Economics, Law and Policy
ISSN 2576-2060 (Print) ISSN 2576-2052 (Online)
Vol. 8, No. 2, 2025
www.scholink.org/ojs/index.php/elp

Original Paper

Research on the Civil Law Protection of Private Information

Jingwen Xu[1]

[1] Dalian Ocean University, Dalian, Liaoning, China

Received: August 10, 2025 Accepted: August 20, 2025 Online Published: August 22, 2025

doi:10.22158/elp.v8n2p147 URL: http://dx.doi.org/10.22158/elp.v8n2p147

Abstract

According to the China Annual Report on Personal Information Security, data breaches nationwide will increase by 23% year-on-year in 2024, and private information such as biometrics, health care, and financial transactions will become the main targets. In this context, Article 1034 of the Civil Code of the People's Republic of China clarifies the legal attributes of private information, stipulates that the relevant provisions on privacy are applied to its protection, and the Personal Information Protection Law applies when there are no special provisions, which makes private information both "private" and "identifiable" as the intersection of privacy and personal information. Theoretically, there is a dispute over the boundary between private information and sensitive personal information, and the protection model also faces differences in the choice of unification and dualization. In this regard, we can learn from the German "field theory" and combine the principle of proportionality in our country's Civil Code, refine the rules from the whole chain of collection, use and storage, set up special regulatory agencies, and empower public participation through education, technical tools, public interest litigation, etc., so as to improve the private information protection system and effectively safeguard the rights and interests of citizens.

Keywords

private information protection, Infringement identification, Privacy, Personal information, Burden of proof

1. Introduction

With the rapid development of the digital information era, the protection of personal private information has attracted increasing attention. In recent years, many incidents involving information leakage and infringement of personal information have occurred on the Internet. However, relevant laws and regulations are not perfect, the definition of personal information is unclear, the scope of protection is not clear, and there are still illegal phenomena.

2. Research Hypotheses

If private information is closely related to privacy rules, it is more likely to apply privacy rules for protection. The reason is that the right to privacy emphasizes the independent control and non-interference of individuals in the field of private life, and private information is an important part of privacy, and when faced with infringement, according to the privacy rules, the information subject can claim his right to conceal private information and not be illegally obtained and disclosed by others, so as to maintain the peace of his private life and personal dignity.

3. Research Design

Systematically explore the logic and protection path of specific rules under the framework of civil law protection, clarify the boundaries of private information and privacy rights and personal information protection rules, clarify the differentiated protection models of private information with different attributes, provide theoretical guidance for handling private information infringement cases in judicial practice, and put forward reasonable suggestions for improving our country's civil law protection system for private information.

4. Empirical Analysis

4.1 The Theoretical Basis of Private Information Protection in Civil Law

4.1.1 Definition and Characteristics of Private Information

Article 1034 of the Civil Code stipulates that private information within personal data shall be governed by privacy rights provisions; where no such provisions exist, the applicable personal information protection regulations shall apply. Personal private information refers to data closely tied to an individual's life, identity, health, and other aspects that they generally wish to keep private. This category includes critical information such as identity verification, physical condition, financial status, communication patterns, and geographical location, all of which carry paramount importance. Information regarding property, health conditions, biometric data, and personal privacy falls under the scope of private information. Additionally, other classifications are provided to categorize private information into different domains.

Professor Zhang Gexin argues that the legal framework lacks clear definitions for private information, given its inherently subjective nature (Zhang, G. X., 2023, pp. 87-94). In practice, such determinations should be context-specific. To strengthen privacy protection, he proposes adopting a "discernibility + relevance" standard: Private information refers to any electronically recorded data containing sensitive attributes of identifiable individuals, which may also be termed private 1information or informational privacy.

In recent years, there has been a growing number of fraud cases caused by personal privacy, including vicious crimes such as financial fraud and identity theft. This not only reflects the urgency of protecting

private information, but also sounds an alarm for us to strengthen the formulation and enforcement of relevant laws.

4.1.1.1 Privacy

Private information has the nature of not being disclosed or disclosed. It is the information that individuals do not want to be known by the outside world, and others cannot easily access or peek into it. Only with the authorization or consent of the owner of the information can others have access to or obtain this information.

4.1.1.2 Sensitivity

Some private information may involve trade secrets. Therefore, if criminals steal or information processors illegally sell information in the process of processing information, it may bring serious property losses and adverse consequences to enterprises.

The leakage of some private information may also damage a person's reputation. For example, hotels install pinhole cameras to take indecent photos of hotel guests and leak them to the Internet for corresponding remuneration.

When it comes to the leakage of private information such as home addresses and personal travel plans, there may be security risks. At the end of 2019, when the COVID-19 pandemic broke out in Wuhan, there was a large-scale over-collection of citizens' ID numbers, home addresses, and other private information under the guise of epidemic prevention. This led to many people being harassed through WeChat messages, phone calls, and verbal abuse (Jiang, H. Y., 2020, pp. 183-194, p. 209).

4.1.1.3 Specificity and Complexity

Confidential information lies at the intersection of privacy and personal data, encompassing multiple dimensions. In handling related cases, it is crucial to prevent factual errors in judgment while minimizing uncertainties in legal application. Through referencing specific cases, modern legal practice continuously accumulates and innovates privacy protection methods. This ongoing process optimizes and enhances China's civil law framework for safeguarding confidential information.

4.1.2 The Connection between the Right to Privacy and Private Information

To determine private information, it is crucial to distinguish between privacy and personal information. Article 1032 of the Civil Code stipulates: Natural persons enjoy the right to privacy. Without permission, no acts such as prying, interfering, disclosing, or publicizing shall be permitted. Paragraph 2 defines personal privacy as private life, activities, and information. The concept of privacy was first introduced in late 19th-century American legal systems, referring to an individual's control over their private life information. With societal evolution, privacy rights now encompass not only personal information protection but also aspects of personal life tranquility and communication confidentiality. Paragraph 2 of Article 1034 of the Civil Code specifies that personal information includes any electronically or otherwise recorded data capable of identifying specific individuals, either independently or in combination with other information. This encompasses names, dates of birth, ID

numbers, biometric data, addresses, phone numbers, email addresses, health records, and location data. Privacy protection serves as a passive safeguard against intrusion, while right holders retain autonomy in personal information decisions during data integration and processing. Article 1033 requires explicit consent for privacy processing, whereas Article 1035 stipulates that consent may be explicit or implied, indicating that explicit consent isn't always mandatory when handling personal information. At the same time, Article 1033 of the Civil Code also states that the explicit consent of the right holder should be obtained when dealing with private information (Zhang, Z. W., 2022). As can be seen from the above, the protection of private information is more similar to the protection of privacy.

Private information constitutes the overlap between privacy and personal information. Article 1034(3) of the Civil Code stipulates that private information within personal data shall be governed by privacy rights provisions, while areas lacking such provisions shall apply personal information protection regulations. The legal text demonstrates that privacy rights take precedence in protecting private information. This principle implies that only inherently private elements within personal data qualify for privacy rights protection under relevant legal provisions.

4.1.3 The Necessity of Protecting Private Information

With the advancement of society, the infringement of personal privacy has become increasingly severe, making civil law protection crucial. The leakage of private information not only jeopardizes individuals' reputation and property security but also compromises personal freedom and dignity, even affecting cross-departmental and societal information security. In this context, leveraging civil law to safeguard personal privacy plays a vital role in maintaining social equity and justice.

To prevent reputational and financial harm caused by the leakage of personal privacy, civil law must provide robust safeguards. When citizens' information is collected online, inadequate storage may leave it vulnerable to hackers who could steal uploaded private data. Such breaches not only cause significant personal repercussions but also lead to potentially disastrous consequences that could ripple through society.

Through in-depth research, we can better understand the threats and risks to private information, thereby formulating more effective security strategies and measures. Preventing the leakage of private information not only safeguards citizens' personal dignity and rights, but also helps curb criminal activities such as property loss and identity theft caused by data breaches, which could otherwise destabilize society. Protecting private information through civil legal frameworks can effectively mitigate these risks, playing a crucial role in maintaining social order and public safety.

Privacy processors who negligently leak or illegally sell others' private information during processing, thereby causing harm, shall face severe penalties. When using apps, authorities must not force the collection or over-collect users' private data. Users should be informed in advance about such data collection to prevent malicious individuals from exploiting their privacy for personal gain, thereby infringing on rights holders' interests.

The current lack of clear legal provisions regarding the classification of private information and liability determination for infringement has allowed criminals to exploit legal loopholes, resulting in privacy violations against citizens without timely accountability. Timely legislation on personal privacy protection not only safeguards citizens' legitimate rights but also demonstrates China's strong commitment to protecting privacy rights.

Personal privacy constitutes a vital component of commercial resources. Protecting such information not only safeguards individual dignity but also fosters an open, transparent, and fair competitive environment for businesses, thereby driving social progress. Moreover, it contributes to the healthy development of the digital economy. Establishing clear definitions and protective measures for private data can enhance public trust in digital ecosystems, unleashing innovative potential and fueling the thriving growth of the digital industry.

To sum up, it is very necessary to take civil law protection measures for private information, which not only protects citizens' legitimate rights and personal dignity, but also highlights the respect for personal dignity. Therefore, we need to constantly improve the protection of private information and strictly crack down on criminals from different dimensions.

4.2 Problems Existing In the Protection of Private Information

In the big data era, personal identity information—including ID numbers, phone numbers, and online search histories—has become part of big data stored in databases, exposing them to risks of exploitation by governments or commercial entities. The illegal acquisition and resale of private data pose serious threats to citizens' privacy security. Internet service providers may store or collect personal information without users' consent, leading to data breaches. The Civil Code stipulates that processing private information requires explicit consent from right holders. Article 1032 explicitly states that natural persons enjoy privacy rights, prohibiting organizations or individuals from infringing these rights through prying, harassment, disclosure, or public exposure. Article 1034 defines the scope of personal information, emphasizing that private information falls under privacy rights protection; otherwise, it follows general personal information protection rules. In practice, internet platforms often forcibly collect users' private data, potentially causing leaks and misuse risks.

4.2.1 The Identification of Private Information in the Law Is Not Clear

According to Article 1034(3) of the Civil Code, the protection of private information negatively excludes provisions for personal information. However, how private information passes the privacy test and becomes an object protected by privacy rights requires in-depth discussion. Regarding the determination of private information, some aspects are undisputed—such as personal health data, criminal records, and financial status naturally fall under private information. Information protected by personality rights like names, voices, and facial features should not be categorized as private information. Given the complexity of infringed information in judicial practice, determining whether it constitutes private information cannot rely solely on the "unwillingness to be known" standard. It must consider both general public perception and specific case circumstances.

4.2.1.1 Privacy and Private Information

Private information constitutes an integral part of privacy. The concept of "fans" is broadly defined to encompass all aspects of personal life that individuals wish to protect from unauthorized access or interference. Within this framework, specific types of private information include concrete details such as personal correspondence and transaction records.

As a category of personality rights, privacy rights primarily protect individuals' private information, emphasizing the safeguarding of personal dignity rather than property attributes. However, confidential information is inherently embedded within personal data, whose defining characteristic lies in its identity-related nature. When citizens engage in shopping or banking transactions, they may inadvertently disclose sensitive details. This demonstrates that such confidential information transcends traditional privacy boundaries and exhibits distinct property attributes.

4.2.1.2 Personal Information and Private Information

The accessibility of personal information is open to society, and its use generally does not significantly impact the rights holder's reputation or social standing. However, if private data is leaked, it can cause substantial psychological harm to the rights holder, including threats to financial security and social standing. When privacy breaches result in emotional distress, the right to privacy constitutes the legal framework for protecting information.

4.2.1.3 Sensitive Personal Information and Private Information

The Civil Code stipulates the private information and its protection principles from the perspective of civil rights protection, while the Personal Information Protection Law stipulates the sensitive information and its processing principles and basic rules from the perspective of personal information processing (Lu, Z., 2021, pp. 86-100). Since sensitive information and private information have overlapping relationships, the private information is also provided with legal protection.

The Personal Information Protection Law categorizes personal information into sensitive and general types. Sensitive information, which may infringe upon an individual's dignity or harm their physical and material well-being if improperly disclosed or illegally used, includes biometric data, specific identity information, location data, and mobile communication records—except for personal information of minors under 14. Article 1034 of the Civil Code further divides personal information into private and non-private categories, with sensitive information similarly reflecting a desire to maintain privacy. As privacy rights constitute part of personality rights, violations of such information can damage the rights holder's personal dignity. According to the Personal Information Protection Law, breaches of sensitive information not only harm personal interests but may also involve social or national security concerns. To distinguish between sensitive and private information, we must examine their distinct perspectives. Sensitive information represents vital privacy that impacts personal dignity and freedoms, while private information focuses on protecting individual privacy from external interference. Scholar Zhang Lu argues that private information primarily manifests through two characteristics: secrecy and exclusivity. Secrecy refers to the right holder's legitimate expectation of

privacy protection and public recognition of such protection. Exclusivity ensures that the protection, storage, and consequences of privacy breaches concern only the right holder's interests without affecting others. Zhang Lu pointed out that privacy is an important factor in determining whether it belongs to private information (Yu, Y., & Yu, J. Q., 2021, pp. 64-73).

A comparative analysis of the aforementioned concepts reveals that the distinctions between private information, privacy, personal information, and sensitive personal information remain ambiguous. The difficulty in differentiating private information often leads to challenges in defining such data within information infringement cases. Neither the Civil Code nor the Personal Information Protection Law provides clear definitions of private information through a "generalized+specific enumeration" approach.

4.2.2 The Identification of Invasion of Private Information Is Not Clear

The determination of private information infringement remains ambiguous in judicial practice. Due to the lack of clear legal guidance, judges often have to make judgments based on their understanding of case circumstances and individual case specifics. This subjective approach may lead to inconsistent rulings, potentially undermining the predictability and credibility of the law. In handling personal information infringement cases, discrepancies in the application of tort liability elements result in varying determinations of liability. For instance, in the case of plaintiff Gu versus defendant Liaoning Unicom Company and other telecommunications service providers, the presiding judge applied the tort liability element of causing damage. As plaintiff Gu failed to provide evidence of specific damages incurred, the court ruled that the defendant was not liable for compensation.

Under China's current legal framework, victims of privacy violations must prove before courts whether their leaked personal information originated from malicious actors or inherent internet vulnerabilities. This creates significant obstacles for rights holders in evidence collection and litigation. In the privacy rights dispute case between Pang Lipeng and China Eastern Airlines Co., Ltd., Pang Lipeng had booked a flight through Qunar (a subsidiary of Beijing Quna Information Technology Co., Ltd.) on behalf of Lu Chao. Later, Pang received an anonymous call informing him that his flight had been canceled. China Eastern Airlines subsequently sent a text message notifying him of schedule changes. When Lu Chao contacted the airline's customer service for confirmation, he was told the flight had been canceled. Pang claimed that Quna and China Eastern Airlines had leaked his personal data. The court dismissed his information infringement claim in the first instance. During appeal, the appellate court identified potential liability from both China Eastern Airlines and Qunar regarding the breach. While Pang's personal information exposure caused both financial losses and emotional distress, the case highlighted legislative gaps in fact-finding and judicial remedies. This precedent underscores the urgent need for enhanced privacy protection legislation in China. In information networks, where infringers are often unidentified and infringement methods are highly complex, rights holders face significant challenges in providing and listing concrete evidence of infringement under existing laws. This difficulty leads to unfavorable consequences of "failure to provide evidence" for rights holders

who cannot submit sufficient proof, making it hard for plaintiffs to obtain reasonable and effective legal remedies through litigation. Consequently, they find themselves in a situation where their information is leaked but rights protection remains difficult to achieve.

To sum up, the identification and compensation standards for privacy infringement need to be more clear and specific, and the legislation of privacy protection should be further improved to clarify the tort liability.

4.2.3 Internet Platforms Infringe Users' Private Information

According to the "Measures for Identifying Illegal and Improper Collection and Use of Personal Information by Apps" (hereinafter referred to as the "Measures") issued in 2019 by China's Cyberspace Administration and Ministry of Industry and Information Technology, the following scenarios may lead to app-related personal information collection being identified: "failure to publicly disclose collection rules", "failure to clearly state purposes, methods, and scope of data collection", "collecting personal information without user consent", "violating the principle of necessity by collecting irrelevant data", "providing personal information to third parties without authorization", and "failure to provide legally mandated deletion or correction functions, or lack of published complaint reporting channels".

In today's rapidly developing digital economy, users often face mandatory authorization requests when logging into or using apps to grant platforms access to location data, photo albums, contact lists, and other information (Hoffman, S., & Podgurski, A., 2007, p. 331). If users reject these permissions, they may be unable to access essential features or even the app itself. For instance, during the crackdown on apps infringing user rights in Sichuan and Chongqing, authorities discovered an app called "Lubel". Upon activation, it displays a privacy policy prompt that collects sensitive information including ID documents, facial recognition data, and fingerprints. The terms explicitly state that the app can commercially use de-identified data without user consent. When users attempt to reject these requests, the system forces them to read and agree to the privacy policy through a pop-up window. If rejected, users are compelled to exit the app.

China has not established comprehensive regulations defining the scope of private information protection. While existing laws contain guidelines similar to the "Security Regulations", their limited public awareness and absence of legal authority make personal data frequently vulnerable to infringement. Users often face forced or excessive collection of sensitive information during app usage, causing significant inconvenience to rights holders (Zhang, G. X., 2023, pp. 84-96).

According to Article of the "Regulations", when collecting user personal information, apps may not collect non-essential data or permissions unless users explicitly consent to such actions. In the personal information protection case between Wang Moumou and Tencent, Wang initially logged into Weishi through WeChat, granting permission for the app to access his gender, location, and contact list. After uninstalling Weishi and resetting his phone to factory settings, Wang attempted to log in using his original WeChat ID. Despite not authorizing the "Find Friends Using This App" feature during this

login attempt, Weishi still displayed browsing history of his WeChat contacts. Tencent maintained access to Wang's contact information even after explicit user prohibition. However, following a 2021 system update, these features were removed, meaning Weishi no longer searches unauthorized user data when using the same WeChat account. The Regulations further stipulate that apps must obtain user consent only through service quality improvements, enhanced user experiences, targeted content delivery, or new product development. In this case, Tencent's Weishi app's request for authentic gender and location data violated the principle of necessary information collection.

4.2.4 Illegal Processing of Private Information by the Private Information Processor

The protection rules of privacy rights shall be given priority to the private information. According to Article 1033 of the Civil Code, if the right holder does not have explicit consent or the law does not provide otherwise, the processing of the right holder's private information shall be deemed as illegal processing of the private information.

Privacy processors are individuals who possess, manage, or have access to specific personal information. They bear clear responsibilities and obligations to ensure the security and compliance of such data. The continuous collection, acquisition, and processing of private information stem from multiple factors. Employers may seek to retain their most valuable employees, while marketers utilize this data to provide tailored services, enhance user experiences, and ultimately retain more customers (Felt, A., & Evans, D., 2008).

On September 6, 2015, Youlian Company was officially registered. Zhao Haijun, the defendant, served as the company's general manager, while Zeng Xi acted as its business director. In early 2015, Zhao Haijun obtained customer information stored by Kai Zhou Unicom employees through professional connections. Later that year, Zeng Xi acquired client data via her former colleague at Kai Zhou Unicom. In 2017, Zeng Xi further obtained membership records from Kai Zhou Aiyin Image Beauty Salon through its owner. As data custodians, these Unicom employees abused their positions to facilitate illicit activities, resulting in the leakage of sensitive customer information.

As public awareness of personal privacy grows, new ethical dilemmas continue to emerge. Financial institutions have increasingly resorted to collecting customer information for profit. In recent years, banks and insurance companies across China have faced penalties for improper use of client data. Insurance providers exploited their access to vast amounts of customer information to conduct illicit transactions beyond their authorized scope, illegally profiting from such activities. For example, a criminal judgment document published by Shanghai Jing'an District People's Court in April 2023 revealed that employees of Ping An Life Insurance Yancheng Central Branch violated clients' privacy by accessing and supplementing personal information, then selling it for illicit gains totaling nearly 270,000 yuan. Another high-profile case involved "Fat Cat" (a pseudonym) who was defrauded of 510,000 yuan and committed suicide by jumping into a river. Tan sued Liu, Fat Cat's sister, for privacy infringement. After the case came to light, Tan successfully recovered over 136,000 yuan from Fat Cat's father through mediation. However, Liu claimed the money had been spent on Tan and expressed

resentment, stating she would “never let her live easy”. She further leaked screenshots of private chats and transfer records between Tan and Liu via Fat Cat’s phone onto public platforms, with most images depicting Tan using psychological manipulation tactics against Fat Cat and labeling her as both a “fraudster” and “a woman to be exploited”. Liu Mou, under the guise of defending his brother, deliberately intercepted chat records unfavorable to Tan Mou. He manipulated public opinion against Tan Mou while illegally publishing their private conversations online without consent. Later, by creating a new account to comment on forums and invite friends to join the discussion, he amplified the incident's impact to garner sympathy from netizens. This campaign led to widespread online abuse targeting Tan Mou, including threatening transfers with obscene messages. The actions not only disrupted Tan Mou’s daily life but also compromised cybersecurity standards.

4.3 Suggestions for Improving the Protection of Private Information in Civil Law

4.3.1 Clarifying the Identification Criteria of Private Information

To establish clear definitions of private information, a multi-pronged approach is required. This includes clarifying its definition and scope, improving relevant laws and regulations, enhancing judicial determinations in practice, raising public awareness, and strengthening regulatory oversight and law enforcement. Through implementing these measures, we can better protect personal privacy while maintaining social order and safeguarding public interests.

In the discussion of civil legal protection for personal privacy information, establishing clear identification criteria for sensitive data is paramount. This serves not only to safeguard individual interests but also significantly impacts the fairness and efficiency of legal applications. With internet usage growing exponentially, the transmission formats and methods of confidential information have become increasingly diverse. Therefore, in practical implementation, we need to precisely define the scope of private information.

The criteria for determining private information should balance its confidentiality with potential consequences of disclosure. Confidentiality primarily refers to the prohibition of unauthorized dissemination. If such information is illegally disclosed, it may jeopardize the rights holder’s personal safety and property security. For instance, when a company improperly shares employees’ salary data with third parties, it not only causes financial harm but also inflicts dual psychological trauma on affected individuals.

When determining whether information qualifies as private, we should not only consider public perception and specific circumstances, but also employ a risk assessment model that evaluates the information’s value, potential leakage risks, and potential damages. This model allows us to determine the privacy level of information based on different scenarios, effectively addressing the challenge of right holders being at a loss when attempting to provide evidence of infringement.

4.3.2 Strengthening the Multi-Dimensional Protection of Private Information

First, it is imperative to comprehensively refine relevant legal frameworks. To address regulatory gaps in privacy protection legislation, clearer and more specific provisions must be established. This includes defining clear responsibilities and obligations for all parties involved while imposing stricter penalties for violations. For instance, China could adopt the EU's General Data Protection Regulation (GDPR) model by imposing substantial fines on entities or individuals breaching privacy protection regulations, thereby creating a deterrent effect. Although both the Civil Code and Personal Information Protection Law contain provisions on privacy protection, their differing approaches and objectives often lead to legal ambiguities. Ambiguous legal concepts also create opportunities for misconduct. A prime example is Article 28(2) of the Personal Information Protection Law, which defines "specific purposes"—the exact interpretation of these criteria directly impacts the determination of infringement cases. Therefore, it is crucial to provide clear legal interpretations of how these provisions should be applied, building upon existing protective mechanisms.

Secondly, in judicial practice regarding privacy infringement cases, courts must ensure prompt and fair adjudication while minimizing victims' burden of proof. This prevents the imbalance of evidentiary responsibilities from compromising legitimate rights. To enhance case handling efficiency, authorities should simultaneously raise public legal awareness and strengthen social oversight mechanisms. The public is encouraged to actively participate in safeguarding personal privacy by reporting violations and exercising supervision. Furthermore, media outlets should intensify publicity campaigns and coverage on privacy protection to elevate societal awareness and commitment to safeguarding private information.

Professor Zhang Gexin argues that the protection of private information should be categorized, as its manifestation may differ in personal interests or commercial value (Wang, Y. N., 2023, p. 113). Internationally, a categorized approach to privacy protection has been adopted. The European Union implemented the General Data Protection Regulation (GDPR), which strictly regulates personal data protection through rights of data subjects, obligations of data processors, and cross-border data transfers. The United States enforces multiple laws including the Privacy Act and the Electronic Communications Privacy Act (ECPA). The Privacy Act primarily governs federal government handling of personal information, covering collection, usage, disclosure, and confidentiality. The ECPA establishes corresponding protections for communication content and records, explicitly defining service providers' responsibilities while emphasizing robust security measures for stored private data. In China, information can be classified by source and protection purposes into: 1) Personal identification data (e.g., names, ID numbers, home addresses); 2) Financial data (e.g., bank account numbers, credit card transaction records); 3) Health information (e.g., medical records, health check reports); 4) Communication data (e.g., emails, texts, chat logs); 5) Work-related information (e.g., trade secrets, work documents).

4.3.3 Strengthen the Protection of Users' Private Information by Internet Platforms

4.3.3.1 Establish a Safety Inspection Mechanism

On internet platforms, users grant websites and apps the right to collect private information. While data processors ultimately benefit from this collection, the rights holders must bear the associated risks. If processors misuse collected data for personal gain through illegal processing, it may jeopardize both the reputation and financial security of rights holders. To address this, data processors must strictly comply with relevant laws and regulations. All information-gathering entities should establish robust information security management systems, ensuring proper custody of personal data while maintaining strict oversight over its collection, storage, usage, and transmission. In the event of data breaches, they must implement appropriate response measures while respecting users' fundamental rights—including the right to be informed and the right to rectification.

Within the legal and regulatory framework, individuals who disregard established guidelines for managing private information should face appropriate oversight and penalties. Effective supervision ensures that privacy handlers diligently fulfill their duties and adhere to established norms and standards. Additionally, compliance with prescribed procedures for processing private information must be monitored.

Regular inspections should be conducted to ensure the security of user information. A penalty mechanism serves as a crucial regulatory tool. If data handlers neglect their obligations, such as allowing information leaks or data misuse, they should face appropriate penalties including fines and corrective guidance to rectify their actions. These disciplinary measures aim to serve as a deterrent, but should not be excessively harsh.

Foreign scholars have proposed that applications can display information to users through special labels. By restricting content in conditional sections, apps can prevent third-party leaks of sensitive data. The server within the program promptly clears elements in these sections. Private data access is only permitted when users utilize cached images from the server and do not send leakage requests to external servers.

Only by strengthening the responsibility of private information processors can we effectively protect the private information of rights holders, maintain information security and network order, and promote the healthy development of the information industry. At the same time, it also helps to enhance public trust in information processing activities and promote the smooth operation of society.

4.3.3.2 Adjust the Burden of Proof

In both real-world and digital environments, the infringement of personal privacy has become increasingly prevalent. However, in judicial proceedings, individuals often lack sufficient evidence to assert their rights. Given circumstances involving presumed fault, presumed causation, and evidentiary collection challenges, implementing an inverted burden of proof should be prioritized. The Foshan Consumer Council in Guangdong Province recently released a research report titled "Research Report on Evidence Difficulties in Civil Disputes Over Consumer Personal Information", proposing reforms to

break away from the conventional burden of proof allocation framework under current laws. This would legally establish provisions for information providers to bear the burden of proving they failed to disclose private information. Such an approach better aligns with the nature of information infringement, reduces the evidentiary burden on victims, helps protect citizens' privacy rights, strengthens accountability for responsible parties, and ultimately curbs such violations at their source.

In the past, the burden of proof for information infringement cases followed the "he who asserts must prove" principle. However, with rapid advancements in information technology, infringers can now employ AI face-swapping and voice-altering techniques. Additionally, when economic capabilities or political statuses differ between parties, the rule of presumed fault may apply (Shen, X., Tan, B., & Zhai, C. X., 2007, pp. 4-17). When applying Article 69(1) of the Personal Information Protection Act regarding presumed fault liability, right holders need not prove the processor's fault. Instead, information processors must demonstrate their innocence, shifting the burden of proof to them. This reform significantly reduces the burden on right holders. When personal information is infringed, the no-fault liability principle should be adopted, requiring parties to provide evidence focusing on three essential elements: the infringement act, damages, and causal relationship.

After installing an app, users might skip or misread privacy policies in haste. When declining to share personal information, they expect options to reject authorization or revoke partial consent. This allows the app to function properly without hindering usage. If the requested data isn't essential for the service, developers should promptly respond to such revocation requests.

In real-world practice, users exhibit varying levels of acceptance toward information collection and utilization. While some users adamantly reject having all personal data collected, others willingly provide detailed information to help apps and websites better meet their specific needs. Therefore, foreign scholars Xuehua Shen, Bin Tan, and ChengXiang Zhai believe that it is necessary to adjust the level of privacy protection for different users to accommodate varying preferences in personalization and privacy protection trade-offs.

4.3.4 Strengthen the Code of Conduct for Private Information Processors

Regulating the behavior of private information processors is of great significance for safeguarding individual rights and interests, social stability and the development of information industry.

4.3.4.1 Strictly Follow the Obligation of Disclosing Private Information

Knowledge forms a cornerstone of privacy protection. When right holders fully comprehend how online platforms process personal data, understand the specific purposes behind information collection, and recognize the services these data support, they can more effectively prevent privacy violations. This awareness also streamlines the burden of proof during legal proceedings, ensuring stronger safeguards for data rights.

When handling private information, the most crucial aspect is that data processors must inform rights holders about processing purposes, procedures, and necessary matters related to services. However, some notification rules are overly complex and lengthy, making it difficult for users who lack patience

to read them in full. Certain notification protocols pose significant comprehension challenges due to insufficient information explaining the intent behind processing such private data. This ambiguity may leave users at a disadvantage in application disputes and undermine the effective protection of their legitimate rights. Data processors must promptly, accurately, and comprehensively inform information subjects about every stage of processing private information, including collection, use, storage, and sharing. Only with full understanding can rights holders make rational decisions regarding consent to data processing and how to protect their interests. By strictly adhering to privacy notification obligations, we can build trust with users, safeguard their right to information, enhance transparency in data handling, and prevent misunderstandings and disputes caused by information asymmetry. This will also encourage data processors to exercise greater prudence in their operations, align more closely with legal requirements, and fulfill their responsibilities to ensure user protection and information security.

4.3.4.2 Use Private Information Wisely

First of all, there must be a clear legal purpose, and the collection of information irrelevant to the purpose should not be arbitrary. The Method also stipulates that the collected information should be related to the services provided. Moreover, before the collection of private information, the explicit consent of the right holder must be obtained.

When handling information, strictly adhere to agreed-upon methods and boundaries to ensure data security. Implement robust technical safeguards and management protocols to prevent leaks. All collected and utilized materials must undergo thorough review and evaluation. Unauthorized use of personal data for illegal purposes is strictly prohibited, and sharing with third parties without proper authorization is forbidden.

Private information should be destroyed in a timely, thorough and secure manner after use to eliminate hidden dangers.

For financial institutions that may pose significant risks, such as banks and insurance companies, establishing relevant regulations is crucial. This requires us to not only collect private information but also ensure its security, thereby preventing employees from exploiting customer privacy leaks or unauthorized access to confidential data for personal gain.

5. Conclusion

When collecting and using personal confidential information, it is necessary to ensure that it has a legitimate purpose and obtain explicit permission from the rights holder. Any unauthorized collection and use is a violation of the privacy rights of others and should be subject to legal sanctions. At the same time, we should ensure that personal confidential information is not improperly used during storage, transmission, and use, and take necessary technical and management measures to safeguard the security of information. Through the above measures, we aim to comprehensively protect citizens' privacy rights, maintain social order and stability. A secure network environment and a society that respects privacy will be more conducive to the flourishing development of the information industry.

While promoting innovation in the information industry, we should also ensure that citizens have the right to access personal and private information, allowing them to freely express their voices and share their experiences.

References

Felt, A., & Evans, D. (2008). *Privacy protection for social networking platforms*. Web, 2008.

Hoffman, S., & Podgurski, A. (2007). In sickness, health, and cyberspace: Protecting the security of electronic private health information. *BCL Rev.*, 2007(48), 331.

Jiang, H. Y. (2020). On Personal Information Protection in the Context of the Epidemic—From the Perspective of the Principle of Proportionality. *Journal of China University of Political Science and Law*, *2020*(04), 183-194, 209.

Lu, Z. (2021). What is private information?—Discussion on the intersection of privacy rights and personal information protection in the Civil Code. *Journal of Gansu University of Political Science and Law*, *2021*(01), 86-100.

Shen, X., Tan, B., & Zhai, C. X. (2007). *Privacy protection in personalized search*. ACM SIGIR Forum. New York, NY, USA: ACM, 2007, 41(1): 4-17. https://doi.org/10.1145/1273221.1273222

Wang, Y. N. (2023). Burden of Proof Allocation in Personal Information Protection Disputes. *People's Judicial*, *2023*(17), 113.

Yu, Y., & Yu, J. Q. (2021). Civil Law Regulation of Personal Information Infringement in the Era of Big Data—From the Perspective of Personal Information Collection and Use by Mobile Apps. *Academic Exchange*, *2021*(05), 64-73.

Zhang, G. X. (2023). Defining the Scope of Private Information and Enhancing Legal Protection. *Journal of China University of Political Science and Law*, *4*(2023), 84-96.

Zhang, G. X. (2023). On Notice and Consent in the Processing of Private Information. *Journal of Southwest Petroleum University (Social Sciences Edition)*, *25*(05), 87-94.

Zhang, Z. W. (2022). *The Distinction Between Privacy and Personal Information: Judicial Determination Standards for Private Information* (Shanghai Law Studies Collection, 2022, Vol. 13—Emerging Rights and the Rule of Law in China, p. 11). Department of Law, Harbin Engineering University.