GEOPRIVACY KNOWLEDGE, ATTITUDES, AND BEHAVIORS IN CONTEMPORARY CHINA

Hongyu Zhang[a]* and Grant McKenzie[b]

[a] *Department of Earth, Geographic, and Climate Sciences, University of Massachusetts Amherst, Amherst, United States*

[b] *Department of Geography, McGill University, Montreal, Canada*

*honzhang@umass.edu

ABSTRACT. China has an Internet penetration rate of over 70 percent and a massive user base of social media. However, the topic of privacy attitudes among Chinese individuals remains understudied. We analyzed geoprivacy concerns in China through an online survey and regression analysis. Our findings suggest a positive relation among privacy knowledge, attitude, and behavior, consistent with related literature. Declarative knowledge (such as privacy rights), on the other hand, was found to have a negative relation with privacy concerns, which has not been reported previously. In terms of demographic moderators, females had less privacy knowledge but more privacy protection behaviors, while the impact of age on privacy concerns was inconclusive. A notable discovery was the regional difference in privacy concerns within China, suggesting the potential geopolitical influence on individuals' values and beliefs. Combined with the uncovering of behavioral change in response to involuntary location disclosure, the results of this article challenge the conventional notion that Chinese individuals are indifferent to their online privacy, thus reintroducing an underexplored perspective from the Global South into geoprivacy studies.

Keywords: geoprivacy, privacy concerns, knowledge, attitude, behavior, China.

Cite this article: Zhang, H., & McKenzie, G. (in press). Geoprivacy knowledge, attitudes, and behaviors in contemporary China. *Geographical Review*. doi: 10.1080/00167428.2024.2422873

The development of the World Wide Web and ubiquitous computing fosters an online environment that encourages information sharing. At the same time, users' perceptions of online privacy risks persist substantially. During the pandemic, users' geoprivacy concerns have been scrutinized and reexamined as many COVID-19 control measures have relied on individual-level geodata (Cann and Price 2023; Kwan and others 2023). People's views on geoprivacy may have changed in the post-COVID context. Therefore, measuring individuals' levels of privacy concerns is both necessary and timely, as it represents a critical pathway toward privacy-aware design.

This article examines geoprivacy concerns arising from geosocial media platforms such as WeChat, Weibo, and Douyin, which enable users to share location information. Our society needs to be cautious about prevalent location data collection in essential online services and interactions. China, as an authoritarian state, was able to implement a widely applicable rule of compulsory location disclosure. By the end of April 2022, the Internet-protocol-based location (or IP location) feature has been universally adopted on all major Chinese social media, including versatile platforms such as WeChat that can be difficult to break away from. Displayed at the provincial level for Chinese and country level for overseas IPs, the feature is less intrusive than publishing street-level locations, but the majority is prohibited from turning off the feature. As a result, IP location fundamentally alters the effectiveness of conventional practices for controlling information flow, such as limiting post access. Users have become increasingly concerned about regional discrimination, the exposure of travel trajectories for out-of-province travellers, and unwelcome harassment, with female users being particularly affected (Zhang and McKenzie 2024). The public access to personal regional information has forced users to cope with the new norm.

Geoprivacy concerns and the unethical use of personal location information have been extensively debated by geographers, particularly with the rise of location-based services (Dobson and Fisher 2003; Keßler and McKenzie 2018; Zhang and McKenzie 2023; Fisher and Dobson 2003). Several trends have emerged in this discourse, including the decreasing cost of surveillance, the increasing perceived benefits of being monitored, and the diminishing public resistance, often framed through the lens of Jeremy Bentham’s panopticon (Dobson and Fisher 2007). In the case of China, privacy concerns have been particularly prominent in discussions surrounding the Social Credit System (SCS). Western media frequently portrays the system as a tool for social and political control (Creemers 2018; Liang and others 2018) with substantial impacts on data privacy (Chen and Cheung 2017). However, on closer examination, researchers found that the SCS primarily focuses on “financial and commercial activities rather than political ones” (Liang and others 2018). The system also enjoys high approval ratings, especially among socially advantaged groups (that is, wealthier, better-educated, and urban residents), who view the system as a means to promote honesty and generate benefits (Kostka 2019). Further research into public opinions regarding the IP location feature would expand our understanding of geoprivacy concerns in China.

To the best of the authors’ knowledge, this is the first study to explore the regional differences in geoprivacy concerns within China. There is a scarcity of studies that have specifically addressed geoprivacy concerns of Chinese individuals, even on a national scale (Li 2020). Jianwei Huang and others (2021) compared people’s level of privacy concerns regarding location tracking for COVID-19 containment in the United States, Hong Kong, and South Korea. However, the study did not survey citizens in mainland China. Jialiu Lin and others (2013) identified some location-sharing patterns of Chinese students, but the participants were all from one university in Beijing. Considering the recent progressions in IP location policy and drawing upon the knowledge-attitude-behavior model, this article aims to fill the research gap by conducting a survey involving participants from diverse occupations and regions throughout mainland China. The primary objective is to address the following research questions:

Q1. What factors moderate Chinese individuals' privacy knowledge and attitudes? Here, we explore the impact of demographic variables such as gender, age, and region on privacy literacy and expectations.

Q2. Does privacy knowledge and attitudes influence privacy-related behaviors in contemporary China? This inquiry investigates the potential interplay between knowledge and attitudes, knowledge and behaviors, and attitudes and behaviors.

Q3. Does the introduction of the IP location feature change Chinese individuals' privacy behaviors? Are there substantial privacy concerns that could prompt users to stop posting on affected social media platforms? Or is there a privacy paradox where individuals continue using the applications despite acknowledging the privacy risks?

The findings of this study will enhance our understanding of the dynamics of geoprivacy in the Chinese context. They can also help geosocial media platforms develop dynamic privacy protection mechanisms (Özdal Oktay and others 2024) to suit diverse user needs across various use case scenarios.

THE KNOWLEDGE-ATTITUDE-BEHAVIOR MODEL

THEORETICAL BACKGROUND

The knowledge-attitude-behavior (KAB) model, which uses the accumulation of knowledge to explain shifts in attitudes and subsequently behaviors, has been investigated in the context of modelling perceived privacy in location-based services (LBS) (Poikela 2020; Seidl and others 2020). Although there is a wealth of research on privacy concerns, existing theories on information disclosure offer diverse explanations for users' cognitive processes and online behaviors, lacking a consensus (Barth and De Jong 2017). This section aims to review the pertinent theories and applications in the field.

The privacy calculus theory (Culnan and Armstrong 1999) offers one explanation for the knowledge and behavior relationship, stating that users engage in a rational risk-benefit assessment when deciding whether to disclose personal information. Users intend to disclose personal data when perceived benefits are greater than risks. Privacy knowledge (or literacy) is required in this mental process to assess the value of social rewards and make logical decisions about information disclosure. Generally, privacy knowledge can be divided into declarative knowledge and procedural knowledge (Debatin and others 2009; Park 2013). The former refers to the knowledge of facts and information, such as privacy rights and associated risks, whereas the latter is about the skills and methods required to protect privacy effectively. Both types of privacy literacy enhance an individual's ability to participate in active privacy management (Baruh and others 2017), which means that additional knowledge may lead to increased privacy concerns (Prince and others 2023) and more conservative information disclosure behaviors. Contrarily, other studies have reported an opposite effect, indicating that increased knowledge may result in reduced privacy concerns (Wirtz, Lwin, and Williams 2007) and more permissive behaviors. Users may value more about application functionality, design, and costs and care less about potential privacy risks, even with adequate technical knowledge and financial resources (Barth and others 2019). In other words, risk perception is not persuasive in applying privacy protection strategies (Oomen and Leenes 2008).

The ambivalent relationship is more evident between privacy attitude and behavior. Previous studies have found that while some users recognize privacy risks from using mobile LBS, they do not take appropriate actions to protect their location information. This disparity between one’s attitude towards privacy and their actual privacy-related actions is known as the privacy paradox (Cottrill and Thakuriah 2015; Li 2020). One widely cited explanation is the privacy calculus theory mentioned previously: people are willing to trade their private information for personal or social benefits through a rational risk-benefit calculation (Barth and others 2019; Cottrill and Thakuriah 2015; Huang and others 2021). Other theories include affection-based explanations of the privacy paradox. Users could rely on their instincts without evaluating the potential risks of sharing information online (Barth and De Jong 2017). Situational factors can bias these affect-based heuristics (such as subconscious valuation) and lead to decisions in contradictory to people’s generic privacy attitudes (Culnan and Armstrong 1999). Online environment is a situational factor that promotes information sharing. The fuzzy boundaries make privacy violations less tangible and sensible in cyberspace compared to the real world (Acquisti and others 2015). Consequently, individuals disregard cybersecurity and privacy incidents, and persist in sharing their personal information in exchange for perceived advantages. Although the privacy paradox exists, a meta-analysis (Baruh and others 2017) reviewed 166 studies from 34 countries and concluded that privacy concerns usually lead to less frequent information disclosure and more frequent privacy protection. Moderating factors such as gender, culture, and regulations do not alter the generalized conclusion. In this sense, the positive correlation between privacy attitude and behavior is observed more frequently. Therefore, we propose:

H1. Privacy knowledge is positively associated with privacy concerns.

H2. Privacy knowledge is positively associated with privacy protection behaviors.

H3. Privacy concerns are positively associated with privacy protection behaviors.

MODERATING FACTORS

The conflicting interpretations between knowledge, attitude, and behavior, as described in the prior sections, indicate the need for moderators in mediating the relations of the three (Ajzen and Fishbein 2005; Baruh and others 2017). Gender, age, and culture are three factors that can cause substantial variations. In terms of gender, females were found to have higher privacy concerns (Huang and others 2021; Ketelaar and Van Balen 2018), were less knowledgeable about technical countermeasures of privacy threats (Park 2015), but more likely to act as privacy-conscious decision makers (Hoy and Milne 2010). Inconsistent findings were observed for privacy concerns between different age groups (Hoofnagle and others 2010; Miltgen and Peyrat-Guillard 2014). In certain instances, young people had higher privacy concerns (Huang and others 2021) and adjusted their information-sharing behaviors more frequently (Ketelaar and Van Balen 2018). In alternative scenarios, young people were more confident in their ability of personal data protection and showed less concern on privacy-related issues (Miltgen and Peyrat-Guillard 2014). Culture (for example, collectivism vs. individualism) also influences people’s geoprivacy attitude and behavior as seen in the studies among

European countries (Miltgen and Peyrat-Guillard 2014), between the United States and China (Lin and others 2013), and between the United States and East Asia (Huang and others 2021). While a probe into privacy concerns within a single country and their geographical variances was not identified, it is worth noting that geographic regions influence people's privacy attitudes to some extent based on national comparisons. The reason behind the absence of literature from this perspective can be explained by Tobler's first law of geography: nearby things are more correlated than distant objects (Tobler 1970), so do individual minds, beliefs, and social norms within a national boundary. A notable variation in privacy concerns is less likely to be observed in a region with a similar cultural background. Therefore, we propose:

H4. Females possess lower levels of privacy knowledge, but exhibit higher levels of privacy concerns and privacy protection behaviors.

H5. Young individuals possess higher levels of privacy knowledge, but exhibit lower levels of privacy concerns and privacy protection behaviors.

H6. Privacy knowledge, attitude, and behavior do not exhibit a significant difference among users from a single culture, even when considering their provincial origins.

A research model is developed based on the literature review and the six hypotheses (Figure 1).

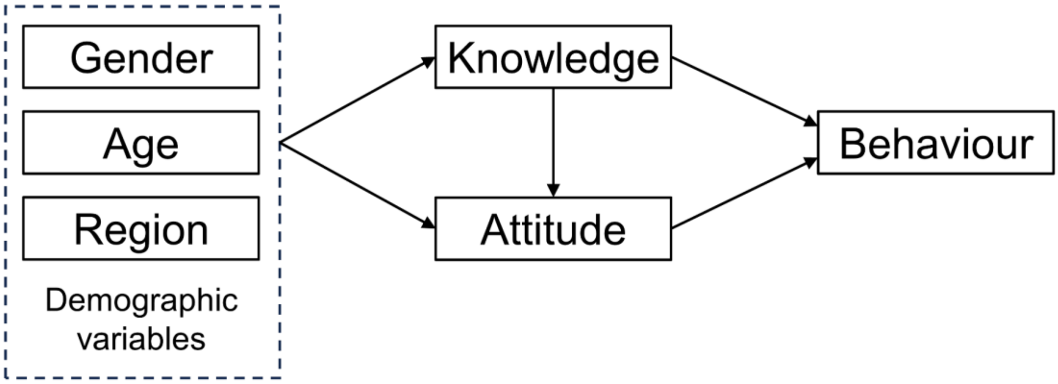

Figure 1. Research Model. On the left side, we hypothesize that demographic variables, including gender, age, and region of origin, influence users' privacy knowledge and attitude. On the right side, we posit that privacy behavior is associated with these privacy knowledge and attitude.

METHODOLOGY

MEASUREMENT

We designed our online survey to comprise 22 questions (refer to Appendix A), drawing from existing scales of online privacy and relevant studies in geoprivacy. A consent form was presented at the commencement of the survey and required agreement before proceeding. The first section asked about respondents' Internet experience (Q2–4), which determined their level of engagement on the social media platforms of interest and their prior encounter with privacy breaches. This section was necessary because users' privacy concerns were dependent on the online platforms they interact with (Zafeiropoulou and others 2013). Next, we surveyed participants' geoprivacy knowledge based on the online privacy literacy scale (Trepte and others 2015) and the online privacy questions (Hoofnagle and others 2010), with the former targeting Europeans and the latter fitting Americans. Both procedural (Q5 and 7) and declarative (Q6) knowledge were covered, such as knowledge of Personal Information Protection

Law (PIPL). Specific questions about IP location were asked, with the remainder tailored to the Chinese context. Following privacy knowledge, a significant portion of the survey questions (Q8–9, 11–13) focused on geoprivacy attitudes. Questions (Q8 and 11) in this section employed a five-point Likert scale, which were inspired by the Internet users' information privacy concerns (IUIPC) (Malhotra and others 2004) and the privacy-concerns-related questions (Hoofnagle and others 2010; Zafeiropoulou and others 2013). Map scale was explored (Q12) as it impacted people's perceived location disclosure risk (Kim and others 2021). Then, geoprivacy behaviors were inquired (Q14–15) by adapting questions from previous studies (Hoofnagle and others 2010; Seidl and others 2020). Again, the Likert scale was used to assess participants' personal beliefs. Privacy protection practices such as misrepresentation (Jiang and others 2013) were considered. Regarding geoprivacy, people could choose to enter inaccurate locations when prompted (Q14.4). The last section (Q16–22) covered demographic variables such as respondents' gender, age, and geographic origins. Attention check questions (say, Q1 and 10) were included throughout the survey, and two Likert scale questions (Q8.3 and 8.4) were repeated in Q11 using slightly different phrases to ascertain respondents' attentiveness to the questions and the consistency of their responses.

DATA COLLECTION AND CLEANING

We chose to host the survey on Credamo,[1] a professional research and survey platform that has more than 3 million users. The platform was selected because Credamo had the highest valid response rate during pilot distributions. Only registered users who were over 18 years old were invited to participate in the study. China was selected as the study area because of its large population base and cohesive cultural composition. The majority of individuals from China (73 percent) have access to the Internet (World Bank

2021). Among those Internet users, over 97 percent interact with at least one social media platform (Kemp 2023). The survey was randomly distributed by Credamo in 31 provincial-level administrative regions of China (excluding Hong Kong, Macao, and Taiwan) from December 2022 to January 2023. Each participant was offered a cash incentive of three Chinese yuan (about US$ 0.44). Fifty responses were collected per iteration, resulting in a total of 1,000 responses obtained. After multiple iterations, we noticed that more females completed the survey, so males were targeted to improve the sample's representativeness. We did not oversample other variables due to budgetary constraints. To avoid data scarcity, respondents' self-reported province of origin were grouped into seven regions based on Figure 2.

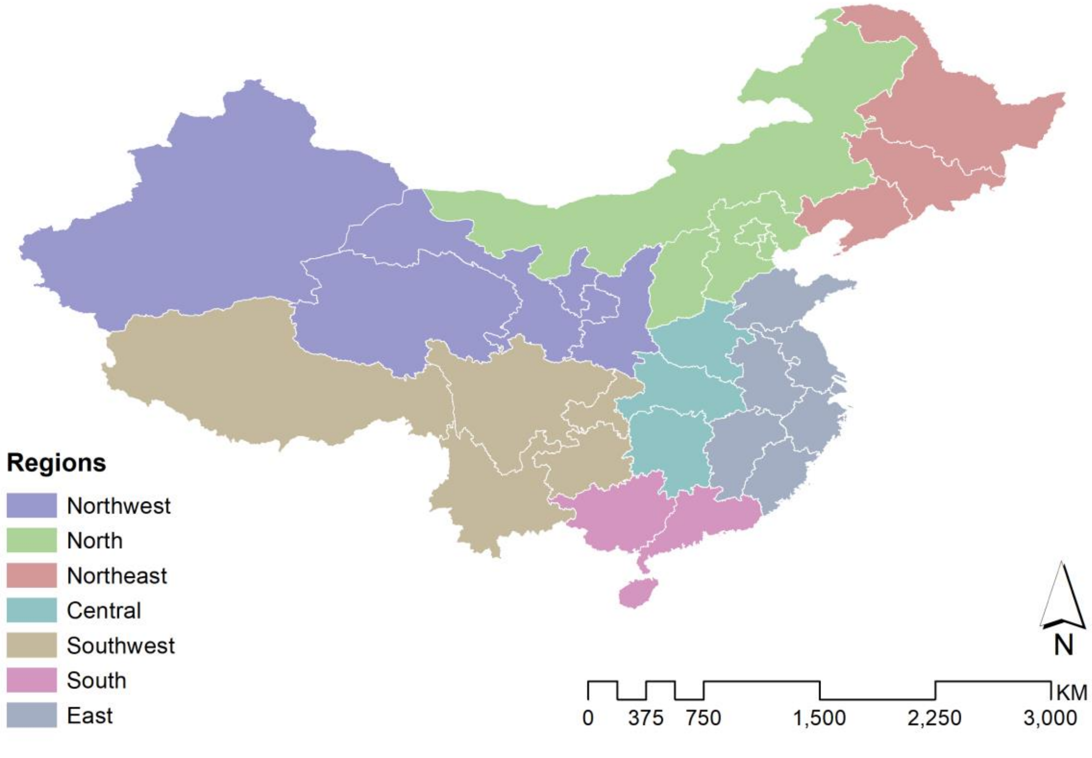

Figure 2. Regions of Mainland China Explored in the Study[2]

Data cleaning was conducted to ensure the validity of the analysis. Responses that fell outside the acceptable range, either exceeding the 95th percentile in duration of completion or falling below the 5th percentile, were excluded from the analysis. Attention check questions (see Q1 and 10) were also used to filter valid responses, and only responses that answered the questions correctly were kept. The answers of Q8.3 and 8.4 were compared with the repeated counterparts (the answers of Q11.4 and 11.3), and only responses that were less than or equal to one Likert point away were accepted. If "Not sure" was selected in Q8.3 or 8.4, the counterpart had to be the same to remain in the analysis. Finally, to ensure the moderating factors could be properly assessed, participants who reported "Prefer not to answer" in their demographic statistics were removed as the final step. This process yielded a total of 491 responses available for subsequent data analysis.

DATA ANALYSIS

Ordinal regression has been frequently used in analyses of privacy preferences (Cho and others 2019; Poikela 2020; Seidl and others 2020). In this analysis, we employed ordinal logistic regression using backward elimination based on the ordered categorical variables extracted from the survey (see Table I). Different Likert scales were transformed into a common five-point scale. Measures in reverse order were recoded so that higher scores consistently indicate greater levels of privacy knowledge, increased privacy concerns, and enhanced privacy protection behaviors. Males and females were coded as 1 and 0 respectively. Spearman's correlation matrix (Spearman 1904) was implemented to spot significant predictors of the response variables. An ordinal regression model was built for each knowledge, attitude, and behavior variable in Table I. Only statistically significant explanatory variables ($p<0.05$) were included in the models, except for the categorical variable of respondents' geographic origin. Results of the most relevant regression models, categorized by knowledge (models 1 to 2), attitude (models 3 to 13), and behavior (models 14 to 20), are presented in Table III and Table IV. Additional models can be found in Appendix B.

Table I. Variable Definitions

RESULTS

SAMPLE CHARACTERISTICS

Table II showcases the demographic distribution of the 491 participants who remained in the study. The majority of the participants were between the age of 20 to 39, with the median in the range of 30 to 34. The respondents were highly educated: more than 90 percent of the respondents hold a bachelor's degree or above. However, income inequality is observed despite a skewed distribution of education backgrounds. One explanation of the widespread distribution of monthly income could be the various economic development levels across the country. Most participants originated from east China (40.7 percent), followed by north China (17.5 percent) and south China (15.7 percent). The region with the lowest representation was northwest China (3.3 percent), which reflects the unequal population distribution on the vast land.

Table II. Demographic Statistics

GENERAL GEOPRIVACY CONCERNS

We first illustrate the general trends in participants' Internet experience and their knowledge, attitudes, and behaviors related to geoprivacy. According to the violin plots (Figure 3), Douyin (E2) emerged as the most widely used social media platform, surpassing the popular microblogging site Weibo (E1) and instant messaging app WeChat (E3). Only a small proportion of respondents reported no prior experience of privacy breaches in the past five years (E4), with the majority encountering such breaches once or twice. In Figure 4, while participants demonstrated a general awareness of the potential methods of location data collection on social media (K1), their knowledge regarding countermeasures for location surveillance (K3) was comparatively limited. In fact, their declarative knowledge (K2), especially regarding the recently implemented PIPL, was notably low, with a majority of respondents expressing uncertainty about its specifics. Regarding geoprivacy attitude (Figure 5), the majority of participants agreed that they were not always willing to share their locations on social media (A1), and their concerns regarding pervasive location data collection remained high (A2). In fact, the respondents' geoprivacy concerns were more pronounced compared to five years ago (A3). Interestingly, while some respondents felt that others were overly concerned about privacy, a larger number of individuals indicated otherwise (A4). When comparing privacy concerns related to publicly displayed personal locations (A5) and locations collected in the background (A6), more concerns were observed in the latter case.

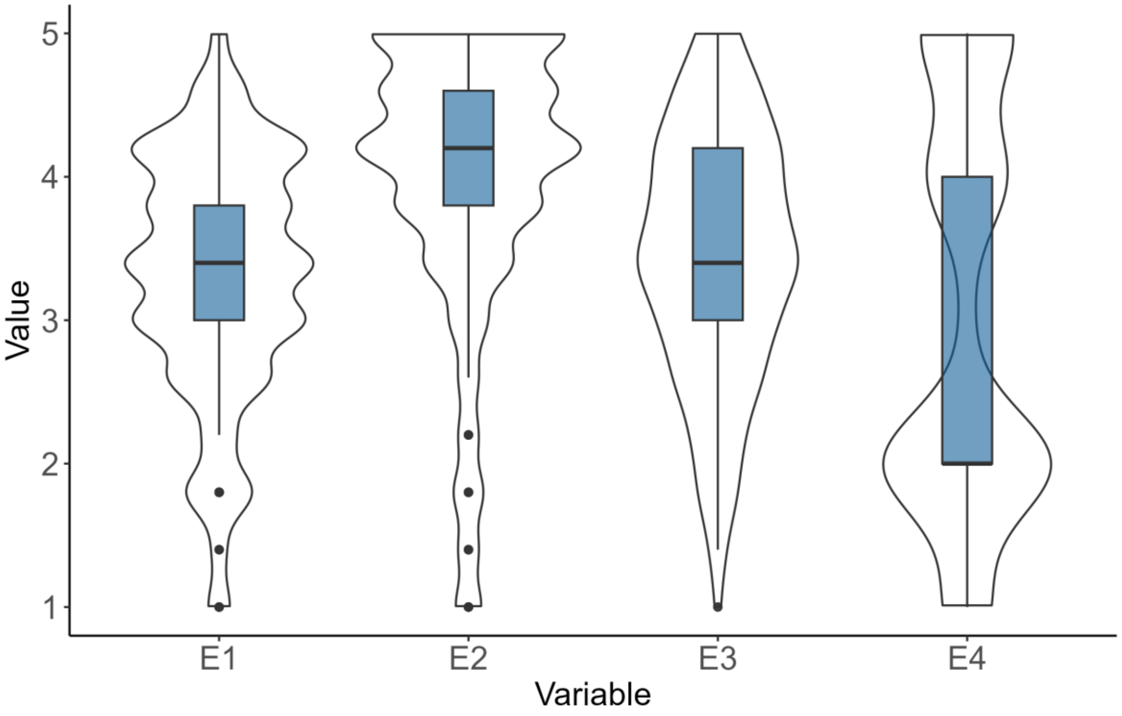

Figure 3. Violin Plots of Experience: Weibo (E1), Douyin (E2), and WeChat (E3) usage frequency, as well as prior experience of privacy breach (E4).

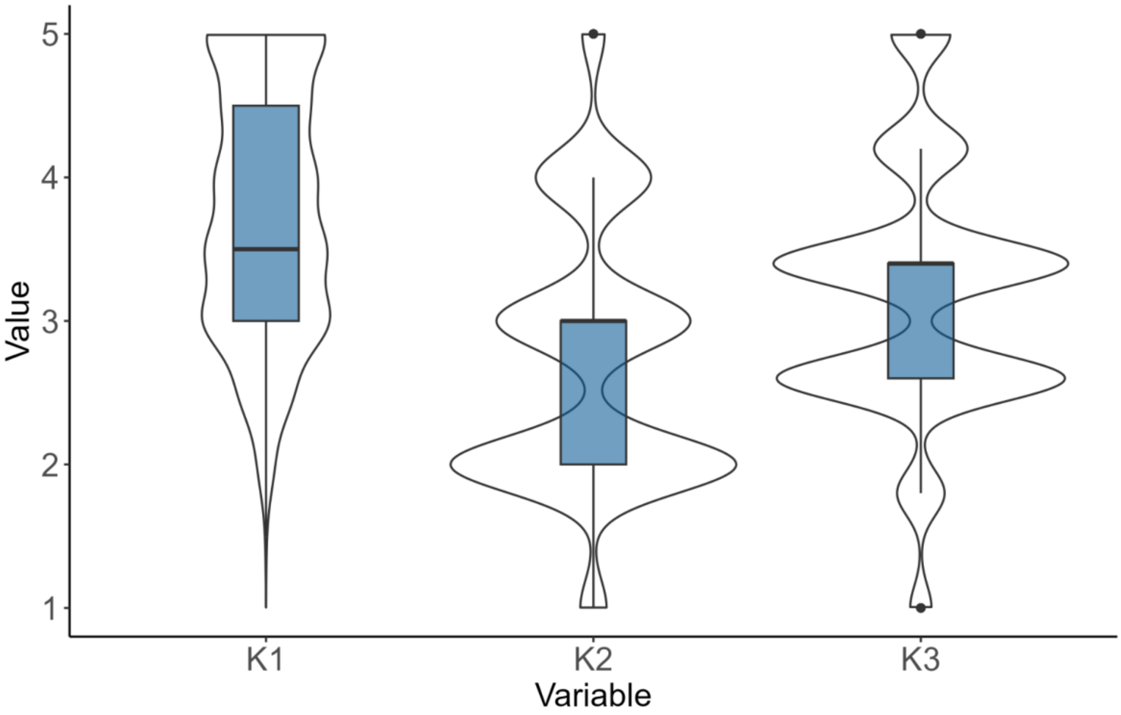

Figure 4. Violin Plots of Knowledge: Location data collection practices (K1), privacy law (K2), and geoprivacy protection techniques (K3).

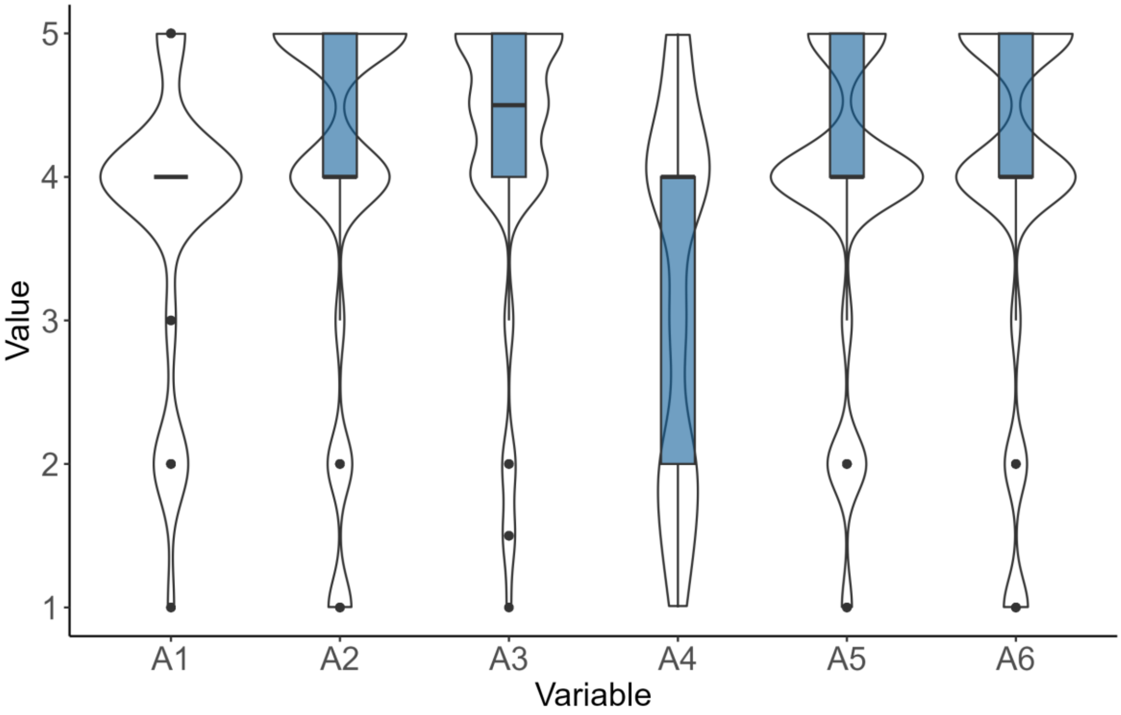

Figure 5. Violin Plots of General Attitudes: The concerns of location disclosure (A1) and location data collection (A2), temporal change of geoprivacy concerns (A3), views of others' geoprivacy concerns (A4), and attitudes towards the misuse of displayed (A5) and collected (A6) location information.

In terms of geoprivacy behavior (Figure 6), the privacy paradox was evident: despite the high level of privacy concerns expressed, people demonstrated a willingness to share their locations and did not adopt more restrictive behaviors. Most individuals kept their location services enabled (B1) and consented to location access when prompted (B3). Although respondents displayed some selectivity in sharing their locations on social media (B2), the majority did not intentionally provide inaccurate location information (B4).

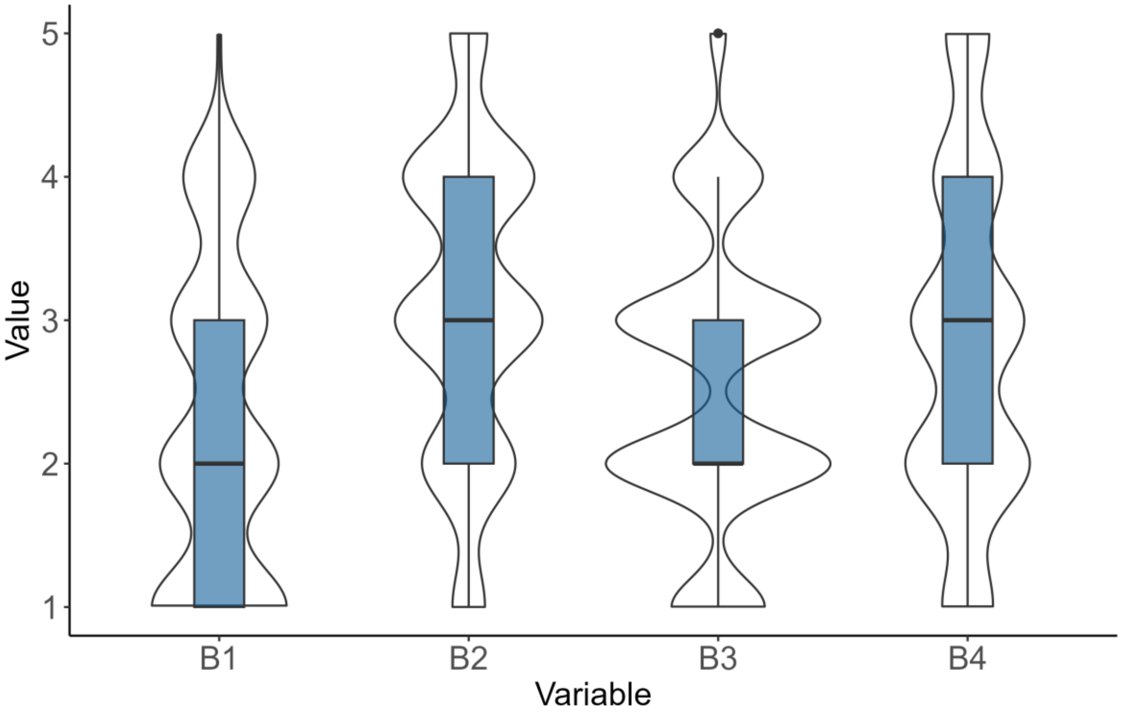

Figure 6. Violin Plots of General Behaviors: Turning off mobile location services (B1), not sharing locations on social media (B2), not allowing location access when prompted (B3), and entering inaccurate location data (B4).

Correlations Between Knowledge, Attitude, and Behavior

The correlation matrix is calculated to understand the relationship between knowledge, attitude, and behavior. Only significant correlation coefficients ($p \leq 0.05$) are presented in Figure 7. Regarding Internet experience, higher engagement on one social media platform was associated with increased participation on others (0.32 to 0.41). However, social media usage negatively correlated with prior experiences of privacy breaches (-0.09 to -0.13). Generally, greater social media usage and previous negative experiences were linked to a higher level of privacy knowledge (0.10 to 0.32). One exception was that respondents with more privacy violation experiences exhibited lower levels of declarative privacy knowledge (-0.13). In terms of attitude, individuals who used social media more frequently expressed lower privacy concerns (-0.10 to -0.24), while those who had experienced privacy breaches held opposite views (0.18 to 0.31). A similar relationship could be noted between Internet experience and privacy behavior (-0.09 to -0.25 for E1 to E3 vs. B1 to B4, and 0.14 to 0.29 for E4 vs. B1 to B4).

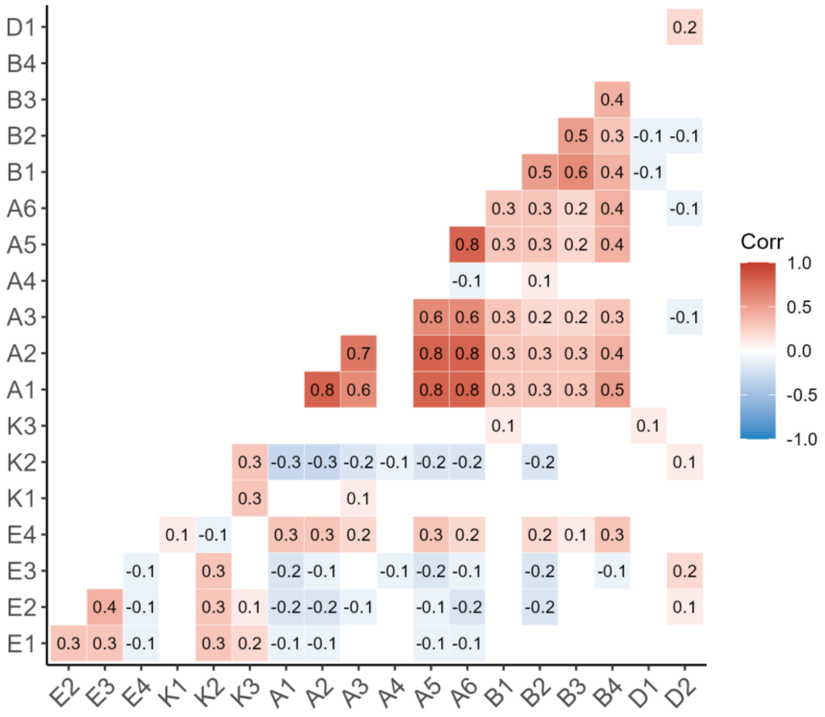

Figure 7. Correlation Matrix. Displayed values are statistically significant correlation coefficients (significance level = 0.05).

Overall, knowledge, attitude, and behavior variables positively correlated with themselves. While not all correlations were statistically significant, increased procedural knowledge (K1 and K3) tended to be associated with higher privacy concerns (0.09 to 0.14), while greater declarative knowledge (K2) was linked to reduced concerns (-0.12 to -0.26). The relationship between knowledge (K1 to K3) and behavior (B1 to B4) was not clear, with both positive and negative correlations present, and few significant results were found. Regarding attitude (A1 to A6) and behavior (B1 to B4), privacy concerns were generally positively associated with privacy behaviors (0.15 to 0.47).

In terms of demographic variables, males demonstrated higher privacy knowledge (0.13) and lower privacy protection behaviors (-0.09 to -0.11), while older respondents displayed more declarative knowledge (0.21) and fewer privacy concerns (-0.06 to -0.07). The relationships between gender and attitude, as well as age and behavior, were not established.

ORDINAL REGRESSION RESULTS

Ordinal regression results are presented in Table III and 4, where the former lists the model coefficients, and the latter provides the fit-measure statistics of the regression models. First, about knowledge and demographic variables (Model 1), it was observed that older respondents possessed higher levels of declarative privacy knowledge. In terms of countermeasures for location surveillance (Model 2), male respondents exhibited greater knowledge. The southwest had the highest level of procedural knowledge in location spoofing, followed by northwest, while northeast had the lowest level.

Next, we summarize the findings with privacy attitude as the response variable (Models 3 to 8). Regarding experience, an increase in Weibo usage was associated with a lower belief that other people were overconcerned about geoprivacy. In contrast, an increase in WeChat usage showed the opposite effect (Model 6). Additional engagement in Douyin, similar to WeChat users, resulted in fewer concerns about location sharing on social media (Model 3). Consistently, prior privacy breach experiences increased respondents' level of geoprivacy concerns across the board (except for Model 6, where E4 was insignificant). For knowledge and attitude, declarative knowledge consistently decreased respondents' privacy concerns (Models 5, 7, and 8), while procedural knowledge had the opposite effect (Models 3 to 8). Regarding demographic variables, age and gender were not significant moderating factors of attitude. Compared to northeast China, other regions exhibited a higher level of privacy concerns (Models 3, 6, and 7). Northwest experienced the greatest increase in concerns about location sharing on social media (Model 3) and the potential misuse of public location data (Model 7). On the other hand, east China had the lowest degree of agreement on the statement regarding overconcerned media and netizens about privacy (Model 6).

We then built our models with privacy behavior as the dependent variable (Models 14 to 17). In terms of experience, frequent users of each platform displayed their own characteristics. Frequent Weibo users were less likely to allow location access when prompted (Model 16), frequent Douyin users shared their location on social media more frequently (Model 15), and frequent WeChat users enabled location services on their phones less frequently (Model 14). Prior experiences of privacy incidents led to an increase in inaccurate address submissions online (Model 17) and a decrease in location disclosure on social media (Model 15). Regarding knowledge and behavior, we observed that greater knowledge about location spoofing resulted in less frequent enabling of location services (Model 14). In the relationship between attitude and behavior, a higher degree of privacy concerns corresponded to a higher degree of privacy protection behaviors. This relationship was consistent across all four behavioral variables (Model 14 to 17). Regarding demographic variables, males more frequently enabled location services on their phones and shared locations on social media (Model 14 and 15). Compared to northeast China, southwest exhibited the largest increase in privacy protection behaviors (Model 14 and 16), making it the most conservative region when it comes to enabling location services and granting location access on phones. Participants from northwest China exhibited a surprising openness to location disclosure, which contradicted their high level of privacy concerns (Model 14 to 16). However, the decrease in privacy protection behaviors in the northwest region was not statistically significant (p ranges from 0.28 to 0.99).

Table III. Regression Results

Table IV. Regression Model Summary

SPECIFIC CONCERNS REGARDING IP LOCATION

This section reports IP-location-related privacy attitudes and behaviors of the survey participants. Starting at attitudes (Figure 8), the distributions to answers of A7, A8, and A9 were similar. The majority of respondents agreed that limiting the scope of the IP location feature will reduce their privacy concerns (A7), and users’ privacy is violated when the feature cannot be turned off (A9). Still, the preponderance also agreed that the IP location feature is less intrusive than GPS location (A8), and the accuracy of their IP locations can be trusted (A11). The satisfaction of location accuracy was followed by a strong desire to know the location determination process (A10), signalling the importance of transparency. In terms of the most appropriate geographic scale (A12), nearly 40 percent of respondents preferred IP location to be displayed at the provincial level (if necessary), followed by country and regional levels. Less than 15 percent of respondents believed that a finer scale would balance between privacy protection and antidisinformation, and none selected street level in the responses. In Model 13 (Table III), we discovered that Douyin users (-0.17) and male respondents (-0.43) preferred a finer scale. In comparison, WeChat users (0.20) and respondents with more location data collection knowledge (0.32) voted for a coarser scale. Compared to northeast China, respondents from all other regions preferred a coarser scale, with participants from east China expressing the strongest preference for the coarsest scale (0.84).

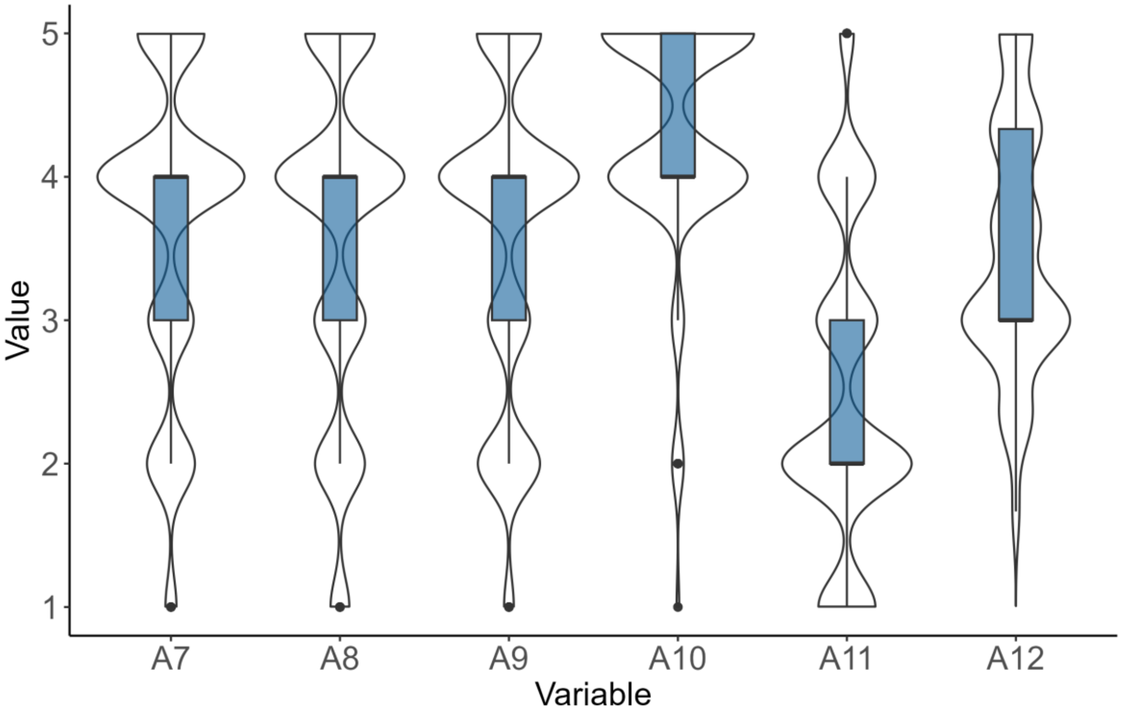

Figure 8. Violin Plots of Attitudes Specific to IP Location: Scope of the IP location feature (A7), IP location vs. GPS location (A8), the missing function of hiding IP location (A9), cares towards the IP locating process (A10), lack of confidence in IP location accuracy (A11), and geographic scale of IP location (A12).

Regarding behaviors (Figure 9), most respondents did not use IP location to follow the latest activities of celebrities (B5). Although many participants seemed to care about their IP location accuracy, only a portion of participants tested their assumption that their IP locations were accurately displayed (B6). In terms of the behavioral change after the introduction of the IP location feature (B7), the answers were divided: nearly 60 percent of respondents agreed or strongly agreed that they stopped using specific social media platforms since April 2022, while the rest disagreed, including a small percent of unsure participants. In Model 20 (Table III), we found that the level of Weibo usage (0.27) and participants' privacy concerns had a positive correlation (0.45 to 0.54 for A1, A3, and A5) with their choice of quitting social media.

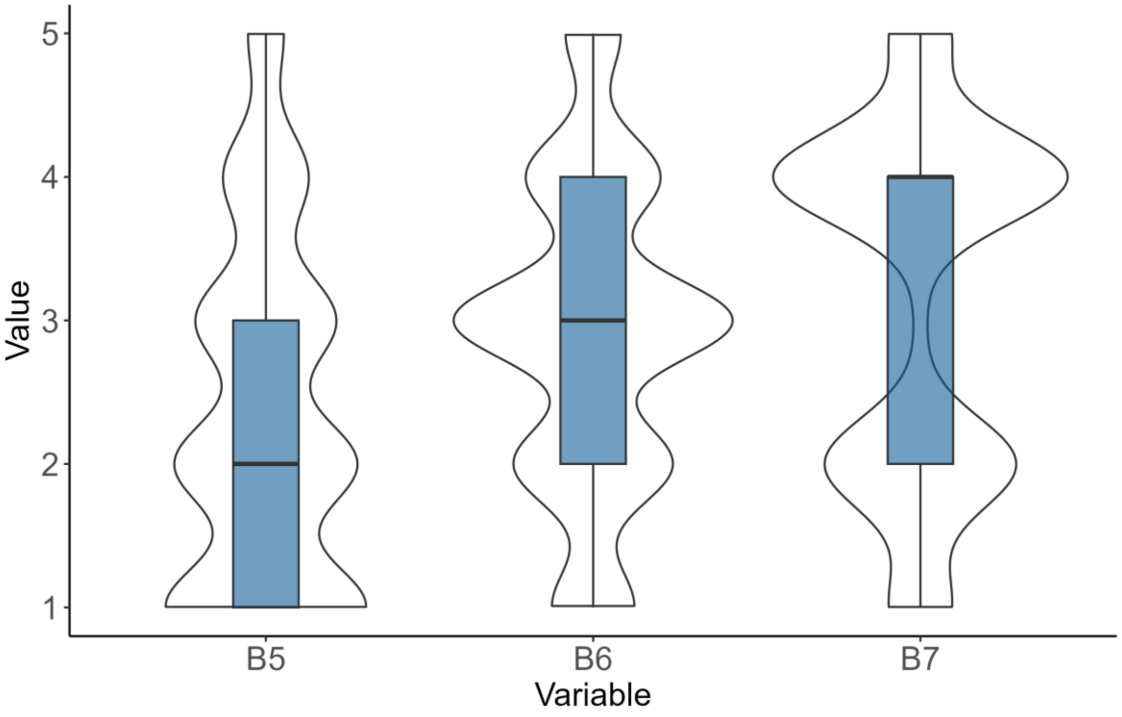

Figure 9. Violin Plots of Behaviors Specific to IP Location: Using IP location to follow celebrities (B5), testing IP location accuracy (B6), and quitting social media after April 2022 (B7).

DISCUSSION

The majority of survey respondents report a higher level of privacy concerns compared to five years ago, which appears to correlate with the widespread experience of privacy breaches and heightened awareness of privacy risks. Therefore, there is no better time to discuss geoprivacy concerns in China. Two themes arise from the survey results, namely transparency and control. Participants worried about the misuse of personal location information passively collected by social media platforms and were interested in learning how their IP locations were determined. These results indicate that respondents desire a more transparent process of location data collection and transfer. Additionally, to reduce participants' level of privacy concerns, the authority could limit the scope of when and where IP location is applied or allow social media platforms to offer an option to toggle the feature. These responses suggest that individuals prefer to have more control over how and when their IP locations are shared.

The correlation and regression outputs determine whether the hypotheses are true. Generally, geoprivacy knowledge positively influences geoprivacy attitude (H1) and behavior (H2), with one exception---that declarative knowledge was negatively associated with geoprivacy concerns. This exception may be explained by the increased trust from learning more about PIPL, which in turn lessens the respondents' sensitive nerves about geoprivacy. Thus, H1 (knowledge vs. attitude) holds if its subject is specified as "procedural privacy knowledge" (that is, technical steps of privacy protection). For H2 (knowledge vs. behavior), only one supporting evidence between K3 and B1 was observed (Model 14), so H2 holds, but more evidence is needed to make a stronger argument. A robust positive relationship was observed between privacy attitude and behavior, with consistent results across all variables. Therefore, H3 (attitude vs. behavior) is also supported. The effect of the moderating factors are summarized below. H4 (gender vs. knowledge/attitude/behavior, or KAB) partially holds as we only found statistically significant evidence to support that males possess higher levels of privacy knowledge and exhibit lower levels of privacy protection behaviors. Both age and gender did not significantly moderate privacy attitudes, suggesting the presence of potential alternative moderators. Although H5 (age vs. KAB) does not hold due to the lack of statistically significant coefficients, we discovered that senior respondents were more knowledgeable about PIPL. H6 (region of origin vs. KAB) was found to be false, although it is usually assumed that individuals from one country share similar concerns and behaviors due to coherent social norms and cultural identity. Specifically, northeast China consistently exhibited the lowest level of privacy knowledge and concerns as well as a relatively low level of privacy protection behaviors. This phenomenon is likely related to the geopolitical context of northeast China, where the three provinces were among the pioneering industrialized regions (Zhang 2008).

Although the era of collectively planned heavy manufacturing has come to an end, people in northeastern China, especially the older generation, still miss the old days and prefer stable careers supported by the government, partly because there are few better jobs than civil servants in the postindustrial era (Attrill 2020). This reliance on the central regime may explain their attitude and behavior towards geoprivacy. On the contrary, respondents from east China expressed the least agreement with the statement regarding the overconcern of others. They preferred the coarsest geographic scale of IP location, suggesting that this group of respondents believed that people’s privacy concerns need to be recognized, shared, and discussed. This liberal mindset of east China is probably linked to its high level of economic development and openness to Western ideologies. Interestingly, responses from southwest China had the highest level of location protection knowledge and behavior, and responses from northwest China shared the highest level of geoprivacy concerns. This phenomenon is likely associated with the agglomeration of visible minorities and the politically charged atmosphere in west China. Privacy paradox was also observed in our analysis. Collectively, although respondents had relatively strong geoprivacy concerns, they did not exhibit a high level of privacy protection behaviors and still shared their locations frequently. A specific case was northwest China, where the participants had a relatively high acceptance level of location disclosure compared to their comparatively elevated level of privacy concerns.

People's privacy concerns were also platform-dependent. Douyin users, for example, demonstrated fewer privacy concerns and shared locations more frequently, while Weibo users were more cautious. WeChat users also valued personal location protection and acted accordingly. The difference between Douyin and WeChat arises from their use cases: Douyin is a short video platform, while WeChat is mainly for messaging with close contacts (Elegant 2019). Weibo is distinct because its debut of the IP location feature sparked intense debate and made geoprivacy a trending topic. A substantial number of respondents chose to discontinue using specific social media platforms, citing privacy concerns and specifically mentioning Weibo.

LIMITATIONS

This study is not without limitations. First, backward elimination has been criticized because the stepwise approach may exclude real explanatory variables that are not statistically significant (Smith 2018). However, this issue is mitigated in our analysis as each category has more than one response variable, so the chance of missing true explanatory variables is reduced. It would also be unpersuasive to reject the null hypotheses if insignificant independent covariates were included in our models. Second, respondents' regions of origin were not equally distributed, with the majority from east China, so the generalizability of our findings was limited to some extent. Yet, in observational data, achieving an equal geographic distribution is often unfeasible. In cases of rare events where significant concerns may arise, the threshold for defining rare events was set at 1 percent or less of the sample size (King and Zeng 2001). In our analysis, the category with the smallest number of respondents (northwest) accounted for more than 3 percent of the total sample, suggesting that the issue may be mild. Finally, sampling bias is unavoidable when using any data collection platform. Since our survey was distributed on Credamo, users who did not sign up for Credamo were out of reach.

CONCLUSIONS

The norm of privacy has not been adequately addressed in Chinese society historically, but the development of PIPL served as a wake-up call of better privacy protection. The implementation of the IP location feature countered the latest regulation, which led to heated debate on social media, making this study a timely topic in the field of society and space. Through analyzing the responses of an online survey, this article fills the research gap of geoprivacy concerns in China. Using ordinal logistic regression, we discovered that privacy knowledge and attitudes positively influenced privacy protection behaviors. Privacy knowledge and attitudes shared the same positive relation except declarative knowledge, which had an opposite effect on privacy concerns. In terms of the moderating factors, male respondents exhibited extra procedural knowledge and less protection behaviors, while senior respondents were more knowledgeable about their privacy rights. The regional difference in geoprivacy concerns was also notable, with participants from the northeast at the bottom, while those from the northwest, southwest, and east ranked among the top. Although privacy paradox was observed, more than half of the respondents reported decreased social media usage since the introduction of the IP location feature, suggesting the potential influence of behavioral changes resulting from unintended location disclosure. From our analysis, Chinese citizens care about their geoprivacy and act following their privacy attitudes. The policy makers should therefore consider the impact of Internet policy on individual behaviors.

NOTES

[1] https://www.credamo.world/

[2] This map of the study area does not depict geopolitical boundaries that are controversial or under dispute.

References

Acquisti, A., L. Brandimarte, and G. Loewenstein. 2015. Privacy and Human Behavior in the Age of Information. *Science* 347 (6221): 509–514.

Ajzen, I., and M. Fishbein. 2005. The Influence of Attitudes on Behavior. In *The Handbook of Attitudes*, edited by D. Albarracín, B. Johnson, and M. Zanna, 173–221. Mahwah: Lawrence Erlbaum Associates Publishers.

Attrill, N. 2020. Northeast China's Rust Belt Politics: A New Governing Challenge for the Party-State in a Post-Industrial Era? Available at SSRN 3667616.

Barth, S., and M. D. De Jong. 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.

Barth, S., M. D. De Jong, M. Junger, P. H. Hartel, and J. C. Roppelt. 2019. Putting the Privacy Paradox to the Test: Online Privacy and Security Behaviors Among Users with Technical Knowledge, Privacy Awareness, and Financial Resources. *Telematics and Informatics* 41: 55–69.

Baruh, L., E. Secinti, and Z. Cemalcilar. 2017. Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *Journal of Communication* 67 (1): 26–53.

Cann, K., and M. Price. 2023. The Ethics of Location Tracking During the COVID-19 Pandemic and Beyond: Building Awareness and Consensus. *The Professional Geographer* 75 (3): 430–440.

Chen, Y., and A. S. Cheung. 2017. The Transparent Self under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System. *Journal of Comparative Law* 12 (2): 356–378.

Cho, H., S. Roh, and B. Park. 2019. Of Promoting Networking and Protecting Privacy: Effects of Defaults and Regulatory Focus on Social Media Users' Preference Settings. *Computers in Human Behavior* 101: 1–13.

Cottrill, C. D., and P. V. Thakuriah. 2015. Location Privacy Preferences: A Survey-Based Analysis of Consumer Awareness, Trade-Off, and Decision-Making. *Transportation Research Part C: Emerging Technologies* 56: 132–148.

Creemers, R. 2018. China's Social Credit System: An Evolving Practice of Control. Available at SSRN 3175792.

Culnan, M. J., and P. K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science* 10 (1): 104–115.

Debatin, B., J. P. Lovejoy, A.-K. Horn, and B. N. Hughes. 2009. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication* 15 (1): 83–108.

Dobson, J., and P. Fisher. 2003. Geoslavery. *IEEE Technology and Society Magazine* 22 (1): 47–52.

———. 2007. The Panopticon's Changing Geography. *Geographical Review* 97 (3): 307–323.

Elegant, N. X. 2019. For China's Social Media Giants, It's a Battle for the Ages. Fortune. Accessed: 2023-08-29. [https://fortune.com/2019/10/25/wechat-douyin-tiktok-china/].

Fisher, P., and J. Dobson. 2003. Who Knows Where You Are, and Who Should, in the Era of Mobile Geography? *Geography* 88 (4): 331–337.

Hoofnagle, C. J., J. King, S. Li, and J. Turow. 2010. How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies? Available at SSRN 1589864.

Hoy, M. G., and G. Milne. 2010. Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *Journal of Interactive Advertising* 10 (2): 28–45.

Huang, J., M.-P. Kwan, and J. Kim. 2021. How Culture and Sociopolitical Tensions Might Influence People's Acceptance of COVID-19 Control Measures That Use Individual-Level Georeferenced Data. *ISPRS International Journal of Geo-Information* 10 (7): 490.

Jiang, Z., C. S. Heng, and B. C. Choi. 2013. Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research* 24 (3): 579–595.

Kemp, S. 2023. Digital 2023: China. Data Reportal. https://datareportal.com/reports/digital-2023-china.

Keßler, C., and G. McKenzie. 2018. A Geoprivacy Manifesto. *Transactions in GIS* 22 (1): 3–19.

Ketelaar, P. E., and M. Van Balen. 2018. The Smartphone as Your Follower: The Role of Smartphone Literacy in the Relation Between Privacy Concerns, Attitude, and Behaviour Towards Phone-Embedded Tracking. *Computers in Human Behavior* 78: 174–182.

Kim, J., M.-P. Kwan, M. C. Levenstein, and D. B. Richardson. 2021. How Do People Perceive the Disclosure Risk of Maps? Examining the Perceived Disclosure Risk of Maps and Its Implications for Geoprivacy Protection. *Cartography and Geographic Information Science* 48 (1): 2–20.

King, G., and L. Zeng. 2001. Logistic Regression in Rare Events Data. *Political Analysis* 9 (2): 137–163.

Kostka, G. 2019. China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval. *New Media & Society* 21 (7): 1565–1593.

Kwan, M.P., J. Huang, and Z. Kan. 2023. People's Political Views, Perceived Social Norms, and Individualism Shape Their Privacy Concerns for and Acceptance of Pandemic Control Measures That Use Individual-Level Georeferenced Data. *International Journal of Health Geographics* 22 (1): 35.

Li, H. 2020. Negotiating Privacy and Mobile Socializing: Chinese University Students' Concerns and Strategies for Using Geosocial Networking Applications. *Social Media + Society* 6 (1): 2056305120913887.

Liang, F., V. Das, N. Kostyuk, and M. M. Hussain. 2018. Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure. *Policy & Internet* 10 (4): 415–453.

Lin, J., M. Benisch, N. Sadeh, J. Niu, J. Hong, B. Lu, and S. Guo. 2013. A Comparative Study of Location-Sharing Privacy Preferences in the United States and China. *Personal and Ubiquitous Computing* 17 (4): 697–711.

Malhotra, N. K., S. S. Kim, and J. Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15 (4): 336–355.

Miltgen, C. L., and D. Peyrat-Guillard. 2014. Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven European Countries. *European Journal of Information Systems* 23 (2): 103–125.

Oomen, I., and R. Leenes. 2008. Privacy Risk Perceptions and Privacy Protection Strategies. In *Policies and Research in Identity Management,* edited by E. Leeuw, S. Fischer-Hübner, J. Tseng, and J. Borking, 121--138. New York: Springer.

Özdal Oktay, S., S. Heitmann, and C. Kray. 2024. Linking Location Privacy, Digital Sovereignty, and Location-Based Services: A Meta Review. *Journal of Location Based Services* 18 (1): 1–52.

Park, Y. J. 2013. Digital Literacy and Privacy Behavior Online. *Communication Research* 40 (2): 215–236.

Park, Y. J. 2015. Do Men and Women Differ in Privacy? Gendered Privacy and (In)Equality in the Internet. *Computers in Human Behavior* 50: 252–258.

Poikela, M. E. 2020. *Perceived Privacy in Location-Based Mobile System*. Springer.

Prince, C., N. Omrani, A. Maalaoui, M. Dabic, and S. Kraus. 2023. Are We Living in Surveillance Societies and Is Privacy an Illusion? An Empirical Study on Privacy Literacy and Privacy Concerns. *IEEE Transactions on Engineering Management* 70 (10): 3553–3570.

Seidl, D. E., P. Jankowski, K. C. Clarke, and A. Nara. 2020. Please Enter Your Home Location: Geoprivacy Attitudes and Personal Location Masking Strategies of Internet Users. *Annals of the American Association of Geographers* 110 (3): 586–605.

Smith, G. 2018. Step Away from Stepwise. *Journal of Big Data* 5 (1): 1–12.

Spearman, C. 1904. The Proof and Measurement of Association Between Two Things. *The American Journal of Psychology* 15 (1): 72–101.

Tobler, W. 1970. A Computer Movie Simulating Urban Growth in the Detroit Region. *Economic Geography* 46 (sup1): 234–240.

Trepte, S., D. Teutsch, P. K. Masur, C. Eicher, M. Fischer, A. Hennhöfer, and F. Lind. 2015. Do People Know About Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS). In *Reforming European Data Protection Law,* edited by S. Gutwirth, R. Leenes, and P. Hert, 333–365. New York: Springer.

Wirtz, J., M. O. Lwin, and J. D. Williams. 2007. Causes and Consequences of Consumer Online Privacy Concern. *International Journal of Service Industry Management* 18 (4): 326–348.

World Bank. 2021. Individuals Using the Internet (Percent of Population) - China. The World Bank Group. [https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=CN].

Zafeiropoulou, A. M., D. E. Millard, C. Webber, and K. O’Hara. 2013. Unpicking the Privacy Paradox: Can Structuration Theory Help to Explain Location-Based Privacy Decisions? In *Proceedings of the 5th Annual ACM Web Science Conference*, edited by H. Davis, H. Halpin, and A. Pentland, 463–472. Danvers: The Association for Computing Machinery.

Zhang, H., and G. McKenzie. 2023. Rehumanize Geoprivacy: From Disclosure Control to Human Perception. *GeoJournal* 88 (1): 189--208.

———. 2024. Geoprivacy Attitudes on Chinese Social Media: A Case Study of Weibo. Unpublished manuscript.

Zhang, P. 2008. Revitalizing Old Industrial Base of Northeast China: Process, Policy and Challenge. *Chinese Geographical Science* 18: 109–118.

Table I. Variable Definitions

Groups	Var.	Descriptions	References to Survey Questions
Experience	E1	Weibo usage frequency	Average of Q2_Weibo and Q3_Weibo
	E2	Douyin usage frequency	Average of Q2_Douyin and Q3_Douyin
	E3	WeChat usage frequency	Average of Q2_WeChat and Q3_WeChat
	E4	Prior experience of privacy breach	Q4
Knowledge	K1	Location data collection practices	Sum of correct options selected in Q5
	K2	Privacy law	Q6
	K3	Location privacy protection techniques	Sum of correct options selected in Q7
Attitude	A1	Concerns of location disclosure	Q8.1
	A2	Concerns of location data collection	Q8.2
	A3	Temporal change of location privacy concerns	Average of Q8.3 and Q11.4
	A4	Views of others' location privacy concerns	Recoded average of Q8.4 and Q11.3
	A5	Misuse of displayed location information	Q11.1
	A6	Misuse of collected location information	Q11.2
	A7	Scope of the IP location feature	Q11.5
	A8	IP location vs. GPS location	Q11.6
	A9	The missing function of hiding IP location	Q11.7
	A10	Cares towards the IP locating process	Q11.8
	A11	Lack of confidence in IP location accuracy	Recoded Q11.9
	A12	Geographic scale of IP location	Recoded Q12
Behaviour	B1	Turn off mobile location services	Recoded Q14.1
	B2	Not share locations on social media	Recoded Q14.2
	B3	Not allow location access when prompted	Recoded Q14.3
	B4	Enter inaccurate location data	Q14.4
	B5	Use IP location to follow celebrities	Q14.5
	B6	Test IP location accuracy	Q14.6
	B7	Quit social media after April 2022	Q15
Demographic	D1	Gender	Q16
	D2	Age	Q17
	D3	Regions of origin	Aggregated Q18 based on Figure 2

Table II. Demographic Statistics

Variables	Levels	Frequency	Percentage (%)
Gender	Male	240	48.9
	Female	251	51.1
Age	19	2	0.4
	20-24	86	17.5
	25-29	147	29.9
	30-34	145	29.5
	35-39	53	10.8
	40-44	14	2.9
	45-49	24	4.9
	≥50	20	4.1
Region of origin	Northwest	16	3.3
	North	86	17.5
	Northeast	31	6.3
	Central	49	10.0
	Southwest	32	6.5
	South	77	15.7
	East	200	40.7
Education	High school or below	5	1.0
	Associate	41	8.4
	Bachelor’s	358	72.9
	Master’s or above	87	17.7
Monthly income (¥)	≤1,500	30	6.1
	1,501-3,000	36	7.3
	3,001-5,000	63	12.8
	5,001-8,000	128	26.1
	8,001-10,000	89	18.1
	10,001-15,000	67	13.6
	15,001-20,000	40	8.1
	≥20,001	38	7.7

Table III. Regression Results

Model	Resp. Var.	Predictor	Estimate	SE	Z	p
1	K2	D2	0.161	0.056	2.890	0.004
2	K3	D1	0.465	0.168	2.760	0.006
	K3	D3: E – NE	0.456	0.348	1.310	0.190
	K3	D3: C – NE	0.581	0.420	1.380	0.167
	K3	D3: N – NE	0.649	0.380	1.710	0.088
	K3	D3: S – NE	0.783	0.385	2.030	0.042
	K3	D3: NW – NE	1.066	0.553	1.930	0.054
	K3	D3: SW – NE	1.153	0.479	2.410	0.016
3	A1	E2	-0.312	0.102	-3.060	0.002
	A1	E4	0.445	0.072	6.180	<.001
	A1	K2	-0.484	0.108	-4.480	<.001
	A1	D3: E – NE	1.083	0.404	2.680	0.007
	A1	D3: C – NE	1.526	0.488	3.120	0.002
	A1	D3: N – NE	1.379	0.439	3.140	0.002
	A1	D3: S – NE	0.912	0.442	2.060	0.039
	A1	D3: NW – NE	2.226	0.646	3.440	<.001
	A1	D3: SW – NE	0.984	0.529	1.860	0.063
4	A2	E4	0.315	0.063	4.980	<.001
	A2	K2	-0.551	0.103	-5.350	<.001
	A2	K3	0.348	0.107	3.260	0.001
5	A3	E4	0.286	0.061	4.720	<.001
	A3	K1	0.198	0.095	2.090	0.037
	A3	K2	-0.227	0.092	-2.470	0.014
6	A4	E1	0.266	0.103	2.588	0.010
	A4	E3	-0.268	0.100	-2.677	0.007
	A4	K2	-0.243	0.099	-2.452	0.014
	A4	D3: E – NE	1.097	0.329	3.337	<.001
	A4	D3: C – NE	0.216	0.391	0.553	0.580
	A4	D3: N – NE	0.197	0.351	0.562	0.574
	A4	D3: S – NE	0.778	0.363	2.143	0.032
	A4	D3: NW – NE	0.434	0.556	0.781	0.435
	A4	D3: SW – NE	0.322	0.432	0.746	0.456
7	A5	E4	0.395	0.065	6.040	<.001
	A5	K2	-0.365	0.105	-3.470	<.001
	A5	K3	0.192	0.107	1.790	0.073
	A5	D3: E – NE	0.762	0.371	2.050	0.040
	A5	D3: C – NE	0.932	0.442	2.110	0.035
	A5	D3: N – NE	0.939	0.403	2.330	0.020
	A5	D3: S – NE	0.979	0.412	2.370	0.018
	A5	D3: NW – NE	1.677	0.588	2.850	0.004
	A5	D3: SW – NE	0.660	0.495	1.330	0.183
8	A6	E4	0.212	0.061	3.460	<.001
	A6	K2	-0.332	0.097	-3.410	<.001
	A6	K3	0.253	0.105	2.420	0.016
13	A12	E2	-0.174	0.088	-1.982	0.047
	A12	E3	0.203	0.100	2.022	0.043
	A12	K1	0.323	0.097	3.345	<.001

	A12	D1	-0.432	0.168	-2.576	0.010
	A12	D3: E – NE	0.843	0.378	2.231	0.026
	A12	D3: C – NE	0.410	0.436	0.940	0.347
	A12	D3: N – NE	0.431	0.405	1.065	0.287
	A12	D3: S – NE	0.327	0.406	0.804	0.422
	A12	D3: NW – NE	0.471	0.575	0.819	0.413
	A12	D3: SW – NE	0.633	0.470	1.345	0.179
14	B1	E3	0.243	0.100	2.433	0.015
	B1	K3	0.270	0.096	2.816	0.005
	B1	A1	0.540	0.117	4.603	<.001
	B1	A3	0.236	0.115	2.048	0.041
	B1	D1	-0.373	0.171	-2.185	0.029
	B1	D3: E – NE	0.505	0.379	1.332	0.183
	B1	D3: C – NE	-0.026	0.455	-0.057	0.954
	B1	D3: N – NE	0.677	0.410	1.652	0.098
	B1	D3: S – NE	0.708	0.416	1.702	0.089
	B1	D3: NW – NE	-0.651	0.600	-1.085	0.278
	B1	D3: SW – NE	1.420	0.480	2.961	0.003
15	B2	E2	-0.270	0.087	-3.094	0.002
	B2	E4	0.147	0.062	2.375	0.018
	B2	A1	0.515	0.091	5.633	<.001
	B2	A4	0.153	0.068	2.256	0.024
	B2	D1	-0.439	0.171	-2.572	0.010
	B2	D3: E – NE	0.742	0.358	2.075	0.038
	B2	D3: C – NE	0.986	0.424	2.325	0.020
	B2	D3: N – NE	0.578	0.386	1.495	0.135
	B2	D3: S – NE	0.831	0.390	2.128	0.033
	B2	D3: NW – NE	-0.004	0.575	-0.007	0.994
	B2	D3: SW – NE	0.742	0.448	1.655	0.098
16	B3	E1	0.239	0.100	2.386	0.017
	B3	A1	0.692	0.091	7.640	<.001
	B3	D3: E – NE	0.622	0.357	1.739	0.082
	B3	D3: C – NE	0.740	0.424	1.746	0.081
	B3	D3: N – NE	0.718	0.392	1.832	0.067
	B3	D3: S – NE	0.980	0.394	2.487	0.013
	B3	D3: NW – NE	-0.517	0.561	-0.922	0.356
	B3	D3: SW – NE	1.654	0.454	3.647	<.001
17	B4	E4	0.235	0.062	3.780	<.001
	B4	K2	0.177	0.094	1.890	0.059
	B4	A1	0.646	0.139	4.650	<.001
	B4	A5	0.443	0.125	3.550	<.001
20	B7	E1	0.269	0.105	2.570	0.010
	B7	A1	0.535	0.153	3.500	<.001
	B7	A3	0.452	0.124	3.640	<.001
	B7	A4	-0.213	0.072	-2.950	0.003
	B7	A5	0.458	0.143	3.200	0.001

Note: E = East, C = Central, N = North, S = South, NW = Northwest, SW = Southwest, NE = Northeast.

Table IV. Regression Model Summary

Model	Resp. Var.	Deviance	AIC
1	K2	1245	1255
2	K3	1397	1421
3	A1	958	984
4	A2	1158	1172
5	A3	1435	1453
6	A4	1719	1749
7	A5	1108	1134
8	A6	1199	1213
13	A12	1514	1544
14	B1	1277	1307
15	B2	1333	1363
16	B3	1273	1297
17	B4	1336	1352
20	B7	1032	1050

Note: AIC = Akaike information criterion.

A Questionnaire

A.1 Internet Experience

Q1. Which of the following options is not a popular online social media platform in China?

- WeChat
- Douyin
- QQ
- Xiaohongshu
- Parking lot
- Sina Weibo
- Baidu Tieba
- Kuaishou
- Zhihu

[**Q2**] Scale 1-6: (1) Never (2) Less than one hour per week (3) At least one hour per week (4) At least five hours per week (5) At least ten hours per week (6) At least fifteen hours per week

Q2. How much time do you spend browsing the following social media platforms?
Platforms covered: Sina Weibo, Douyin, WeChat, Others

[**Q3**] Scale 1-6: (1) Never (2) Less than once per month (3) At least once per month (4) At least once per week (5) At least once per day (6) At least five times per day

Q3. How often do you participate in discussions (including posting, reposting, commenting and liking content) on the following social media platforms?
Platforms covered: Sina Weibo, Douyin, WeChat, Others

Q4. How often have you experienced some form of privacy breach in the last five years?

- Never
- Once or twice
- Three to five times
- More than five times
- Not sure/Don’t know

A.2 Location Privacy Knowledge

Q5. To the best of your knowledge, which of the following methods could mobile social media applications use to collect location data from users? (Select all that apply)

- Satellite-based location sensors (e.g., GPS, Beidou)
- Internet Protocol (IP) addresses
- Browsing history
- Purchasing habits
- Usage patterns (e.g., screen time)
- Photographs
- Self-disclosed geotags (e.g., “From···”)
- Textual contents (e.g., reviews, microblogs)
- Not sure/Don’t know

China’s PIPL is the country’s first comprehensive legislation regulating the protection of personal information and data of “natural persons” located within China.

Q6. Are you aware of China’s Personal Information Protection Law (PIPL), which went into effect on Nov. 1, 2021?

- I am not aware
- I have heard about the law, but am not sure about the details
- I have heard about the law and have basic understanding of what it covers
- I have heard about the law and fully understand my rights (e.g., obtaining consent; right to delete)
- I know all the details of the law

Q7. To the best of your knowledge, which of the following methods could protect one’s location privacy? (Select all that apply)

- IP Proxy
- Virtual Private Network (VPN)
- Tor
- Turning off your phone
- Use a backup phone number
- Not sure/Don’t know

A.3 Location Privacy Attitude

[**Q8.1-8.4**] Scale 1-5: (1) Strongly disagree (2) Somewhat disagree (3) Not sure (4) Somewhat agree (5) Strongly agree

Q8. Do you agree with the following views?

1. It bothers me to give location information to social media platforms.
2. Pervasive location information collection makes me worry about my location privacy when accessing social media platforms.
3. Compared to five years ago, I am more concerned about location privacy on the internet.
4. I believe other people (e.g., netizens and media) are too concerned with location privacy issues.

Q9. *If participants respond positively to Q8.3, Q9.1 will be displayed. Conversely, if participants respond negatively to Q8.3, Q9.2 will be displayed. Q9 will be skipped if participants choose "Not sure" for Q8.3.*

1. I am more concerned about location privacy issues on the internet than I was five years ago because:
   - I know more about location privacy risks online
   - I have more to lose if my location privacy were violated
   - I have had an experience that has changed my mind about location privacy
   - Some other reasons (please specify)
   - Not sure/Don't know
2. I am less concerned about location privacy issues on the internet than I was five years ago because:
   - Government regulations on data privacy have been strengthened
   - I feel safe even when my location information is disclosed
   - I feel powerless to make meaningful changes
   - Some other reasons (please specify)
   - Not sure/Don't know

IP location refers to the use of IP (Internet Protocol) addresses to identify the true geographic location of devices, such as cell phones and computers. On March 4, 2022, Sina Weibo debuted an IP location feature to counter disinformation about the crisis in Russia and Ukraine. The feature was introduced to several social media platforms (including Douyin, WeChat, Zhihu, Xiaohongshu, etc.) in April of the same year.

Q10. Which of the following screenshots does not contain the user's IP location information?
Screenshots from: Sina Weibo, Douyin, WeChat, Xiaohongshu, Bilibili

[**Q11.1-11.9**] Scale 1-5: (1) Strongly disagree (2) Somewhat disagree (3) Not sure (4) Somewhat agree (5) Strongly agree

Q11. Do you agree with the following views?

1. I am concerned that my location information published online might be used for purposes other than how I originally intended.
2. I am concerned that my location information collected by social media platforms might be used for purposes other than how I originally intended.
3. I believe other people (e.g., netizens and media) are too concerned with location privacy issues.
4. Compared to five years ago, I am more concerned about location privacy on the internet.
5. My level of privacy concerns will be reduced if the IP location feature is only available on specific topics/users/posts/keywords (e.g., sensitive topics such as the Russia-Ukraine war).
6. Public IP location is less intrusive than public GPS location.
7. I believe that online location privacy is invaded when the IP location feature cannot be turned off.
8. It is important to me that I am informed about how my IP location information is determined.
9. I am satisfied with the steps that social media platforms take to ensure that the published IP location is accurate.

Q12. At which geographic scale do you think the IP location feature would achieve the best balance between privacy protection and anti-disinformation?

- No IP location
- Country (e.g., USA)
- Region (e.g., south China)
- Province (e.g., Guangdong)
- City (e.g., Shenzhen)
- District (e.g., Futian District)
- Street (e.g., Fuhua 1st Rd)

Q13. Do you have any other points to make about IP location and location privacy?

A.4 Location Privacy Behaviour

[**Q14.1-14.6**] Scale 1-6: (1) Never (2) Rarely (3) Sometimes (4) Often (5) Always (6) Not sure/Don't know

Q14. Which of the following frequencies best matches my Internet behaviour?

1. The location services on my mobile device are turned on.
2. I share my locations through social media applications.
3. I allow an application to access my current location when prompted.
4. I purposefully enter inaccurate address information when required by social media platforms.
5. I use the IP location function to follow the latest locations of celebrities.
6. I test whether my IP location was accurately displayed on the social media platforms.

[**Q15**] Scale 1-5: (1) Strongly disagree (2) Somewhat disagree (3) Not sure (4) Somewhat agree (5) Strongly agree

Q15. I stop using certain social media platforms (or deleted applications) after the introduction of mandatory IP location disclosure (after April 2022).

A.5 Demographic Variables

Q16. Gender

- Male
- Female
- Non-binary
- Prefer not to answer

Q17. Age

- 19 and younger
- 20-24
- 25-29
- 30-34
- 35-39
- 40-44
- 45-49
- 50 and older
- Prefer not to answer

Q18. Your current location

- *A list of Chinese provinces*
- Prefer not to answer

Q19. Education level

- Middle school and below
- High school or technical school
- College degree
- Bachelor's degree
- Master's degree and above

Q20. Monthly income (Chinese Yuan)

- Less than 1500
- 1501-3000
- 3001-5000
- 5001-8000
- 8001-10000
- 10001-15000
- 15001-20000
- > 20001
- Prefer not to answer

Q21. What is your marital status?

- Single
- Married
- Divorced
- Prefer not to answer

Q22. How many children do you have?

- 0
- 1
- Two or more children
- Prefer not to answer

B Supplementary Regression Tables

Table 1: Supplementary Regression Results

Model	Resp. Var.	Predictor	Estimate	SE	Z	*p*
9	A7	K2	0.327	0.092	3.560	<.001
10	A9	E4	0.215	0.060	3.590	<.001
		K2	-0.196	0.098	-2.000	0.045
		K3	0.395	0.100	3.940	<.001
11	A10	E2	-0.211	0.100	-2.110	0.035
		E3	0.276	0.112	2.470	0.013
		K1	0.278	0.103	2.710	0.007
		K2	0.292	0.105	2.780	0.005
12	A11	E2	-0.211	0.094	-2.241	0.025
		E3	-0.332	0.105	-3.179	0.001
		E4	0.252	0.062	4.065	<.001
		K2	-0.881	0.110	-7.975	<.001
		D3: East – Northeast	0.732	0.377	1.942	0.052
		Central – Northeast	1.049	0.446	2.355	0.019
		North – Northeast	0.530	0.407	1.303	0.193
		South – Northeast	0.772	0.411	1.877	0.060
		Northwest – Northeast	0.395	0.587	0.673	0.501
		Southwest – Northeast	1.254	0.492	2.548	0.011
18	B5	E1	0.391	0.106	3.700	<.001
		E2	0.438	0.097	4.530	<.001
		A1	-0.439	0.089	-4.950	<.001
		A4	-0.292	0.066	-4.440	<.001
19	B6	E2	0.517	0.092	5.630	<.001
		K1	0.190	0.096	1.980	0.048
		K2	0.493	0.098	5.040	<.001
		D1	0.329	0.169	1.950	0.051
		D2	-0.113	0.055	-2.060	0.039

Table 2: Supplementary Regression Model Summary

Model	Resp. Var.	Deviance	AIC
9	A7	1326	1336
10	A9	1323	1337
11	A10	959	975
12	A11	1232	1260
18	B5	1346	1362
19	B6	1354	1372

Note: AIC = Akaike information criterion.