ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 3 - 2026

Factors influencing privacy predicaments of Chinese digital platform users: a grounded theory

Xinping Dong[1,*]

[1] Business School, Ningbotech University, Ningbo, Zhejiang, 315100, China

SUMMARY: *The privacy predicament is a new concept, which refers to a broad range of challenges and psychological burdens for digital platform users when dealing with privacy issues. Exploring the influencing factors and formation mechanisms of privacy predicaments of digital platform users can contribute to privacy governance. In the study, 28 digital platform users were comprehensively interviewed in a semi-structured format. Using grounded theory, the study identifies platform, user, national, and social factors that influence the formation of privacy predicaments. Among these factors, national and social factors are external causes of privacy issues, whereas user and platform factors are internal causes, and all have a causal relationship with the formation of user privacy predicaments. Privacy sentiment moderates the impact of social factors causing privacy predicaments. This study emphasizes that collaborative efforts from all actors, including users, digital platforms, and society, are needed to address privacy predicaments. The study provides specific guidelines for these efforts.*

KEYWORDS: *privacy predicament; digital platform users; grounded theory; Glaser and Strauss*

1 Introduction

Digital life has become an integral part of modern life. It completely changes how we do almost everything. With the growing importance of personal data in digital life, there has been a substantial increase in the concerns of digital platform users about the privacy and security of personal information. This increase is because users are losing control over their personal data, due to the rapid development of technologies for data transmission and collection (Hoofnagle et al., 2010). Moreover, the overuse of personal data from digital platforms, coupled with the frequent occurrence of data breaches, has intensified concerns about the privacy of users.

In response to user concerns about data collection, the IEEE Code of Ethics (IEEE, 2020) highlights the company's responsibility to oversee data collection practices and assist society and the public in understanding the technology involved. However, transparency remains an issue. For example, many digital platforms do not explicitly request permission for complete activity tracking, leaving platform users unaware of the extent of data monitoring (GAO, 2022). Even more concerning, some platforms' deceptive or illegal actions associated with data collection have undermined trust and raised ethical concerns. For example, Facebook's “tag suggestion” default function, which used facial recognition technology without user consent, was deemed to be a facial recognition tool, resulting in a $5 billion penalty in July 2019 for engaging in deceptive activities (Lankton et al., 2019).

Besides the inappropriate collection of personal information, data misuse is another

*dongye110@126.com
https://doi.org/10.65102/is20261145 Published: 10 June, 2026

significant privacy concern. Personalized services exemplify data misuse. Platforms utilize technologies such as artificial intelligence to provide tailored experiences, enhancing convenience but also raising concerns about potential privacy violations. For example, e-commerce platforms utilize various kinds of sensitive privacy information, such as customers' online browser history, personal shopping cart records, and payment histories, to provide personalized product recommendations and personalized pricing (Pilton et al., 2021). Clearly, such business practices significantly invade personal privacy.

Data breaches, often caused by hacking from external parties or errors by internal actors, pose a far greater threat to the security of personal information. In 2018, there were 53,308 cybersecurity incidents and 2,216 confirmed data breaches1 (Verizon, 2018). By 2023, although the number of security incidents decreased to 16,312, the number of breaches rose to 5,199 (Verizon, 2023). Notable incidents underscore the vulnerability of digital privacy. In 2014, Yahoo's data breach exposed information from 500 million accounts; eBay experienced a cyberattack that compromised the personal data of 145 million users, including encrypted passwords; In 2016, FriendFinder Networks was hacked, resulting in the leak of more than 412 million accounts. Despite these online privacy breaches prompting users to strengthen online privacy, such as tightening social media settings and adopting strong passwords, individual privacy remains vulnerable to breaches and unauthorized disclosures (Dhirani et al., 2023; Romansky & Noninska, 2020).

Countries worldwide place great importance on privacy protection legislation and have successively enacted a series of privacy-related laws and regulations. Developed economies are advanced in privacy legislation by continuously updating their regulation to meet the changing needs for personal information protection. The European Union (EU) enacted a comprehensive privacy legislation, the General Data Protection Regulation (GDPR), to govern how personal data can be processed and transferred on May 25, 2018. In 2022, building upon the GDPR, the Digital Services Act (DSA) and the Digital Markets Act (DMA) refined the EU legal framework to strengthen cyber security and openness in Europe. Unlike Europe, the United States has no national law for data privacy. However, half of the states, such as Virginia and Colorado, have enacted or are in the process of enacting their own data protection laws at the state level (Klosowski, 2021).

China has also developed its data protection regime. In August 2021, China established a fundamental privacy law, the Personal Information Protection Law. This law was followed by implementing the Network Data Security Management Rules in November 2021 and the Measures for the Security Assessment of Outbound Data Transfers in September 2022. These measures have together strengthened the existing Chinese legislative framework for data privacy and security. However, there are still criticisms about Chinese data protection regulations, particularly regarding the possibility of excessive surveillance under the pretense of national security (Zhao & Feng, 2021).

Despite these privacy protection laws and regulations, due to the limitations of the legislation itself (Hartzog & Richards, 2020) and inadequate enforcement (UNODC), the issue of privacy violations remains serious. Concerns about privacy and cybersecurity are widespread (Martin, 2020). An often-cited phrase, “Privacy Paradox”, precisely describes the situation of online users: Users claim to be very concerned about their privacy but still disclose information to obtain digital services (Barth & De Jong, 2017; Martin, 2020). Besides the privacy paradox, recent research also proposed several concepts, including privacy fatigue (Choi et al., 2018); privacy helplessness (Cho, 2022); privacy cynicism (van Ooijen et al., 2024); privacy indifference; privacy concern; privacy anxiety, to express the user’s challenge and negative attitude towards dealing with personal privacy. This study condenses these phrases into the notion of “privacy predicaments” to streamline the investigation into the range of personal

issues related to privacy.

This research aims to explore the factors and mechanisms that contribute to the privacy predicaments of Chinese digital platforms users. Finding the cause of privacy predicaments and addressing the issue with tailored solutions is important not only for individuals but also for internet businesses, governments, and society (Clarke, 1999; H. Li et al., 2017). Using grounded theory coding of 28 semi-structured interviews, we explain how various factors at the platform, user, societal, and national levels shape privacy predicaments. This study has two main contributions to the literature. First, we clearly define privacy predicaments and elucidate the roles of the key actors—such as platforms, users, and governments—along with the cultural and historical factors influencing these predicaments. Second, based on our findings, we offer targeted recommendations on privacy governance, providing actionable guidance to the stakeholders involved.

The paper proceeds as follows. Section 2 reviews the privacy-relevant literature and defines what the privacy predicament is. Section 3 describes the design of our semi-structured interview. Section 4 introduces the coding process. Section 5 explains the findings. Section 6 discusses, and Section 7 concludes.

2 Fundamental Concepts

2.1 Privacy

Tracing the origins of privacy, people's understanding of privacy initially stemmed from a sense of shame, particularly in relation to intimate and physical secrets. It is also from this feeling of shame that people start to set themselves apart from animals. As socially productive forces have progressed, the boundaries of privacy have expanded significantly. Today, privacy is acknowledged as a fundamental right. Justice Louis Brandeis and Samuel Warren wrote “The Right to Privacy” in 1890, which is considered the first publication to argue for a right to privacy. They conceptualized the privacy right as “the right to be let alone” and sought to “protect the privacy of the individual’ from the law.” Westin (1968) defined privacy in the light of self-determination as “the claim of individuals … to determine for themselves when, how and to what extent information about them is communicated”, which set the foundation for debates about modern privacy. We consider that as information, privacy is personal matters and secrets that do not wish to be disclosed or made public, or simply personal affairs or secrets unrelated to the public interest. As a right, privacy can be defined as a right to control one's personal information and the right to be left alone, free from surveillance or interference by others (Solove, 2002; Thomson, 1975).

The concept of privacy can be broadly divided into two main categories: physical privacy and information privacy (Talukdar, 2019). In the current digital era, information privacy has become the primary area of research concentration. When accessing the internet, individual and consumer privacy rights are often called digital privacy. Digital privacy can be further categorized into information privacy, communication privacy, and individual privacy (Hung & Wong, 2009). Digital privacy is now a multifaceted concept that varies in its definition and application depending on the context and disciplinary focus (Smith et al., 2011). For example, legal scholars analyze legal frameworks concerning privacy, sociologists study social norms and behaviors related to privacy, and economists investigate the cost-benefit trade-off of protecting privacy. Additionally, technologists create algorithms and solutions for issues related to digital privacy.

Privacy perceptions vary not only over time but also among different countries, communities, cultural origins, and even individuals (Y. Li et al., 2017; Zwick & Dholakia, 1999).

Nissenbaum (2004) introduced the concept of "contextual integrity of privacy," which suggests that privacy expectations and norms vary across different contexts. Alaggan et al. (2015) introduced the concept of "heterogeneous differential privacy" and presented a novel mechanism designed to capture variations in privacy expectations among users, as well as across different pieces of information related to the same user.

2.2 Privacy Predicament

This study focuses on the privacy predicaments that digital platform users are facing. Privacy predicament is not a new word in the existing research. Fazlioglu (2024) described the privacy predicament as an unfortunate circumstance where users care about their information but are incapable of protecting it. Bandara et al. (2020) used the privacy predicament to present the situation where "consumers are increasingly worried about their privacy and behave in a manner that can be detrimental to the consumer-vendor relationship." Other scholars also mentioned the term "privacy predicament," but there is still no clear definition or explanation of the idea (Huang & Bashir, 2015; H. Li et al., 2017; Wang, 2014). It is essential to define the concept of privacy predicament and differentiate it from privacy paradox and privacy dilemma, which have similar implications.

The privacy predicament, the privacy paradox, and the privacy dilemma each carry a unique meaning, but can be interrelated in some contexts. Privacy paradox refers to the phenomenon where people express a high value for privacy theoretically but frequently share personal information online in practice, with an emphasis on the contradictory user's behavior and their concerns (Norberg et al., 2007). The privacy dilemma emphasizes the user's difficulties in choosing between sharing personal information and protecting their privacy. Burkhardt (2018) stated that the "privacy paradox is a privacy dilemma" because people are unable to make choices or must disclose their own information in order to obtain services, leading to the privacy paradox. Privacy predicaments emphasize the broad range of challenges and psychological burdens individuals face when dealing with privacy issues, including but not limited to the privacy paradox and privacy dilemma.

In our understanding, a privacy predicament refers to specific negative emotional states, such as feelings of helplessness, betrayal, loss, anger, or indifference, that individuals experience in response to consistent concern for privacy or even perceived loss of control over their privacy. The terms privacy fatigue (Choi et al., 2018), privacy helplessness (Cho, 2022), privacy cynicism (van Ooijen et al., 2024), privacy indifference, privacy concern, and privacy anxiety are all considered manifestations of privacy predicament. Compared to the privacy paradox and privacy dilemma, the term privacy predicament offers a more comprehensive view of the complex nature of users' privacy issues. It emphasizes not only the users' paradoxical circumstances and decision-making challenges but also their emotional and psychological states.

3 Research Methodology

3.1 Design

Grounded theory, first developed by Glaser and Strauss, is one of the most widely used qualitative research approaches in philosophy and social sciences (Glaser & Strauss, 2017). Grounded theory allows for examining particular processes or phenomena and developing new theories based on real-world data acquired (Jia, 2016). It is particularly well suited to understanding complex or evolving phenomena, as well as the intricate social processes, interactions, and behaviors underlying these phenomena (Charmaz, 2006). Therefore, we

employ grounded theory to systematically build a theoretical framework for the privacy predicament and investigate the factors affecting it.

This paper starts with semi-structured interviews with digital platform users, followed by the collection of raw data. The raw data is then analyzed using open, axial, and selective coding according to the grounded theory guidelines (Birks & Mills, 2015). We continue this process until we achieve saturation. Finally, the study develop a model of the factors that influence digital platform users' privacy predicaments.

3.2 Data Collection

The data for this study comes from in-depth interviews with users of digital platforms. The selection criteria for interviewees include the following: first, the participants need to possess a basic understanding of and familiarity with digital platforms; second, they must agree to the interview and be recorded after being informed of the research purpose. Considering the participants' ability to understand the research questions and the fact that the primary audience of Chinese digital platforms is youth, this study primarily selects university students and young professionals as our interviewees. Young online users have rich experience in web surfing and a basic knowledge of what privacy is. Ultimately, 28 participants are recruited for interviews.

This study uses in-person and virtual interviews, with each interview lasting between 20 and 30 minutes. All interviews are conducted in Chinese. The interviews are fully recorded with the permission of the participant. The recordings are first transformed into text files using transcription software; we then listen to the interviews again to review the text files, generating the final raw interview texts with about 50,000 Chinese characters. We randomly select 24 interview documents for three-level coding and theoretical model construction, while the remaining four are used to verify theoretical saturation.

Semi-structured in-depth interviews are conducted to ensure that the interviews adequately capture the privacy challenges encountered by users. The interviews are organized around a set of topics related to the current privacy status of the interviewees and the reasons behind privacy predicaments, including the privacy concerns the interviewees encountered, the decision the users made regarding the disclosure of private data, the psychological feelings and emotions of the users, and views regarding social privacy norms and national regulations. The outline of the interview is shown in Supplementary S1.

4 Data Analysis

The procedural grounded theory approach can be divided into four steps: open coding, axial coding, selective coding, and checks for theoretical saturation. This paper encodes the factors influencing the privacy predicaments of digital platform users according to these four steps. During the coding process, we independently code the raw interview materials, and then the coding results from different members of our team are compared and integrated. For portions where the coding is inconsistent, we conduct analysis and discussion until an agreement is reached.

4.1 Open coding

Open coding is the process of conceptualization and categorization applied to the original interview data, which results in the establishment of initial categories. To accurately represent the interview information, during the open coding process, we code the interview data sentence by sentence using appropriate language. Through the open coding process of the interview

documents, a total of 349 concepts and 187 initial categories are obtained. Supplementary Table S2.1 provides examples of the open coding process.

4.2 Axial Coding

Axial coding involves sorting and organizing large amounts of open-coded data to clarify their logical relationships. This process then reassembles these initial categories into more abstract conceptual categories, known as main categories. We analyze the 187 initial categories derived from open coding and group them into 18 main categories (B1-B18), which include the initial state of platform privacy, platform privacy behavior, user privacy outcomes, and more. This procedure considers the characteristics of the research subject and the research objectives, as well as the logical relationships between the initial categories. Table 1 displays 7 of the 18 main categories; see Supplementary Table S2.2 for details on all main categories.

Table 1: Axial Coding Results

Category	Main (Secondary) Category
Differentiated Data Collection	Platform privacy initial state(B1)
Platform Responsibility	
Scale of Digital Platform	
Professional Legal Team	
Platform Self-regulation	Platform privacy behavior (B2)
Platform Algorithms	
Data-trading Practices	
Privacy Theft	
Forced Consent	
Group Classification	
Privacy Overreach	
Liability evasion for privacy misconduct	Platform privacy outcome (B3)
Low Legal Costs	
Lack of Privacy Trust	
Prevalence of Malware Threats	
Incomplete Privacy Protection System	
Profit Driven	Platform privacy motivation (B4)
Convenience in Providing Services	
Information Security Assurance	
Data Exclusivity	
Platform Dependence	User privacy initial state(B5)
Vulnerable Position	
Privacy Awareness	
Leakage of Identification Information	
Privacy Concern	
User Personality	
Choice Between Platforms	User privacy behavior (B6)
Privacy Trade-off Decision	
Minimal Effort on Privacy	
Demanding Explanations from Platform	
Self-Protection	
Legal Rights Maintenance	
Reducing Usage	
Privacy Complaints	
Privacy Concern	User privacy sentiment (B7)
Privacy Dissatisfaction	
Privacy Indifference	
Privacy Disappointment	
Privacy Sympathy	

4.3 Selective Coding

Next, in the selective coding process, we conduct a comparative analysis of the categories we obtained from the axial coding process. The goal of this process is to identify the core categories that organically connect all secondary categories. Then a storyline is created describing the relationships among the core categories, the main categories, and the concepts. The 18 main categories are classified into four main core categories, such as platform factors, user factors, national factors, and social factors. These influencing factors are then used to develop the influencing factor model. The results of selective coding are shown in Table 2.

Table 2: Selective Coding Results

Typical relationship structure	Relationship	Connotation of relationship structure
Platform Factor → Privacy Predicament	Causal relationship	The initial privacy state of the platform, platform motivations, platform behavior, and the outcomes of platform privacy are key factors in the formation of privacy predicaments.
User Factor → Privacy Predicament	Causal relationship	The initial state of user privacy, user privacy sentiments, user privacy motivations, user privacy behaviors, and the outcomes of user privacy are key factors in the formation of privacy predicaments.
National Factor → Privacy Predicament	Causal relationship	The initial privacy state of the nation, national privacy motivations, national privacy behavior, and the outcome of national privacy are key factors in the formation of privacy predicaments.
Social Factor → Privacy Predicament	Causal relationship	Privacy culture, privacy environment, privacy history, privacy ethics, and privacy incidents are key factors that lead to the formation of privacy predicaments.
Privacy Sentiment ↓ Social Factor → Privacy Predicament	Moderating relationship	Privacy sentiments can moderate the impact of social factors on the formation of privacy predicaments for users.

As shown in Table 2, platform factors, user factors, national factors, and social factors all have a causal relationship with the formation of privacy predicaments. Additionally, privacy sentiments have a moderating effect on the relationship between social factors and the formation of privacy predicaments. Privacy sentiment, influenced by social factors such as privacy culture, history, and social events, has been found to exacerbate privacy predicaments (Goetzen et al., 2021; Westin, 2003). The Edward Snowden case, which brought the subject of privacy to the forefront, exemplifies the moderating role of privacy sentiment. As revelations from the Snowden affair emerged in the media and on social media, an increasing number of people expressed dissatisfaction with the spying. Their social media debates raised public awareness of privacy intrusions, which has further intensified privacy predicaments. However, such sentiment not only exacerbates already-existing privacy predicaments, but it also helps platforms and governments make the required changes, which in turn lessens the chance that similar situations will arise in the future.

Through the analysis of main and core categories, the pathways of influence between categories are identified, ultimately determining the theoretical framework of the model of the

formation of privacy predicaments. The model is shown in Figure 1. We will provide more detailed explanation in Section 5.

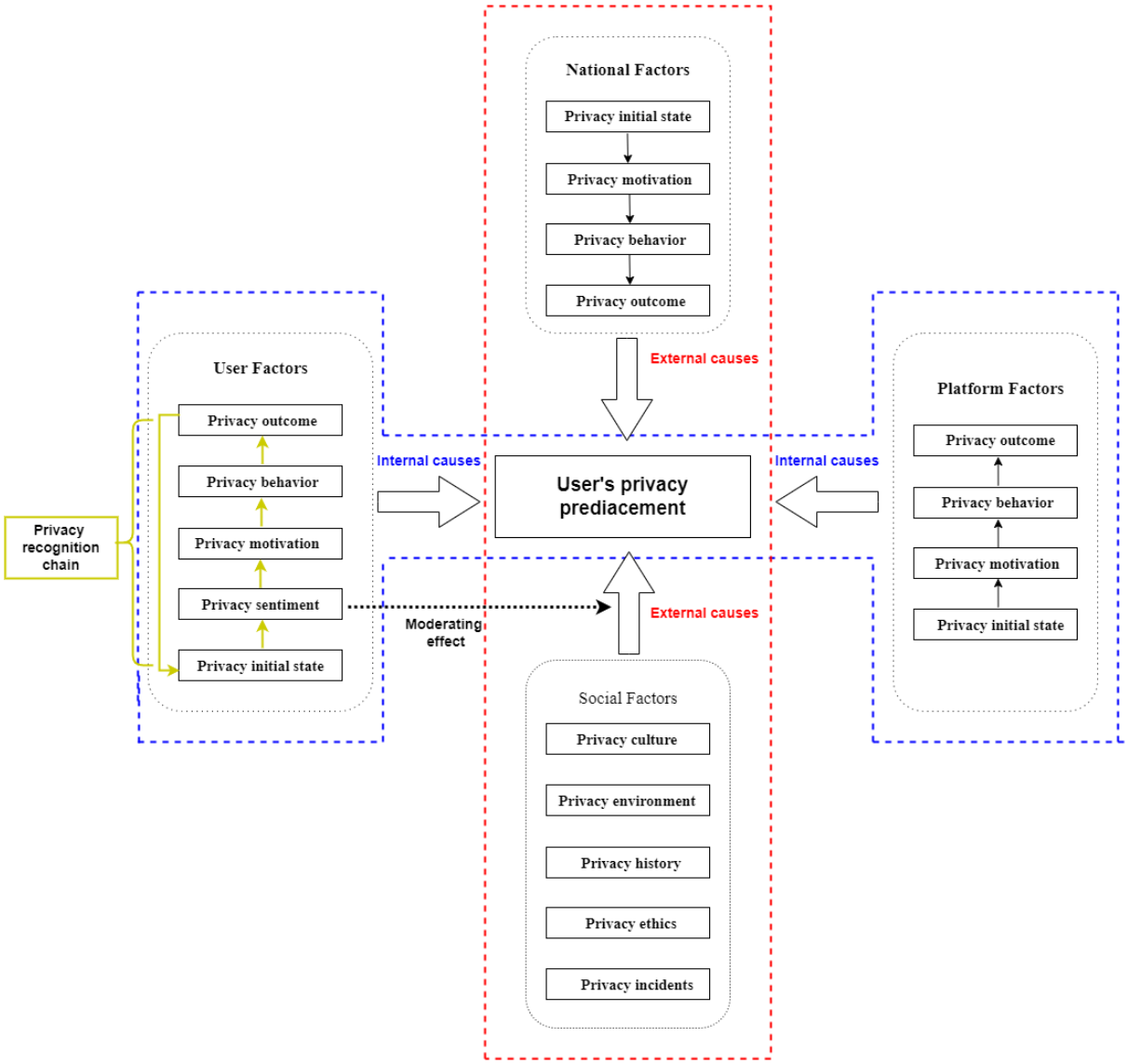

Figure 1: The influencing factor model of the formation of the privacy predicament

4.4 Theoretical Saturation Test

This study utilizes the four interview documents to test theoretical saturation. The results do not reveal new concepts or categories, which confirm that the extraction of concepts from the interview data is sufficient, and the study achieves theoretical saturation.

5 Analyzing Factors Influencing Privacy Predicaments

As the framework of Figure 1 shows, platform factors, user factors, national factors, and social factors are all significant influences in the formation of privacy predicaments among digital platform users, each having a causal relationship with these predicaments. These factors interact and constrain each other. National and social factors are external causes of privacy predicaments, while platform and user factors serve as internal causes.

5.1 Platform Factors

Proposition 1: Platform factors are the internal causes of privacy predicaments. Within the platform factors, the subfactors, including platform privacy initial state, privacy motivation, privacy behavior, and privacy outcomes, are progressive and interconnected.

The **initial state of platform privacy** refers to a digital platform's status as it attempts to balance its utilization of private information and privacy protection. It includes the platform's responsibility, scale, strategies for collecting and processing privacy information, legal teams, and more. A platform's attitude towards social responsibility can have a significant impact on its conduct on privacy. Some platforms feel obligated to protect users' privacy, but some put their own interests over users' privacy experiences. Also, platforms at different stages of business growth and of different scales adopt different standards to assess privacy risks and implement specific strategies to manage privacy data. In general, users perceive that larger platforms are more cautious with personal data because they take privacy risks more seriously. Some interviewees expressed their concerns about small-scale platforms:

"... I am okay with large digital platforms, but I hesitate to use small platforms, particularly those that ask me to enter a lot of personal information."

As the user's awareness of privacy increases, privacy-related lawsuits and complaints are continually arising. Platforms that possess professional legal teams with strong capabilities to handle privacy disputes are more emboldened to adopt aggressive privacy policies. The following statement reflects that users often feel powerless to defend their rights against the legal power of large corporations.

"If I hire a lawyer or defend my rights myself, the money and effort I invest will be quite high. The probability of success is very low, and even if I succeed, I suppose that the compensation is between 50,000 and 100,000 yuan; the time and effort I spend might exceed this value."

Platforms use personal data for certain objectives; this is **platform privacy motivation**. The platform's privacy motivation includes profit-driven motives, convenience in providing services, information security assurance, and data exclusivity. Unlike typical manufacturing enterprises, a digital platform within a conglomerate often serves to obtain group benefits through diverse digital services. That is, these services must address the needs of both the conglomerate and the platform's end customers. For example, Taobao, a subsidiary e-commerce platform of Alibaba, has launched functions like 'thousands of faces' and 'tailored recommendations' that collect extensive personal digital footprints. These functions not only improve user shopping efficiency, but also improve marketing precision and help Alibaba develop new products and services. Thus, the primary motivation of a platform's privacy strategy still seems to be to maximize the benefit of the conglomerate.

Platform privacy behavior is one of the main reasons for the formation of privacy predicaments among digital platform users. Recall that the initial state and motivation differ, as do its privacy behavior. Platform privacy behavior includes platform self-regulation, platform algorithms, forced consent, privacy theft, data-trading practices, and so on. Since a single privacy incident can lead to disastrous consequences, all platforms' operations, including commercial behaviors and data processes, are subject to a degree of privacy self-regulation. However, due to their dominant position over users, platforms often engage in inappropriate practices like promoting forced consent, data trading, and misusing information, which lead to user dissatisfaction, for instance:

"For example, with the platform's privacy policy, if I don't check the box to agree, you can't use the service. It forces me to check the box to agree."

"... real estate agents buy your location information through platforms and then keep bothering you with telemarketing calls, it becomes extremely annoying."

The last platform factor is the **platform privacy outcomes**. The impact of the platform privacy outcome on privacy predicaments can be direct or may follow a sequence from the platform's initial privacy state through platform motivation and behavior, as shown in Figure 1. Research interviews indicate that users generally hold negative opinions towards platform privacy outcomes. Our interviewees expressed doubt over the platforms' efforts to protect privacy, as well as dissatisfaction with the low cost of privacy violations and widespread malware threats. They also call for a comprehensive privacy protection framework and the establishment of accountability measures for platforms.

5.2 User Factors

Proposition 2: Platform user factors, including subfactors such as initial privacy state, sentiment, motivation, behavior, and outcome, are internal causes of privacy predicaments. Each of these subfactors can independently influence privacy predicaments or work in a progressive sequence, transmitting their effects one after the other and ultimately impacting the predicament through the outcomes.

The **initial privacy state of platform users** is the privacy status of users at the early phase of their contact with the platform. This encompasses users' reliance on the platform, users' privacy awareness, user personality, and so on. Users and digital platforms build their relationships based on mutual needs. As the user's reliance on the platform grows, the platform's dominant position becomes more apparent. Simultaneously, users become more aware of and concerned about their privacy issues as their own privacy personalities begin to take shape. We find that most users feel that they are in a passive and vulnerable position when it comes to privacy protection, leading to privacy predicaments.

"E-commerce platforms are powerful, and I'm part of a group that's relatively weaker compared to them. I must play along with them; I don't really have any privacy right..."

User privacy sentiment refers to the attitude and emotion users hold towards personal privacy. These include privacy concerns, privacy complaints, privacy aversion, privacy indifference, etc. During the use of digital platforms, users directly experience and feel how their privacy is managed, which evolves into psychological activities and emotional expressions, forming what we call privacy sentiments. In addition to experiences on the platform, factors such as socioeconomic background, privacy history, privacy ethics, and past privacy incidents also influence privacy sentiments. We find that almost all interviewees had unfavorable sentiments about privacy, and if these feelings persist, they can contribute to the formation of privacy predicaments. As an example,

"(When my privacy is invaded) I often don't know what to do. Sometimes I get very upset and frustrated. Other times, I'm genuinely angry, and I end up venting to my classmates and friends about it. In my mind, I've concluded that we're powerless against platforms; they're too ruthless. I don't know how they manage to get my information, nor do I know how to protect my rights."

Another interviewee said: "I complain about how the platform invades my privacy, and over time, I just let it go..."

User privacy motivation refers to the motivation behind users' privacy decisions when using a platform. These motivations can vary widely. Some users desire convenience and a smooth experience on the platform over privacy protection. Some users have a herd mentality that aligns with peer privacy settings. In addition, certain users prioritize safeguarding both life and property, making efforts to prevent any problems caused by privacy breaches. These varied motivations lead to differing perspectives towards platform services. In our interviews, some interviewees favor functions of personalized recommendation, since they expect platforms to provide tailored services based on their needs. However, others are unwelcome to such

personalized recommendations since they consider the digital footprints collected by platforms to be private and sensitive and want their information and preferences to be kept private from platforms and third parties.

User privacy behavior is driven by their privacy motivations, including platform choice, reduced usage, privacy trade-off decisions, asking for explanations from the platform, etc. Users' privacy behaviors are relative to the platforms' privacy behaviors. Generally, when users are satisfied with a platform's privacy behaviors, their own privacy behaviors are cooperative. On the contrary, dissatisfaction leads to more negative behaviors. From the interviews, interviewees' cooperation with the platform's privacy measures is often conditional, for instance:

"... if I really want to buy something (on the platform), I'll first comply with the (privacy) requirements to make a purchase, and then after I've completed my transaction, I'll disable the relevant features."

User privacy outcomes result from the interactions between users and digital platforms concerning privacy. These outcomes include losing control over personal information, difficulty in enforcing privacy rights, privacy paradox, information cocoons, and so on. User privacy outcomes can either directly lead to privacy predicaments or do so through a sequential process involving various stages of the privacy recognition chain, including initial state, emotions, motivations, behaviors, and final outcomes. The privacy outcome is the final stage in the chain of user privacy recognition. However, in a new privacy environment, these outcomes may transform into a new initial privacy state and start a new cycle of privacy recognition. This process constructs a closed loop of privacy recognition.

5.3 National Factors

Proposition 3: The factors of national privacy include the initial state of national privacy, national privacy motivations, national privacy behavior, and national privacy outcomes, all of which progressively influence one another. National privacy factors are external causes of privacy predicaments.

The initial state of national privacy includes government privacy responsibilities and privacy laws and regulations. The nation has the duty to set baselines to safeguard national digital security and enact privacy regulations to protect the interests of the people, all aimed at ensuring the orderly operation of society.

National privacy motivations include economic stimulation, promoting technological development, fostering win-win outcomes between platforms and users, and enhancing national cybersecurity. Appropriate privacy legislation and regulation not only help balance the interests of users and platforms, but also lay a solid foundation for protecting national cybersecurity. Additionally, allowing platforms, governments, and other organizations to utilize personal data in an appropriate way can improve people's lives, stimulate economic growth, and promote social progress, particularly in the era of big data.

National privacy behaviors include providing privacy guidance, privacy supervision, and implementing governmental privacy policies, among other actions. To realize national privacy motivations, the government continually refines and enforces privacy policies and regulations, enhances privacy protection measures, and executes its regulatory duties.

China's present **national privacy outcomes** are characterized by insufficient privacy laws and lenient privacy regulations. China's national strategy focuses on economic development and national security due to its socioeconomic status. As a result, China's regulations on privacy protection are relatively lax. Furthermore, as China's privacy regime is newly established, compared to developed countries, China's privacy laws and regulations have deficiencies. Our interviewees expressed a strong desire for improvements in both legislation and regulation, for instance,

"Actually, I feel that (compared to relying on corporate responsibility), it is more crucial that the national authorities intervene more significantly in addressing privacy issues."

5.4 Social Factors

Proposition 4: Social factors, including privacy culture, privacy environment, privacy history, privacy ethics, and privacy incidents, are external causes of the formation of privacy predicaments. Each of these subfactors independently impacts privacy predicaments.

Privacy culture and privacy history indirectly impact the formation of privacy predicaments. It is widely acknowledged that China's cultural tradition of collectivism, which favors group interests over personal interests, promotes social cohesion and harmony at the expense of individualism. Historical practices ranging from the strict surveillance of the Qing Dynasty's household registration system to the extreme invasions of personal life during the Cultural Revolution highlight this prioritization of the collective. These cultural traditions and norms contribute to less emphasis on individual privacy among Chinese people. For instance, most Chinese are comfortable with the extensive use of closed-circuit television (CCTV) cameras on the streets (Liu, 2022). Similarly, digital platform users frequently consent to compromises on their personal privacy for the collective interests. For example, users willingly shared location data to aid in public health management during the pandemic. This cultural and historical influence is also reflected in national surveillance requirements that prioritize public safety over individual privacy rights. In China, legislation and policy frameworks often support extensive data collection and monitoring practices, such as the use of facial recognition technology, justified by the need to maintain social stability and security.

Privacy environment, including completeness of laws and regulations, consensus on corporate privacy responsibilities, and individual privacy awareness, also indirectly influence the formation of privacy predicament. The privacy environment is closely linked with the privacy behavior and outcomes of nations, platforms, and users. If privacy laws are insufficient, platforms might exploit loopholes. If there is a lack of consensus on the privacy responsibility of platforms, they may put economic interests ahead of user privacy protection. Furthermore, low awareness of privacy among citizens could increase the difficulty of protecting privacy, lead to more frequent privacy violations, and increase the likelihood of a privacy predicament.

Privacy ethics refers to moral principles about how personal information should be respected and protected. Good privacy ethics should help platforms, governments, and individuals maintain individual dignity and enhance personal privacy. Privacy ethics are shaped by the interplay of legislation, social advocacy, and corporate practices. These privacy ethics, in turn, regulate and direct platforms to follow data protection standards. If platforms can conscientiously uphold privacy ethics and conform to privacy standards, it will help to avert privacy predicaments and establish a privacy-conscious culture.

Privacy incidents also indirectly influence the formation of privacy predicaments. In recent years, with the rapid development of information technology and big data technologies, incidents of personal privacy breaches have occurred frequently. Our results show that significant privacy incidents affect public privacy perceptions and behaviors. People learn a lot about protecting privacy from these incidents, sometimes more effectively than through educational institutions and public awareness campaigns.

6 Discussion

Privacy predicaments not only disrupt users' online experiences and intrude into their personal lives, but also disrupt social harmony, impede the growth of platforms, and even hinder national

digital development. Therefore, it is imperative that all parties take privacy protection seriously. We have discussed how platform, user, national, and social factors contribute to the formation of privacy predicaments in China. Building on our findings, we now provide some recommended strategies from the perspectives of the government, internet companies, society, and internet users, emphasizing that solving these privacy issues requires the collective effort of all stakeholders involved to ensure effective resolutions. The suggestions are as follows:

Users are the primary 'victims' of privacy predicaments. Our analysis reveals that many Chinese platform users lack awareness of privacy issues, often viewing privacy protection as the government's responsibility rather than their own. However, as the main beneficiary of privacy protection, users must actively engage in safeguarding their own data. If users do not prioritize data privacy and understand the data policy, privacy protection will become exceptionally challenging.

Digital platforms play a crucial role in protecting privacy as they manage personal data—from collection and processing to dissemination and application. Any lapses in these processes can expose user information, underscoring the importance of these platforms' proactive privacy measures. We find that users frequently express dissatisfaction with the lack of privacy action by social and shopping platforms. Therefore, to address users' privacy concerns, digital platform companies should adhere to privacy legislation and ethics and actively prioritize protecting privacy rather than exploiting loopholes in privacy rules. Specifically, as the interviewees noted, platforms need to improve their practices regarding user consent, privacy policies, and data trading, among other areas, to better protect user privacy.

Although the national government does not directly participate in the interactions between users and platforms, it still has a significant impact on privacy protection, especially in the context of China. We find that users hold the government to high expectations when it comes to protecting their privacy, as they urge the government to resolve privacy disputes between users and platforms, quickly, fairly, and rigorously, ensuring their privacy is well-protected. It is recommended that the government enhances legislation to keep pace with the rapid advancements in technology and the evolving tactics of data misuse, encourages digital platforms to be more transparent about how they use and share user data, and strengthens the regulation on data protection.

Various social factors, including privacy history, culture, environment, ethics, and incidents, impact the privacy protection ecosystem. Society's influence on privacy is continuous and profound, making it crucial for shaping a civilized and healthy privacy protection environment. Therefore, it is essential that entities at all levels, such as media outlets and research institutions, recognize privacy predicaments and provide strong support for personal privacy protection.

7 Conclusion Remarks

This study employs grounded theory to investigate the formation of privacy predicaments among users of digital platforms. By analyzing data from semi-structured interviews, the study reconstructs users' experiences and feelings during their interactions with platforms. The study develops a theoretical framework that shows how user, platform, national, and social factors influence users' privacy predicaments. The study also provides practical recommendations to mitigate privacy predicaments.

This study acknowledges certain limitations. First, the formation of privacy predicaments on digital platforms is a complex process. As such, the propositions and conclusions drawn from this qualitative research require further investigation and validation. Secondly, since this study focuses on Chinese internet users, the findings may only apply to some national and cultural settings. Lastly, concepts such as privacy predicaments and privacy recognition chains

are newly introduced. Our discussion may capture only some of their complexities, suggesting that more research is needed to fully understand these critical privacy aspects.

Acknowledgements

Thanks: Privacy paradox experiment and privacy responsibility of Zhejiang Internet platform enterprises (23NDJC054Z). This research is supported by Zhejiang Provincial Philosophy and Social Science Planning Project in China.

Author Introduction

Dong Xinping (1973.05-), male, PhD, Associate Professor at Ningbotech University.

References

[1] Alaggan, M., Gambs, S., & Kermarrec, A.-M. (2015). Heterogeneous differential privacy. *arXiv preprint arXiv:1504.06998*.

[2] Bandara, R., Fernando, M., & Akter, S. (2020). Addressing privacy predicaments in the digital marketplace: A power-relations perspective. *International Journal of Consumer Studies, 44*(5), 423-434.

[3] Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and informatics*, *34*(7), 1038-1058.

[4] Birks, M., & Mills, J. (2015). *Grounded theory: A practical guide*. Sage.

[5] Burkhardt, K. (2018, April 1). The privacy paradox is a privacy dilemma. https://blog.mozilla.org/en/products/firefox/the-privacy-paradox-is-a-privacy-dilemma/

[6] Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. sage.

[7] Cho, H. (2022). Privacy helplessness on social media: Its constituents, antecedents and consequences. *Internet Research*, *32*(1), 150-171.

[8] Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42-51.

[9] Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60-67.

[10] Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: a review. *Sensors*, *23*(3), 1151.

[11] Fazlioglu, M. (2024). Overcoming the AI Privacy Predicament. *Infosecurity Magazine*. Retrieved April 10 from https://www.infosecurity-magazine.com/opinions/overcoming-ai-privacy-predicament/

[12] GAO, U. S. (2022). *Consumer Data: Increasing Use Poses Risks to Privacy*.

[13] Glaser, B., & Strauss, A. (2017). *Discovery of grounded theory: Strategies for qualitative research*. Routledge.

[14] Goetzen, A., Dooley, S., & Redmiles, E. M. (2021). Ctrl-Shift: How privacy sentiment changed from 2019 to 2021. *arXiv preprint arXiv:2110.09437*.

[15] Hartzog, W., & Richards, N. (2020). Privacy's constitutional moment and the limits of data protection. *BCL Rev.*, *61*, 1687.

[16] Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *Available at SSRN:* https://ssrn.com/abstract=1589864

[17] Huang, H. Y., & Bashir, M. (2015). Direct-to-Consumer genetic testing: Contextual privacy predicament. *Proceedings of the Association for Information Science and Technology*, *52*(1), 1-10.

[18] Hung, H., & Wong, Y. H. (2009). Information transparency and digital privacy protection: are they mutually exclusive in the provision of e-services? *Journal of Services Marketing*, *23*(3), 154-164. https://doi.org/10.1108/08876040910955161

[19] IEEE. (2020). *IEEE Code of Ethics*. Retrieved April 10 from https://www.ieee.org/about/corporate/governance/p7-8.html

[20] Jia, X. H., Liang. (2016). Research on the Paradigm of Chinese Indigenous Management Theory Building Bases on the Grounded Spirit. *Chinese Journal of Management, 13(03)*, 336-346. https://doi.org/10.3969/j.issn.1672-884x.2016.03.003

[21] Klosowski, T. (2021, March 11). The State of Consumer Data Privacy Laws in the US (And Why It Matters). https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

[22] Lankton, N. K., McKnight, D. H., & Tripp, J. F. (2019). Understanding the antecedents and outcomes of Facebook privacy behaviors: An integrated model. *IEEE Transactions on Engineering Management*, *67*(3), 697-711.

[23] Li, H., Luo, X. R., Zhang, J., & Xu, H. (2017). Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information & management*, *54*(8), 1012-1022.

[24] Li, Y., Kobsa, A., Knijnenburg, B. P., & Nguyen, M. C. (2017). Cross-cultural privacy prediction. *Proceedings on Privacy Enhancing Technologies*.

[25] Liu, C. (2022). Who supports expanding surveillance? Exploring public opinion of Chinese social credit systems. *International Sociology*, *37*(3), 391-412.

[26] Martin, K. (2020). Breaking the privacy paradox: the value of privacy and associated duty of firms. *Business Ethics Quarterly*, *30*(1), 65-96.

[27] Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, *79*, 119.

[28] Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, *41*(1), 100-126.

[29] Pilton, C., Faily, S., & Henriksen-Bulmer, J. (2021). Evaluating privacy-determining user privacy expectations on the web. *computers & security*, *105*, 102241.

[30] Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, *17*(5), 5288-5303.

[31] Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 989-1015.

[32] Solove, D. J. (2002). Conceptualizing privacy. *Calif. L. Rev.*, *90*, 1087.

[33] Talukdar, S. (2019). Privacy and its Protection in Informative Technological Compass in India. *NUJS L. Rev.*, *12*, 287.

[34] Thomson, J. J. (1975). The right to privacy. *Philosophy & Public Affairs*, 295-314.

[35] UNODC. *Teaching Module Series: Cybercrime*. United Nations Office on Drugs and Crime. Retrieved April 1 from https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime.html

[36] van Ooijen, I., Segijn, C. M., & Opree, S. J. (2024). Privacy cynicism and its role in privacy decision-making. *Communication Research*, *51*(2), 146-177.

[37] Verizon. (2018). *2018 Data Breach Investigations Report*. https://www.verizon.com/business/en-nl/resources/reports/DBIR_2018_Report.pdf

[38] Verizon. (2023). *2023 Data Breach Investigations Report*. Retrieved April 10 from https://www.verizon.com/business/resources/reports/dbir/

[39] Wang, Q. (2014). Characteristics of social media communication and privacy predicament. *Forward Position 6*, 20-22.

[40] Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.

[41] Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of social issues*, *59*(2), 431-453.

[42] Zhao, B., & Feng, Y. (2021). Mapping the development of China's data protection law: Major actors, core values, and shifting power relations. *Computer Law & Security Review*, *40*, 105498.

[43] Zwick, D., & Dholakia, N. (1999). Models of privacy in the digital age: Implications for marketing and e-commerce. *Research Institute for Telecommunications and Information Marketing, University of Rhode Island*.