Privacy Policies [J]. Journal of the China Society for Scientific and Technical Information, 2018, 37(4): 362-371.
[23] Li Feng. Research on the Development of WeChat Privacy Policy [D]. Xiangtan: Xiangtan University, 2020.
[24] Dong Lin. Research on Enlightenment from the Revision of User Privacy Policy of the British Library [D]. Dalian: Liaoning Normal University, 2020.
[25] Wen Yuheng, He Yafeng. Cognitive Survey and Correction of Data Property Rights Market Entities [J]. Library Forum, 2022(3): 1-12.
[26] Zhang Yue, Wang Jian, Zhu Qinghua. Research on the Framework Model of Influencing Factors for Medical Consultation APP Privacy Policy Cognition —Based on Grounded Theory Method [J]. Information Studies: Theory & Application, 2019, 42(6): 105-110.
[27] CHARMAZ K C. Constructing grounded theory: a practical guide through qualitative analysis[J]. International journal of qualitative studies on health and well-being, 2006, 1(3): 284-287.
[28] Kathy Charmaz. Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis [M]. Translated by Bian Guoying. Chongqing: Chongqing University Press, 2009.
[29] Jia Xudong, Heng Liang. The "Jungle," Past, and Path of Grounded Theory [J]. Science Research Management, 2020, 41(5): 151-163.
[30] Wu Yi, Wu Gang, Ma Songge. Review of the Origin, Schools, and Application Methods of Grounded Theory—Case Analysis Based on Workplace Learning [J]. Journal of Distance Education, 2016, 35(3): 32-41.
[31] QUESTMOBILE. QuestMobile China Mobile Internet 2021 Half-Year Report [EB/OL]. [2021-12-15]. http://mp.weixin.qq.com/s?**{biz}=MjM5MDk2NzM0Ng==&mid=265153**
[32] Han Shuo. Research on the Impact of the Personal Information Protection Law on APP Privacy Policies - Raw Privacy Policy Data and Coding Process [DS/OL]. Science Data Bank, Knowledge Management Forum [2022-12-29]. DOI: 10.57760/sciencedb.07011.
[33] Cheng Xiao. Expert Interpretation | Important Law for Comprehensive Protection of Personal Information Rights and Interests - Office of the Central Cyberspace Affairs Commission [EB/OL]. [2022-03-04]. http://www.cac.gov.cn/2021-08/25/c_{1631491543035763}.htm.
[34] Yang Heqing. In the Big Data Era, Adding Legal "Protection Locks" to Personal Information [EB/OL]. [2021-12-22]. https://m.gmw.cn/baijia/2021-08/23/1302504877.html.
[35] Supreme People's Court Judicial Case Research Insti-

tute. Interpretation of Key Points in the Application of the Personal Information Protection Law [EB/OL]. [2021-12-21]. http://mp.weixin.qq.com/s?{biz}=MzIxNTYzNzU4NA==&mid=2247525745&idx=1&sn=dcd9936dd667
[36] Zhang Xinbao, Shen Weixing, Cheng Xiao, et al. Multi-dimensional Interpretation and Reflection on the Personal Information Protection Law [J]. China Law Review, 2021, 41(5): 17.
[37] Office of the Central Cyberspace Affairs Commission. Office Release [EB/OL]. [2021-12-25]. http://www.cac.gov.cn/qwfb/bgsfb/A090302index_1.htm.
[38] Pinsent Masons Limited Liability Partnership. About cookie[EB/OL]. [2022-03-18]. https://www.aboutcookies.org/.
[39] Pinsent Masons Limited Liability Partnership. Cookie FAQ' s[EB/OL]. [2022-03-07]. https://www.aboutcookies.org/cookie-faq.
[40] Publications Office of the Union. EUR-Lex - 02002L0058-20091219 - EN - EUR-Lex[EB/OL]. [2022-03-19]. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219.
[41] Proton Technologies Ag. Cookies, the GDPR, and the ePrivacy Directive-GDPR.eu[EB/OL]. [2022-03-19]. https://gdpr.eu/cookies/.
[42] Zhang Xiaobin. Quantitative Evaluation Methods for Law Implementation Effects [J]. Studies in Law and Business, 2006(2): 154-160.

Note: Figure translations are in progress. See original paper for figures.