Article

The Achilles' Heel: the Neglected Bankruptcy-related Terms of Privacy Policies in China

Yaqiong Liu [1], Kaili Du [1], Xiaoxiao Zhang [2,*]

[1] School of Marxism Studies, Central University of Finance and Economics, Beijing, China
[2] Law School, Hunan Normal University, Changsha, China
Correspondence: zhangxx001@foxmail.com

Received: 28 May 2025; Revised: 14 July 2025; Accepted: 12 August 2025; Published: 28 August 2025

Abstract: Against the backdrop of a deteriorating global economy and the pervasive collection of vast amounts of personal health data by mobile applications, the privacy commitments outlined in app privacy policies have garnered significant scrutiny. However, the specific issue of data protection during corporate bankruptcy—particularly concerning bankruptcy-related terms within health app privacy policies—has received scant scholarly attention and remains largely overlooked by the public. This study investigates the unique vulnerabilities of personal health data within bankruptcy proceedings, where existing safeguards are critically inadequate, necessitating urgent regulatory focus. Drawing upon an analysis of privacy policies from 31 top-downloaded health apps on China's Huawei App Gallery and iOS App Store, our research reveals substantial deficiencies in both current privacy policy practices and the supporting judicial mechanisms. Consequently, we propose targeted recommendations for improvement: establishing specific guiding principles for bankruptcy data handling, mandating the integration of robust bankruptcy clauses within privacy policies, and advancing the judicial framework to effectively oversee data protection in insolvency scenarios.

Keywords: privacy policy; bankruptcy; health apps; data transaction; remedies

1. Introduction

In a world full of personal information, it is impossible to ignore the value of data in business. Each application on our mobile phone calls for more personal information in order to offer a more specific and personalized service. This is especially true for applications in the field of personal health management. These applications store a wealth of data with not only personal identification information but also dynamic health information. Additionally, to protect personal data and privacy in a big data society, the mechanism of notice and consent is ubiquitously used in privacy policies. The intensive use of privacy policies attracts the attention of enterprises, legislators and academics. Numerous principles have been proposed to evaluate the effectiveness of the privacy policies and to balance competing rights between users' privacy and the free flow of information. Intensive contributions have been made in this area in order to search for the perfect balancing point between.

Nevertheless, the bankruptcy scenario is missing from mainstream research, particularly in the Chinese academic discourse. When the application continues with proper business, the data will be able to facilitate better service. Yet, the possibility of data leakage is a deadly threat to users' privacy as well, and the concern is especially severe in extreme situations like bankruptcy. This year, 23andMe, a giant in the U.S. genetic testing industry, officially filed for bankruptcy protection. In the 23andMe incident, the genetic profiles of 6.9 million users were sold on the dark web, including pedigree details and health information. This incident exposed the fatal flaw in genetic privacy protection, when the life codes of 6.9 million people were packaged and auctioned, pharmaceutical companies, insurance companies and even AI companies could become buyers of this data, and the

US HIPAA Act could not regulate consumer-grade genetic data. Leaking genetic data can lead to a range of negative consequences, such as insurance discrimination, employment discrimination, and psychological distress. For example, if an insurance company obtains a patient's genetic information, they may increase their premiums or deny coverage based on perceived risk. Similarly, employers may make biased decisions based on an employee's genetic predisposition.

Scholars gravitate toward analyzing the legitimacy, readability and enforceability of privacy policies. However, being the most challenging phase for any company, how the insolvent debtor should comply with its privacy policy is neglected by most contributions whereas the bankruptcy scenario matters drastically to its users. Some scholars have explicitly pointed out that current laws and regulations regarding the obligations of personal information processors when handling user personal information are mostly based on the premise that personal information processors are operating normally, and rarely address what obligations personal information processors should fulfill when they are in bankruptcy liquidation. Therefore, whether the privacy policy contains any provision regarding the bankruptcy scenario and how the provision is drafted is detrimental to the company's behavior when it goes bankrupt. It should be noted that some literature has noted how privacy policies work in bankruptcy proceedings in the United States due to special provisions in the U.S. Bankruptcy Code (Bradley, 2023a). Some scholars examined the empirical practice of privacy policy interpretation and application in U.S. bankruptcy proceedings for further legislative amendments. But this research is in the minority. Besides, little literature focuses on the comparative analysis of the text in privacy policies regarding bankruptcy (Zhao, 2024) scenarios.

In this paper, we intend to analyze bankruptcy-related terms in the privacy policies of typical health management applications in China. By examining the loopholes in the context and application of privacy policies in bankruptcy proceedings, we propose some forward-looking advice based on the findings. The first part of the article explains why bankruptcy proceedings should be assessed separately under the background of data security. Then, we turn to empirical evidence of the status quo in China, and advice based on the analysis is given in the third part.

2. User Data at Edge in Bankruptcy

2.1. Why Bankruptcy Exceptionalism

To discuss user data at edge in bankruptcy, the most fundamental aspect of this research lies on why bankruptcy scenario is different from the ordinary period. It is true that firms licensing, transferring and selling user data in all circumstances, including those in and out of bankruptcies. Hence, the risk of personal privacy leaking happens all the time. According to the 2024 Research Report on Data Security Risks of China's Government and Enterprise Institutions, personal information is the most important type of data for data breaches and black market transactions. Globally, 44.7% of data breaches involve personal information, and the number of pieces of personal information that can be leaked is as high as 34.37 billion. Among the data leakage risk incidents of domestic government and enterprise institutions, 71.8% of the incidents involved personal information, which can cause as many as 26.69 billion pieces of personal information leakage, equivalent to an average of 1.4 billion Chinese can leak about 19 pieces of personal information data per person. Yet, bankruptcy backdrop makes the situation of personal data protection more complicated. The bankruptcy exceptionalism of privacy policies contains two perspectives, including: (1) bankruptcy is the most vulnerable phase of the corporation where user data leaking is highly possible; and (2) bankruptcy law is a lex specialis, thus providing some variance from traditional regulations.

2.1.1 Peculiarity of the Most Vulnerable Phase

The initiation of a bankruptcy proceeding signals a call for guidance and intervention for a dire financial trouble (Warren & Westbrook, 1986). For example, in 2022, during the "dissolution" controversy surrounding Daily Fresh, Chen Bing, Deputy Dean of the Law School at Nankai University and Director of the Competition Law Research Center, expressed concerns about the handling of data from the bankrupt company, which held over 31 million valid user accounts. He

argued that "if user data is mishandled during this process, the primary risk will be privacy breaches, which could severely threaten data security." Internet companies serve as intermediaries connecting resource owners and users, holding vast amounts of data on both operators and consumers. If this data is maliciously stolen or improperly utilized by the platform and leaked, it could result in the disclosure of personal information and critical data, infringing upon individual rights and commercial secrets." When the corporation is still in proper operation, it would be a rational choice for it to comply with data protection regulations due to several reasons. First, it has sufficient technical ability and financial support to protect user data. Second, the income of the corporation comes from the use of user data, thus making the user data a valuable asset worth protection. Third, the punishment when violating data protection rules would overweight the profit of unreasonable use of the data. Despite the subsidy, if the company becomes bankrupt due to severe financial distress, insufficient capital may hinder its ability to fully resolve all creditor claims, let alone allocate funds for user data protection expenses (Qu, 2024). In 2024, U.S. electric vehicle startup Fisker filed for bankruptcy, and Fisker reached an agreement with buyer American Lease to bundle and dispose of "vehicle assets + data services." Fisker sold over 3,000 inventory vehicles and cloud access rights for $46.25 million. To ensure the integrity of vehicle data and the functionality of vehicle software updates, American Lease paid an additional $2.5 million for five years of technical support services, thereby preventing data loss due to server shutdown. This can be considered a practical example of data handling. However, this is an exception. Typically, when bankrupt automakers cease paying cloud service fees, cloud providers typically shut down servers in accordance with contract terms. This not only prevents vehicle owners from accessing historical data (such as charging records and OTA update logs) but may also result in permanent data loss due to missing data migration. At the bankruptcy stage, all of the above reasons supporting proper user data protection mechanism are hanging by a thread.

On the one hand, technical and financial constraints have led to a lack of objective capabilities. Security systems are both technology-intensive and capital-intensive, and after bankruptcy, the company lacks the objective capabilities to protect user data. According to the standard of bankruptcy, a company is in the stage of insolvent if it could not repay its due debts. At this particular phases, any expense of the company should be reviewed carefully since it may be detrimental to its continuity. In order to stay in business, the company would strive to survive by making every penny counts. Data security costs can potentially place a significant burden on companies experiencing financial difficulties, as they must bear the financial burden of technical service costs, maintenance labor, and research and development costs. Such financial demands can dramatically affect companies' cash flow, exacerbating their existing financial challenges, potentially leading to further financial distress.

On the other hand, the effectiveness of the punishment mechanism leads to a lack of subjective willingness. During the liquidation phase, companies have no incentive to protect data and the punishment is effective, so they lose the subjective willingness to protect data. After entering the insolvent phase, the company would no longer rely on user data for its future gains. Moreover, once the liquidation process has been initiated, the dissolved company no longer exists and therefore ceases to have corporate capacity. For example, in many cases of bankruptcy liquidation involving live streaming platforms, administrators directly shut down servers and destroy user data without facing any legal consequences. Hence, no matter how severe the punishment is, the penalty could hardly be of any threat to the company.

Consequently, the bankruptcy stage of a company contrasts significantly with its operational phases, with user data being particularly vulnerable during this period, due to the company's reduced ability to guarantee protective measures. To uphold users' fundamental privacy rights, specific measures are necessary to address the unique challenges associated with bankruptcy, the company's most vulnerable phase.

2.1.2. Lex Specialis Prevails

In bankruptcy proceedings, the adjudicating process aims for a "rough justice" rather than to comply with "stringent requirements" (Seymour, 2022). In order to reach a careful balance between

the basic rights of all related parties and the advancement of the bankruptcy estate valuation, the rules in bankruptcy law offers some exceptions and breakthroughs based on the fundamental laws. In some instances, the bankruptcy court and its judges have adopted several innovative approaches to resolve the dilemmas inherent in bankruptcy proceedings. These creative and flexible measures are appraised and employed especially in reorganization process for the rescue of the companies. As a formal legal mechanism, bankruptcy typically takes precedence over regular law, particularly in circumstances deemed exceptional.

In the Chinese Enterprise Bankruptcy Law, several provisions adjust the ordinary procedures in the Civil Code, Civil Procedure Law and other Legislations. For instance, Article 19 requires all preservation measures and executive programs to be suspended after the initiation of the bankruptcy proceeding, and Article 20 asks all civil actions and arbitration related to insolvent debtors to be discontinued. Another example is Article 21, the bankruptcy law provides that only the court where the bankruptcy proceeding is initiated should have jurisdiction over relevant civil litigation related to the insolvent debtor. This provision overturned the jurisdiction rules in the Civil Procedure Law.

Therefore, the situation where bankruptcy proceeding takes the lead should be considered separately due to its special legal practices. Unique aspects of the Chinese Enterprise Bankruptcy Law do not always align with other laws, and as such, the application of these special rules may potentially affect the outcome of bankruptcy proceedings. This discrepancy becomes particularly significant when conflicts arise between the bankruptcy law and one or more traditional rules. When determining the applicable rules of user data transactions, bankruptcy exceptionalism is highly necessary since the practice of the insolvent company may ignore the protective requirements coded in other laws, especially when the applicable regulation during the phase is vague and uncertain.

2.2. Lost in Legislation

Aside from the action in practice, special requirements are also indispensable in the legislation. The goal of the bankruptcy law and the privacy protection law is not easy to coordinate since bankruptcy seeks efficiency while privacy protection searches for equity. The confrontation between these laws also arises in the legislation in China since the data security in bankruptcy scenario is fully examined neither in privacy legislation nor in bankruptcy legislation. The inadequacy of this situation in China can be seen within the realm of two primary areas: (1) data security law failed to incorporate the unique features associated with bankruptcy, while the bankruptcy statute ignored privacy safeguards; and (2) neither privacy legislation nor bankruptcy law adequately addressed the role and the nature of privacy policies.

Privacy protection legislation primarily concentrates on data security during conventional operation processes, but is limited in terms of bankruptcy references, providing limited, generally brief references. These references lack thorough, detailed explanations. As such, the provisions surrounding bankruptcy in data protection law are basic and imprecise, resulting in a lack of clarity in the practical implementation of bankruptcy law and its relationship to privacy protection. The existing framework remains unstructured and lacks any established guidelines.

The three most important data protection regulations in China are Personal Information Protection Law, Data Security Law and Web Security Law. In these three legal documents, only one article has mentioned the word bankruptcy in Personal Information Protection Law, whereas the other laws ignore the bankruptcy circumstance completely (see Table 1).

Moreover, challenges exist in the application of bankruptcy law as well, with the most crucial issue on the determination of a definitive ambit of the debtor's estate. The scope of the bankrupt estate in China is determined according to Chapter 4, from Article 30 to Article 40, of the bankruptcy law and the Provisions of the Supreme People's Court on Several Issues Concerning the Application of the Enterprise Bankruptcy Law of the People's Republic of China (2). As the Chinese Enterprise Bankruptcy Law is enacted in 2006 before the take-off of the internet and mobile application in recent decades, the problem of user data transaction has not attracted any attention in the bankruptcy legislation. Generally speaking, the rules in the Chinese Enterprise Bankruptcy Law

illustrate that all assets of the debtor are bankrupt estate and does not exclude user data from the estate. However, while various intangible assets have been appropriately treated in earlier bankruptcy proceedings, there has been no judicial precedent in China that has recognized user data as part of the estate (Chen, 2023). Therefore, neither the regulation nor the judicial precedent is able to provide sufficient support for ruling. This legal vacuum has given rise to a series of issues. Users' avenues for redress are systematically blocked. When data is classified as bankruptcy assets, individuals cannot exercise the right to delete data as stipulated by the Personal Information Protection Law nor assert their claims as creditors. Judicial practice has explicitly denied the status of data rights as bankruptcy claims; simultaneously, the risk of data abuse has intensified, as administrators can package and monetize user data to offset debts. Real-world cases indicate that post-hoc notification mechanisms often become mere formalities; More critically, judicial rulings exhibit significant inconsistencies, with some courts recognizing the property attributes of data while others deem it a worthless byproduct. Such divergences constitute institutional loopholes in the bankruptcy order of the digital age.

Table 1. Rules regarding bankruptcy in privacy protection regulations in China

Legislation	Bankruptcy Clause	Related Regulations	Article Reference
Personal Information Protection Law	√	Article 22 Where a personal information processor needs to transfer personal information due to combination, division, dissolution or declaration of bankruptcy, among others, it or he shall notify individuals of the name and contact information of the recipient. The recipient shall continue to perform the obligations of the personal information processor. If the recipient changes the original purposes or methods of processing, it or he shall obtain the individuals' consent anew in accordance with this Law.	Explicit bankruptcy obligations
Data Security Law	×	Null	N/A
Cybersecurity Law	×	Null	N/A

2.3 Data Asset Recognition in Judicial Practice

The practice of Chinese courts in identifying user data as an intangible asset in bankruptcy cases faces complexity and uncertainty due to legislative gaps. Although Article 30 of the Enterprise Bankruptcy Law broadly defines the bankruptcy estate as the "entire property" of the debtor, there is a lack of clarity on whether and how it applies to user data, especially personal information. The courts lack clear statutory guidance on determining whether aggregated user data constitutes a company's proprietary intangible assets, and whether its value is subject to contractually permissible or restricted personality rights (Ou & Zhang, 2024).

In practice, the courts have shown pragmatism but mixed attitudes. In restructuring cases involving technology companies, courts and administrators often default to the value of user data assets and prefer to choose buyers who can maintain the operation of the platform, but have always avoided formally classifying them as intangible assets subject to valuation and distribution in the bankruptcy estate. In liquidation, these assets are often abandoned due to valuation transfer difficulties and privacy concerns (Zhao, 2024). This judicial hesitation and lack of standards highlights the gap between the theoretical value of data and its current practice as an operational asset class in China's bankruptcy law. The lack of legislative definitions and the lack of judicial

recognition standards make the fate of user data in bankruptcy more dependent on individual discretion than clear legal principles.

The deeper dilemma stems from the value conflict between data protection rights and the objectives of insolvency proceedings. The rights and interests of users' personal information are the basic rights established by the Personal Information Protection Law, which requires data processing to comply with the principles of purpose limitation and minimum necessity. Bankruptcy laws, on the other hand, focus on maximizing the interests of creditors and tend to treat data as property that can be freely disposed of. This tension has led to courts being forced to "value ranking" in individual cases - when data assetization may threaten user privacy, such as the transfer of raw data to a third party, administrators often choose to abandon the disposal. The current system does not establish special rules for bankruptcy data protection similar to the EU GDPR, nor does it lack a quantitative assessment mechanism to coordinate the two values, resulting in an "all or nothing" binary dilemma.

3. Inadequate Status Quo in Bankruptcy Practice

Given the uncertain nature of user data transactions in bankruptcy proceedings, inconsistent application of bankruptcy exceptionalism and legislative gaps contribute to the current limited and flawed bankruptcy practices. This section intends to illustrate the problem with real life data from China by examine materials in the following two areas: (1) privacy policies of health management applications in China, and (2) faulty judicial practices relating to bankruptcy scenarios.

3.1 Inadequate Privacy Policies

3.1.1 Research Process

In order to have a first-hand understanding of the status quo, we conducted a study regarding the privacy policies of the top health management applications in China to examine their practice in bankruptcy scenarios. This study consists four stages: (1) forming the research questions to be tackled in the research, (2) selecting health apps from Huawei App Gallery (Android) and IOS App Store (Apple), (3) manually sorting out bankruptcy-related terms in the privacy policies of the selected applications, (4) examining data results and discussing data implications.

The data selected for this analysis were made up of the privacy policies of multiple health management applications in China. The dataset is chosen for two reasons: (1) the health management applications contain numerous sensitive personal data of the users which requires strict limitation for transaction; and (2) these applications are obliged to have thorough privacy policies in order to land on any application market. Most health management applications obtain substantial personal information through multiple means, including: (1) users provide basic information such as height, weight, age, etc.; (2) applications obtain information with users' consent through other hardware like phones, bracelets, scales, etc.; (3) applications track and analyze users' personal preferences without users' specific consent. In conclusion, the privacy policies of health management applications are a compelling case study for future privacy policy analysis.

This study targets the most popular mobile health apps with most downloads on two major platforms in China: the Huawei App Gallery and the IOS App Store. According to these two platform guidelines, all apps uploaded should include its privacy policy as its public information, and users could access these documents as they wish. Hence, the privacy policies used in the study are collected based on the privacy policies openly publicized by the apps.

This research paper is based solely on the "Top 30 App List" in both the Health and Fitness category and the Medical category in China that was available as of June 30, 2023 (asdetailed in Table 2), and includes data from both app platforms. The apps chosen are the ones that appear in the aforementioned lists from both Huawei (Huawei App Gallery, 2023)and IOS (Apple App Store, 2023). Of the 31 apps identified, 13 (41.94%) were in the healthand fitness category, while 18 (58.06%) were in the medical category. Apps that only appeared on either Huawei's list or IOS's list were not included.

This study evaluated mobile health applications for their bankruptcy-related terms in privacy policies, and these terms were carefully classified and arranged in a logical sequence based on the following three aspects: privacy protection, bankruptcy proceedings, and remedies. This can be seen in Table 3.

Table 2. Selected health apps for the study

	Health & fitness			Medical		
No.	App name	Huawei Rank	IOS Rank	App name	Huawei Rank	IOS Rank
1	Huawei health	1	4	Ping An Health	1	22
2	Keep	2	1	National Medical Insurance Service Platform	2	14
3	Daily Rope Skipping	3	13	Xiao Dou Miao	3	5
4	Ding Dong	4	26	Good Doctor Online	4	1
5	Zepp Life	5	10	You Jian Kang	5	4
6	Yue Dong Quan	6	27	Yue Miao	6	6
7	Yue Pao Quan	7	39	Wei Yi	8	21
8	Daily Yoga	8	20	Ark Health Online Pharmacy	9	18
9	WillGo	14	37	Health 160	10	15
10	Wearfit Pro	16	12	Wei Mai	11	39
11	Lovefitt Sport	18	25	Ding Xiang Doctor	13	13
12	Sweating Dance	20	16	Yi Lu	14	19
13	Xun Ji	21	38	Ding Dang Fast Medicine	15	23
14				Hua Yi Tong	16	16
15				Beijing Children's Hospital	18	33
16				Beijing Xiehe Hospital	20	3
17				Tianjin Medical Insurance	23	17
18				Ai Kang Health Checkup	24	28

3.1.2. Evaluation Results

Research Question 1: whether there are any bankruptcy related terms in app privacy policies?

Extracted data reveals that 21 of the 31 privacy policies reviewed in this study contain bankruptcy-related terms. Of the 31 apps analyzed, 67.74% noted the necessity to address bankruptcy as a unique scenario within the data protection provisions. However, since few users actually read and understand privacy policies thoroughly, Ullah et al. (2022) relying on non-regulatory privacy policies is not a satisfactory solution to resolve the dilemma between privacy protection and bankruptcy value maximization (Kreuter et al., 2020). Therefore, in bankruptcy proceedings, the privacy policy of health apps should be ethically interpreted and monitored by legal professionals to ensure user privacy.

The American congress recognized the legislation gap decades ago and passed Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (Williams et al., 2005). In this legislation, the consumer privacy ombudsman regime is established to settle the battles over personal private data transactions in bankruptcy cases (Coordes, 2021). As per the current status of the U.S. Bankruptcy Code, the privacy policy of an application is the first point to be considered by the bankruptcy court when evaluating the feasibility of a personal data transaction (Bradley, 2022). This regulation works in parallel with the Health Insurance Portability Accountability Act in protecting

health apps private data. Moreover, the enactment of these laws has raised awareness among U.S. companies about the criticality and importance of maintaining comprehensive and transparent privacy policies.

Table 3. An overview of the privacy policies examined

No.	App Name	Bankruptcy-related terms	Dedicated Bankruptcy Clause	Data asset transactions allowed
1	Huawei health	No	No	Yes
2	Keep	Yes	No	Yes
3	Daily Rope Skipping	No	No	Yes
4	Ding Dong	Yes	No	Yes
5	Zepp Life	No	No	No
6	Yue Dong Quan	Yes	No	Yes
7	Yue Pao Quan	Yes	No	Yes
8	Daily Yoga	Yes	No	Yes
9	WillGo	Yes	No	Yes
10	Wearfit Pro	No	No	Yes
11	Lovefitt Sport	Yes	No	Yes
12	Sweating Dance	Yes	No	Yes
13	Xun Ji	No	No	No
14	Ping An Health	No	No	Yes
15	National Medical Insurance Service Platform	Yes	No	Yes
16	Xiao Dou Miao	No	No	Yes
17	Good Doctor Online	Yes	No	Yes
18	You Jian Kang	Yes	No	Yes
19	Yue Miao	Yes	No	Yes
20	Wei Yi	Yes	No	Yes
21	Ark Health Online Pharmacy	Yes	No	Yes
22	Health 160	Yes	No	Yes
23	Wei Mai	Yes	No	Yes
24	Ding Xiang Doctor	Yes	No	Yes
25	Yi Lu	Yes	No	Yes
26	Ding Dang Fast Medicine	No	No	Yes
27	Hua Yi Tong	Yes	No	Yes
28	Beijing Children's Hospital	Yes	No	Yes
29	Beijing Xiehe Hospital	Yes	No	Yes
30	Tianjin Medical Insurance	No	No	Yes
31	Elken Health Checkup	No	No	Yes

Although the Chinese Bankruptcy Law does not explicitly address privacy policies, many apps have recognized the potential utility of a privacy policy as a means to transfer personal data in the event of bankruptcy proceedings, provided the prior consent of users. This can be a major problem for all users of these apps as they barely understand what they have agreed to in the privacy

policies. Accordingly, to offer a better protection for the vulnerable group of the users, some regulations addressing supervision over bankruptcy-related terms in privacy policy should be added in the Chinese Bankruptcy Law and relevant data protection laws for better resolving the problem.

Research Question 2: is user data protection and transfer term in bankruptcy drafted with a separate term clearly?

While 21 out of 31 apps include a bankruptcy-related term in their privacy policies, none of them drafts the user data protection and transfer term individually and separately with sufficient details. Moreover, even for those with bankruptcy-related terms carved in the privacy policies, the language and wording used in the privacy policies are vague and ambiguous, leaving abundant room for interpretation. Besides, the bankruptcy-related term is often drafted with other major items and the terms are commonly written as follows: if your personal data should be transferred as a part of a deal, including merger, acquisition, reorganization, spin-off, bankruptcy, asset transfer or other similar transactions, we would inform you with the name and contact information of the receiver and ask the counter-party to shoulder the responsibility of data protection.

For instance, the term in Keep's privacy policy which is one of the most detailed ones among our chosen apps states that "should the need arise for the transfer of personal information due to any circumstances such as mergers, divisions, dissolution, bankruptcies, etc., we will respectfully inform you of the recipient's name, personal details and contact information, and we will accordingly request the recipient to continue to fulfill the obligations of a personal information processor. Should the recipient change the original purpose or method of processing the above-mentioned personal information, we will require your renewed consent. Important changes referred to in this policy include, but are not limited to, major changes in our ownership structure, organizational structure, etc., such as changes in ownership due to business adjustments, bankruptcies, mergers and acquisitions, etc." While this term seems to correlate with rights and obligations, numerous pitfalls remain. First, when and how should the users be informed? Second, which form should the renewed consent be acquired? Third, what obligations are included as a personal information processor under the specific privacy policy? Accordingly, interpretations can function drastically under these circumstances.

As shown in the study, some apps have only briefly touched data transfer in bankruptcy with a general rule. Therefore, the apps have not realized that bankruptcy is different from other major transactions and a specifically designed term is in need for bankruptcy situations.

Research Question 3: could the insolvent app companies transfer user data in bankruptcy?

Almost all apps allow transferring user data in bankruptcy transactions, and only one app, Zepp Life, is exceptional. Zepp Life promises to exclude any transaction of data and allows only necessary data sharing. The recent trend has seen user data become increasingly valuable (Collins & Lanz, 2019), and has held especially pivotal position in internet company estate as the Internet companies hold mostly intangible asset (Birch et al., 2021), and its role in the estates of Internet companies has become particularly pivotal. Given that Internet companies primarily hold intangible assets, the majority of apps have come to understand the need to include data assets in their asset portfolios. Therefore, it is recommended to have bankruptcy data transferring terms incorporated in application's privacy policies. Since the transfer of app data may violate consumer privacy in some way, a relevant bankruptcy data transfer term should include both permission and restriction on the sale of data.

Research Question 4: how is data transfer restricted in bankruptcy?

Of the sampled apps with private policies that include bankruptcy-related terms, 21 apps permit user data transactions that may occur during bankruptcy, albeit they all impose certain restrictions on such transactions. In contrast, only 11 apps provide advance notice when they plan to engage in data transactions that may be affected by filing bankruptcy. Moreover, only Beijing Xiehe Hospital requires prior consent before the transactions.

When it comes to data recipients' duties, all 21 apps require a rule that says they must either follow their own privacy policy (as outlined by the company), or follow legal rules (as defined by national or international laws). But the real kicker is that only one app makes both of these rules, saying that data recipients must follow both their own privacy policy and legal rules. This application, named Health 160, highlights the importance of both, stressing the need for all parties involved in the exchange of data to ensure the protection of user privacy and to fulfil all legal obligations. In cases where data recipients plan to change the scope of data collection or the method of processing, the need for renewed consent is mandatory in privacy policies of all apps listed (Table 4). And the results of the percentage distribution are shown in Figure 1.

Table 4. Restrictions on data transfer transactions in bankruptcies

No.	App Name	Notice	Compliance of privacy policies	Compliance of legal duties	Consent required in adjustments
1	Keep	Yes	No	Yes	Yes
2	Ding Dong	No	Yes	No	Yes
3	Yue Dong Quan	No	Yes	No	Yes
4	Yue Pao Quan	No	Yes	No	Yes
5	Daily Yoga	Yes	No	Yes	Yes
6	WillGo	Yes	No	Yes	Yes
7	Lovefitt Sport	No	Yes	No	Yes
8	Sweating Dance	Yes	No	Yes	Yes
9	National Medical Insurance Service Platform	Yes	Yes	No	Yes
10	Good Doctor Online	Yes	Yes	No	Yes
11	You Jian Kang	No	Yes	No	Yes
12	Yue Miao	No	Yes	No	Yes
13	Wei Yi	Yes	No	Yes	Yes
14	Ark Health Online Pharmacy	Yes	Yes	No	Yes
15	Health 160	Yes	Yes	Yes	Yes
16	Wei Mai	No	Yes	No	Yes
17	Ding Xiang Doctor	No	Yes	No	Yes
18	Yi Lu	Yes	Yes	No	Yes
19	Hua Yi Tong	No	Yes	No	Yes
20	Beijing Children's Hospital	No	Yes	No	Yes
21	Beijing Xiehe Hospital	Yes	No	Yes	Yes
	Total Percentage (%)	52.38	71.43	33.33	100

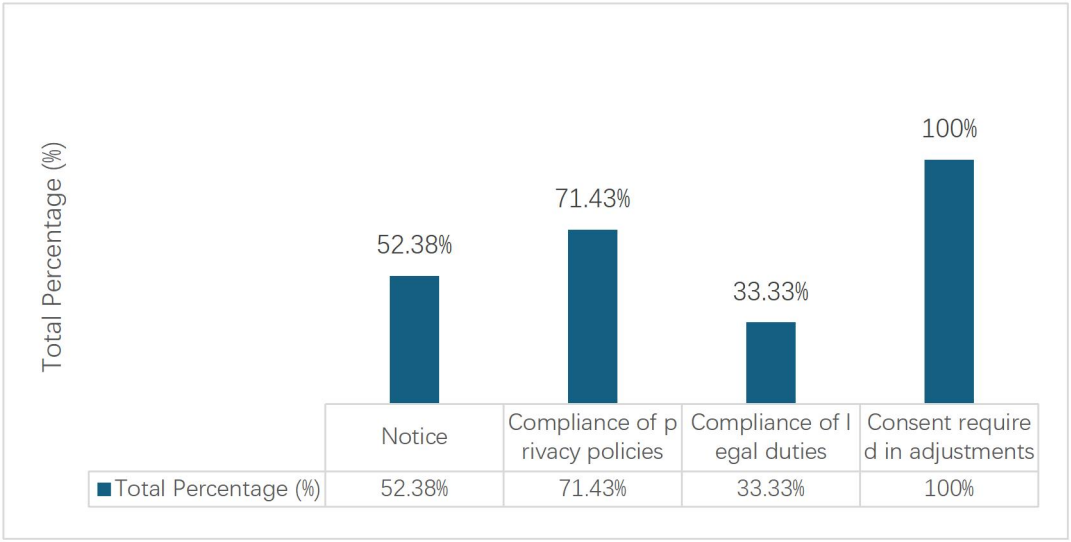

Figure 1. Assessment results of bankruptcy-related provisions in the privacy policy of mobile health applications

It should be noted that the privacy restrictions emphasized in the health app privacy policies are in line with existing privacy and data protection legislation in China. However, the drawback lies in the legislation gap in China. While no consistent and well-established qualified buyer standard has been recognized in China, numerous segmented rules lie within data security law, privacy protection law and antitrust law, all of these fragmented restrictions should be taken into consideration in bankruptcy data transactions. To briefly look at its counterpart in the U.S., a well-structured standard has been illustrated in the Toysmart case where a qualified buyer framework was established to supplement the notice and consent mechanism of privacy policies (Beckmann, 2000). According to the qualified buyer framework in the U.S., the buyer of the data should engage in similar business and comply with previous privacy policy (Bradley, 2022). Although some restrictions still remain unclear and unsatisfactory, the fundamental rules concerning qualified buyers were accepted in the subsequent cases after the Toysmart in America (Bamberger & Mulligan, 2010). Accordingly, a more coherent rule on these issues is in need in China.

Research Question 5: how could users seek remedies if a violation of privacy policies happens in the bankruptcy data transfer?

As privacy laws rise around the world, so do the implementation of corrective measures (Scholz, 2019). An essential part of these measures is the range of recourse options available to customers experiencing privacy violations. In this study, we reviewed the privacy policies of various health apps and found that customers can seek redress through a variety of channels, including account cancellation, withdrawal of consent, deletion of personal information, legal action against the app for breaching privacy policies, or filing a complaint. However, it is worth noting that none of the apps provided a specific remedy for privacy policy violations in the event of bankruptcy.

The concern is that all remedies set out in health app privacy policies rest heavily on the normal function of the app, or the company's commitment to comply with privacy policies following transactions (Bradley, 2023a). Moreover, the remedies set in privacy policies are reckoned to be inadequate even in non-bankruptcy situations (Solove & Citron, 2017). Given bankruptcy situations, existing privacy policies may become unenforceable once a company files for bankruptcy and becomes liquidated or reorganized as the company lacks the ability to shoulder such responsibility anymore. Therefore, judicial remedies specifically designed to curb intrusive privacy actions should be implemented during these complex legal proceedings.

3.2. Inadequate Judicial Mechanism

3.2.1 Absent Presumption

The presumption of data transaction capacity is whether user data is presumed to be transferable or not in bankruptcy proceedings where no consensus is reached in the privacy policy. If users were presumed to consent to the data transaction, the absence of bankruptcy-related terms in the privacy policy would not be a barrier; however, if users were presumed to reject the data transaction without a clear and deliberate intention, the absence of bankruptcy-related terms in the privacy policy would be problematic during bankruptcy proceedings. As illustrated by the analysis of existing privacy policies for typical applications in China, the lack of bankruptcy-related language is not exceptional in practice. In the Bluegogo bankruptcy case, the inability to refund large amounts of user deposits has become the central issue. Additionally, the ownership and handling of user riding data (such as travel routes and personal information) remain unresolved. The company's privacy policy did not anticipate bankruptcy scenarios and did not specify how user data should be handled in such extreme circumstances. During the court proceedings, the primary focus was on recovering assets and repaying deposits. However, the court failed to provide clear rulings or standards on critical issues such as whether user data constitutes bankruptcy assets, whether it can be transferred or sold to settle debts, and how to protect users' privacy rights. This has left user data in a "gray area," with its ultimate handling unclear. This fails to effectively serve the goal of maximizing the value of bankruptcy assets (if the data has value) and also fails to adequately protect users' privacy rights. Therefore, a unified instruction for this situation is needed. However, no specific regulations have yet been issued in China.

Due to the lack of complete instructions, when privacy policies do not contain any terms regarding the bankruptcy scenario, the justification and explanation rests with the judicial authority. Therefore, the presumption applied when privacy policy is absent on the subject is pivotal in the actual judicial process. Bankruptcy proceedings have two main objectives: (1) to manage the estate efficiently and (2) to maximize the value of the estate for a fair distribution among creditors. Privacy rights are considered to be one of the core human rights. The dilemma of presumption stands between the confrontations of bankruptcy and privacy. And it is detrimental to the fulfillment of both bankruptcy and privacy goals.

3.2.2 Lacked Supervision

Aside from the absence of presumption when bankruptcy-related terms are neglected in privacy policies, in bankruptcy cases, the lack of adequate supervision over the disposal of user data instead of its transfer represents another key shortcoming in judicial practice in China. Although this data does not attract potential buyers in liquidation situations or gain recognition during reorganization proceedings, it remains valuable and should not be discarded or overlooked without careful consideration. If user data is mishandled, including without proper disposal supervision or leakage, it can have harmful consequences for these same users. For example, users' personal data could end up being sold on the black market and used in fraudulent activities, going unnoticed until it's too late. A certain e-commerce platform holds a large amount of highly sensitive user data, including payment account information, ID card scans, and detailed transaction records. However, during the bankruptcy proceedings, the court and the administrator did not require the formulation of a reviewed data cleanup plan, nor did they specify that the data should be completely deleted, anonymized, or sealed. The disposal process was completely opaque, and users were not notified or provided with any explanation of the process. The risks were essentially out of control. The opposing party possesses specific order and delivery information, and multiple users encountered precise fraud by counterfeit customer service representatives during the bankruptcy period, strongly indicating internal data leaks. Judicial authorities responded passively, and users who reported data leakage risks did not receive investigations or responses. In such cases, user data is treated as "worthless liabilities" rather than "strictly regulated assets," assuming the administrators act in good faith while ignoring their lack of professional capabilities, particularly the failure to establish mandatory data audit and traceability mechanisms. Inadequate supervision

led to the inability to trace the data after the breach. The core issue is not data ownership but the lack of oversight in the disposal process, ultimately leaving users to bear the consequences of the breach. Given this level of detail, users are more likely to be taken advantage of, deceived or manipulated in these circumstances.

In the bankruptcy arena, judicial supervision is essential for several reasons: (1) The bankrupt debtor is unable to assume further sanction or liability. When the company is liquidated, the life of the company comes to an end and all its assets are fully distributed to creditors. Therefore, if the user data is not properly disposed of, users could hardly ask a dead company to compensate for their loss. (2) The obligation is not owed by anyone because the user data is not transferred. If user data is sold to another buyer, users could always track the buyer if any data leaks occur after the transaction. However, the situation is different when user data is not sold but disposed of. No buyer will be responsible for any data leakage that occurs as a result of disposal. (3) The trustee's obligation may not adequately cover the data protection obligation. First, it is well recognized that the responsibility to protect the value of property and to exercise due diligence in the bankruptcy proceedings is laid down in the bankruptcy legislation. However, it is questionable whether the protection of user data is part of the ambit of the liability. Second, while data protection regulations impose obligations on data processors, the definition of a data processor is still uncertain in bankruptcy proceedings. Whether the bankruptcy trustee is recognized as the data processor, the delegation of the data processor or the intermediary agency in data transactions is debatable in China because all laws are silent on this issue. Accordingly, the inadequacy illustrated in these three perspectives calls for strong oversight with a neutral stance.

From the above analysis, it is evident that China's current bankruptcy procedures have significant institutional gaps in protecting user data privacy. On the one hand, mainstream privacy policies generally ignore data disposal rules in bankruptcy situations, resulting in a lack of user authorization and unclear responsibilities. On the other hand, judicial mechanisms have systemic deficiencies in data presumption, such as ownership determination and supervision of the disposal process, making bankruptcy procedures a "legal gray area" with high privacy risks and difficult remedies. These deficiencies not only undermine users' fundamental rights but also hinder the orderly disposal and realization of the value of data assets in bankruptcy. Given that these critical shortcomings have become core obstacles in practice, it is imperative to establish a systematic solution. Therefore, targeted improvements must be implemented at multiple levels.

4. Proposed Improvements

4.1 Specified Principles

4.1.1 Privacy vs. Bankruptcy - who holds the trump card?

Ultimately, the central dispute underlying the unresolved issues between privacy and bankruptcy laws centers on a crucial conflict between justice and practical concerns. In order to fully address the contradiction between bankruptcy and user privacy, it is imperative to first establish fundamental principles before delving into specific issues. Indeed, the divergence between privacy principles and the objectives of bankruptcy proceedings is brought to light in the context of user data transactions. While privacy rules serve as a check on the unrestricted trade in personal information, bankruptcy proceedings often necessitate flexible user data transactions to maximize the value of the estate. This is particularly relevant for companies that use customer databases as their most expensive and important asset (Miller Jr & O'Rourke, 2001).

4.1.2 Nature of Privacy Polices in Bankruptcy

Despite many criticisms of the implications of privacy policies in the digital world, these policies remain the most critical and vital resource when it comes to resolving disputes and issues. Unfortunately, the nature of privacy policies remains somewhat unclear due to a number of factors.

One of the most significant reasons for this ambiguity is the huge diversity of privacy policy formations that currently exist. Typically, the main two means to poster a privacy policy are: (1) to

post it on the application website; and (2) to pop-up on an interactive page of the applications. Hence, the privacy policy is most likely to be classified as contracts, disclaimers or compliance rules. With it posted on the website, the privacy policy seems to be more of a disclaimer or statement as it represents a unilateral declaration of intent of the application. Yet, the pop-up form of the privacy policy seems to offer users an opportunity to accept the terms, making it more like a contract. In addition to these two views, some argue that the privacy policy to be a compliance rule that the administrative authority could regulate the application on the basis of the privacy policy. Moreover, some scholars convey that the privacy policy should contain all of the above in order to function properly (Ding, 2023). This paper tends to argue that privacy policies should primarily be interpreted as contractual relationships, as their core function is to establish a framework of rights and obligations between users and platforms regarding data processing, and they rely on some form of user consent, even if merely by clicking "agree", which constitutes the foundation of a contractual relationship. Although its standardized format and non-negotiable nature give it unique characteristics, such as those of a standard form contract, classifying it as a contract is most advantageous for providing clear remedies for breach of contract when user rights are violated, especially in critical scenarios such as bankruptcy.

On one hand, the nature of the privacy policy may be a determining factor in assessing whether a breach of the privacy policy can be rectified. If the privacy policy were a disclaimer, an individual user could hardly obtain any remedy because it is a unilateral promise. Yet, the remedy would be much clearer if the privacy policy were a bilateral contract since the user could always defend his or her rights with the breach of contract. However, either disclaimer or contract could make privacy policy the cornerstone of any administrative penalty.

On the other hand, vagueness in privacy policies can significantly affect how user data should be treated. Being a statement means that the privacy policy is not binding, and the court could not rule based on the privacy policy in bankruptcy proceedings. However, even if the privacy policy is treated as a contract, it still faces multiple outcomes in bankruptcy proceedings. First, because the privacy policy is drafted by the application and can not be negotiated and modified by the users, the privacy policy may be classified as a standard form of contract. Second, changes to the privacy policy may be ex parte for some applications. The validity of the terms subsequently modified without the user's consent is questionable. Therefore, the version of the privacy policy is crucial for these situations. Third, the bankruptcy law gives the trustee a special right to determine the validity of any executory contract signed by the insolvent debtor. The executory contract, also refers to the current contract in the European Insolvency Regulation, is “an agreement where 'the obligations of both the bankruptcy and the other party are so far unperformed that the failure of either to complete performance would constitute a material breach excusing performance of the other'” (Chuah & Vaccari, 2023). The question would be: if a privacy policy is considered a contract, could it be classified as an executory contract in bankruptcy? If the answer is yes, could a trustee terminate this contract without the consent of the users?

In the absence of specific privacy or bankruptcy legislation on this issue in China, the responsibility for determining how the concept of privacy policy should be applied in bankruptcy proceedings falls squarely on the shoulders of the court.

4.2 Improved Privacy Policies

4.2.1 Integrated Bankruptcy-related Terms

The content of privacy policies matters dramatically in bankruptcy proceedings, as it comes first when the court intends to make an informed decision on the transaction of user data. Without a well-written term for data protection in bankruptcy proceedings, the bankruptcy judges would have to use their discretion on the issue. Yet, users should have broad autonomy over whether they allow their data to be sold. Only Zepp Life provides data transfer veto rights, proving that users' right to choose is practical and that the user authorization mechanism is feasible. Hence, an integrated bankruptcy-related term in the privacy policy is necessary.

On the one hand, to have a negotiable term for data transactions in this particular scenario not only complies with the "notice-consent" mechanism incorporated into personal privacy legislation, but also provides data providers with autonomy over their use of personal data. If consent to the transaction is obtained in the privacy policy, it would be helpful to sell user data properly and efficiently during bankruptcy proceedings, thus increasing the total value of the estate. This is not only beneficial to the application in bankruptcy proceedings, but also beneficial to the valuation of the company in the normal course of business. Because the bankruptcy-related term in the privacy policy eliminates the company's data asset transaction risk and facilitates the exit of the investment, the valuation amount could be altered by this detail.

On the other hand, a separate draft insolvency term should contain several elements. First, if the user agrees with the data transaction in a bankruptcy proceeding. Second, under what circumstances and requirements could the transaction be carried out. Third, which remedy could the data provider seek if the bankruptcy application violates its liability. These provisions would be helpful in providing essential sources for users to protect their basic rights.

The following is an example of model bankruptcy provisions to illustrate the characteristics of good provisions:

Article [X] Processing of User Data in Bankruptcy or Similar Proceedings

1. Consent and Scope: You hereby expressly acknowledge and agree that if [Company Name] enters into bankruptcy liquidation or reorganization proceedings (hereinafter collectively referred to as "Bankruptcy Proceedings"), the administrator or related parties may treat the personal data you have provided and stored on this platform (as defined in Section [X] of this Policy) as part of the company's assets for disposal, including but not limited to sale, transfer, or licensing (hereinafter referred to as "Bankruptcy Data Transactions").

2. Terms and conditions of the transaction:

a. Anonymization requirements: Before any bankruptcy data transactions are implemented, your personal data must be thoroughly anonymized to the extent that it cannot be identified or associated with a specific individual, and this process must be irreversible.
b. Qualifications of the transferee: The data transferee must prove to the administrator that it has data protection standards and security measures that are equivalent to or higher than those promised by [company name] under this policy.
c. Purpose Restriction: The transferee shall use the anonymized data solely for the purposes necessary to complete the distribution of bankruptcy assets, or for purposes directly related to [company name]'s original services and reasonably expected by you, and shall not use the data for any other unrelated purposes or purposes not agreed to by you.

3. User Rights and Remedies:

a. Right to know: In the event of a bankruptcy data transaction, the administrator shall notify you of the basic details of the transaction (such as the name of the transferee, the scope of the data, and the anonymization status) through reasonable means (e.g., the email address you registered or in-app announcements).
b. Objections and Remedies: If you have reasonable grounds to believe that these terms have not been complied with (e.g., data has not been sufficiently anonymized, or the transferee does not meet the qualifications), you have the right to raise objections to the administrator and the competent court, and may request the suspension of the transaction, the deletion of data, or seek other damages permitted by law.

4. Amendment of Terms:

Any material amendment to these Terms (such as expanding the scope of transactions or lowering protection standards) shall require your prior express consent prior to the commencement of bankruptcy proceedings.

Accordingly, the inclusion of a separate and comprehensive clause in the bankruptcy arena privacy policy is beneficial not only to the application but also to the users of the application. In

addition, bankruptcy-related terms in the privacy policy are vital not only for bankruptcy proceedings but also for relevant tort proceedings.

4.2.2 Clarified Interpretation

In practice, having a different understanding of the same term in a privacy policy is unavoidable. This problem would be exacerbated by the scarcity of prior practice and inadequate regulation, as is the case in the bankruptcy proceedings in China.

Firstly, while the privacy policy is primarily in the form of a contract, it is not an ordinary contract. In a contract where there is total agreement between the parties, the terms of the contract should be explained according to semantics only. However, since the privacy contract is drafted solely by the application, the explanation should be directed to those who have not drafted the content. While users express their consent when using the app, they rarely read, let alone protest, the content of the privacy policies. Hence, the power to interpret the contract should be shifted to balance the rights of the participating parties.

Secondly, the contract should be explained on the basis of the principle of protecting the weaker. In real life, privacy policies are written without full discussion, negotiation and consensus from users. And the terms of privacy policies are often ambiguous and difficult to understand (Bradley, 2023b), which requires interpretation in bankruptcy proceedings. Based on this background, the interpretation of the contract could hardly be objective or neutral in the usual way without any prejudice. Explaining the contract in terms of user preference would better serve the purpose of fairness and consistency.

With clear and consistent interpretation of privacy policy principles, it is important in the bankruptcy proceeding as it would help both efficiency and fairness. On the one hand, the principle narrows the interpretation gap between the parties, reduces the risk of disputes, and provides a solid basis for judicial decision, thus increasing the efficiency of bankruptcy proceedings and reducing the duration of litigation. On the other hand, with user-friendly protection, it could bring the parties to a more balanced position and avoid further injustice. This is especially important as privacy data has a huge impact on users' daily lives and should not be given up easily.

4.3 Improved Judicial Mechanism

4.3.1 Constructive Refusal

The presumption is crucial for user data transactions in bankruptcy applications. The presumption could be divided into three categories: (1) presumed transactionable, (2) presumed transactionable with supplementary consent, and (3) presumed non-transactionable. According to the first assumption, if user data are allowed to be sold in liquidation or transferred for reorganization, the value of the estate could be realized efficiently and the total value of the estate could be maximized. Such a presumption would be preferable for the bankrupt debtor. Yet, this presumption would infringe on users' privacy rights. According to the second assumption, if the user data is allowed to be managed with supplementary consent, the value of the estate could still be maximized with the value of the user data and the user's right to privacy is respected. However, the value of the estate may depreciate to some extent during the acquisition of consent as the user data could not be sold immediately. According to the last assumption, if the user data is not allowed to be sold or transferred in the event of bankruptcy, the user privacy can be fully protected. Yet, the goal of bankruptcy, maximizing the value of the estate, cannot be achieved. This is particularly problematic when the bankrupt debtor primarily holds user data and related digital assets. Creditors' rights could not be protected.

It could be easily identified with the comparison in Table 5. None of the assumptions could fully satisfy the objectives of bankruptcy as well as the goal of privacy protection. In order to strike a balance between the goals, the target priority ladder should be established. However, the priority among these goals is different in each country. For example, while the European Union prefers privacy, the United States favours efficiency. To adequately protect both sides, the presumption

when there is no explicit statement should be understood as a lack of consensus. However, this presumption could be refuted with an additional consent of the users.

Table 5. Evaluation of the Aims Fulfilled under Different Presumptions

Legislation	Aims	Transaction Allowed	Transaction With Consent	Transaction Denied
Bankruptcy Law	Efficiency	√	×	×
	Value Maximization	√	Uncertain	×
Data Protection Law	Privacy Right	×	√	√

4.3.2 Disposal Supervision

While bankruptcy is the most vulnerable process in a company life, the process of disposing of unwanted personal data is the most neglected of all. At this stage, the responsibility for the disposal of the remaining personal data rests with the trustee. However, the trustee is only responsible for data protection during the bankruptcy proceedings, and the remaining data has no other person in charge during the bankruptcy proceedings. In practice, trustees are mainly intermediary agencies such as lawyers and accountants in China. These agencies, while enjoying some credibility with the public, have neither the authority to face the public nor the professional capacity to evaluate data processing. Therefore, it would be more reliable to have an official authority to oversee the data disposal process.

In bankruptcy proceedings, the adjudicating court may be the best choice to oversee data disposal in China. For one thing, the judiciary enjoys a well-known reputation and credibility among the public. First, being an objective and impartial party, the judiciary would not attempt to reduce the cost of disposal. Secondly, the disposal of user data is linked to the public interest, and the judicial authority cares more about the public than the private party. On the other hand, the court has the best knowledge of the case. The judicial authority not only obtains the full information of the users' data, but also realizes how much money could be used to dispose of the data. With a thorough understanding of the situation, the judicial authority would be able to monitor the disposal process appropriately.

However, relying solely on judicial oversight has its limitations. Judicial authorities typically lack the specialized technical capabilities required to assess whether personal data has been completely and securely destroyed, such as verifying the thoroughness of storage medium erasure or physical destruction. Therefore, under a court-led supervision framework, it is more reasonable to introduce local information technology regulatory agencies, such as cyber administration departments, to provide specialized technical support. The involvement of technical departments can ensure the scientific and reliable assessment of data destruction, addressing the technical shortcomings of judicial oversight.

Looking internationally, South Korea operates under an independent regulatory-led model. The country's data processing activities, including those related to bankruptcy, are primarily supervised by its independent Personal Information Protection Commission (PIPC). The PIPC possesses robust technical capabilities and enforcement authority, enabling it to independently issue guidelines, conduct investigations, and impose penalties. In bankruptcy scenarios, the PIPC requires administrators to submit detailed data disposal plans for review and filing, with the disposal process and outcomes also reported to the PIPC. Its advantages lie in its high level of specialization and centralized authority; however, its independence from the judicial system may limit its coordination efficiency with bankruptcy proceedings. The EU adopts an embedded data protection officer (DPO) model. The EU GDPR requires data controllers, including bankruptcy administrators designated as processors, to appoint a Data Protection Officer (DPO). During bankruptcy proceedings, the DPO is responsible for overseeing data protection compliance,

including the disposal phase. The DPO must possess specialized knowledge and report to regulatory authorities. Its advantages include having a dedicated technical role embedded in the process; however, the DPO is appointed by the administrator, which may result in limited independence and oversight, and its primary role is to provide compliance advice rather than enforce strict regulations.

Compared to the South Korean model, which is led by an independent agency and supervised by EU commissioners, China's proposal involves courts exercising core supervisory authority to ensure procedural fairness and clear responsibilities, while introducing external professional technical regulatory agencies to ensure operational compliance and the destruction of invalid data. This model combines judicial authority with technical expertise, forming a dual safeguard mechanism. This "judicial-technical dual-track coordination" model leverages the courts' central role in bankruptcy proceedings and their ability to assess public interest, while also utilizing the specialized capabilities of departments such as the Cyberspace Administration in enforcing and verifying data security technical standards. This approach is expected to provide a more comprehensive and effective solution to the challenges of supervising the disposal of bankruptcy data.

Given the continuous expansion of the digital economy and the coexistence of bankruptcy risks, user data protection has become a major public interest issue that cannot be ignored. The harm caused by the current institutional gaps is becoming increasingly apparent. Therefore, it is imperative that legislative bodies and regulatory agencies attach great importance to this issue, accelerate the revision of relevant laws and the formulation of supporting policies, clarify the responsibilities of all parties, set operational standards, establish accountability mechanisms, and promote the implementation of a "dual-track coordination" mechanism to provide a solid legal guarantee for data security and user rights in bankruptcy proceedings.

5. Conclusion

This study also has certain limitations. In terms of platform sampling, the research sample focused on applications in the Huawei App Market and iOS App Store, failing to cover lightweight platforms such as WeChat and Alipay mini programs, as well as regional government-related platforms such as "Yuejian Tong." This sampling bias may lead to an underestimation of the special compliance requirements of government platforms. Future research should combine the Ministry of Industry and Information Technology's filing list to implement full platform sampling to improve representativeness.

At the data collection level, privacy policy text analysis carries the risk of non-response bias. This method cannot capture differences in users' actual authorization behaviors, such as the distinction between "one-click consent" and reading each clause individually, nor can it identify internal enforcement loopholes within companies, such as policies that stipulate deletion but result in actual data leaks. Subsequent research should integrate user surveys and judicial case reviews to address this shortcoming. In terms of improvement recommendations, research on cross-border governance differences is insufficient. For example, China's implementation of "anonymization prior to processing" requirements may pose risks of violating WTO digital trade rules. Conducting comparative studies on international bankruptcy data disposal cases holds significant value.

Author Contributions: X.Z.: study concept, data interpretation, writing the paper, review & editing. Y.L.: data acquisition, review & editing. K.D.: review, editing and revising.

Funding: This research received no external funding

Conflicts of Interest: The authors declare no conflict of interest.

References

Apple App Store. (2023). The Top Free Health, Fitness & Medical Apps Chart (iPhone, China). Available online: https://apps.apple.com/cn/charts/iphone/fitness-and-health-apps/6013, and https://apps.apple.com/cn/charts/iphone/medical-apps/6020. (accessed on 30 June 2023).

Bamberger, K. A., & Mulligan, D. K. (2010). Privacy on the Books and on the Ground. *Stan. L. Rev., 63*, 247.

Beckmann, R. A. (2000). Privacy Policies and Empty Promises: Closing the Toysmart Loophole. *U. Pitt. L. Rev., 62*, 765.

Birch, K., Cochrane, D. T., & Ward, C. (2021). Data as asset? The Measurement, Governance, and Valuation of Digital Personal Data by Big Tech. *Big Data & Society, 8(1),* 20539517211017308.

Bradley, C. G. (2022). Privacy Theater in the Bankruptcy Courts. *Hastings LJ, 74,* 607.

Bradley, C. G. (2023a). Privacy for Sale: The Law of Transactions in Consumers' Private Data. *Yale J. on Reg., 40*, 127.

Bradley, C. G. (2023b). Privacy Policy Indeterminacy. *Conn. L. Rev., 56,* 405.

Chen, X. (2023). Data Protection and Processing in Bankruptcy Proceedings. *Leg. App. 83*, 84.

Chuah, J., & Vaccari, E. (Eds.). (2023). *Executory Contracts in Insolvency Law: A Global Guide*. Edward Elgar Publishing.

Collins, V., & Lanz, J. (2019). Managing Data as an Asset. *The CPA Journal, 89(6),* 22.

Coordes, L. N. (2021). Unmasking the Consumer Privacy Ombudsman. *Mont. L. Rev., 82,* 17.

Ding, X. (2023). A Multidimensional Interpretation of Privacy Policy: Reflection on the Nature of Informed Consent and Institutional Reconstruction. *Modern Law, 45(34),* 35.

Huawei App Gallery. (2023). The Sports & Health and Medical Apps Download Rankin g. Available online: https://appgallery.huawei.com/mwsecondchildtab?tabid=7e04648230ca4bbaa836fa8c027517ba&tabName=%E8%BF%90%E5%8A%A8%E5%81%A5%E5%BA%B7 (accessed on 30 June 2023).

Kreuter, F., Haas, G. C., Keusch, F., Bähr, S., & Trappmann, M. (2020). Collecting Survey and Smartphone Sensor Data with an App: Opportunities and Challenges around Privacy and Informed consent. *Social Science Computer Review, 38(5),* 533.

Miller Jr, W. W., & O'Rourke, M. A. (2001). Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card. *Hous. L. Rev., 38,* 777.

Ou, F. & Zhang, X. (2024). On the Regulation of Cross-border Data Flow in Bankruptcy Proceedings in China. *J. Soc. Sci. Hunan Norm. Univ., 53*, 75.

Qu, M. (2024). In the Midst of Bankruptcy: How Cryptocurrency's Classification Affects Creditors Who Were Once Customers. *Wash. L. Rev., 99,* 323.

Scholz, L. H. (2019). Privacy Remedies. *Ind. LJ, 94,* 653.

Seymour, J. M. (2022). Against Bankruptcy Exceptionalism. *U. Chi. L. Rev., 89(8),* 1925.

Solove, D. J., & Citron, D. K. (2017). Risk and Anxiety: A Theory of Data-breach Harms. *Tex. L. Rev., 96*, 737.

Ullah, S., Khan, M. S., Lee, C., & Hanif, M. (2022). Understanding Users' Behavior towards Applications Privacy Policies. *Electronics, 11(2),* 246.

Warren, E., & Westbrook, J. L. (1986). *The Law of Debtors and Creditors: Text, Cases, and Problems*. Wolters Kluwer.

Williams, S. M., Turner, A. A., & Basharis, G. (2005). Bankruptcy Abuse Prevention and Consumer Protection Act of 2005. *Law & Explanation,* 2005.

Zhao, J. (2024). On the Disposition of Enterprise Data Assets in Bankruptcy Proceedings. *China Leg. Sci., 3,* 103.