Negotiating Privacy and Mobile Socializing: Chinese University Students’ Concerns and Strategies for Using Geosocial Networking Applications

Haili Li

Abstract
Privacy risks have significant increase with the widespread use of geosocial networking applications (GSNAs). The Facebook data breach case in 2018 triggered many users’ concerns and focused attention on the debate about the trustworthiness of GSNAs globally. Particularly, the rapid development of Chinese GSNAs such as WeChat and Momo has been frequently cited as contributing to an increase in privacy risks in recent years. However, existing studies have primarily focused on the privacy risks of using GSNAs in Western contexts, while little is known about these issues in the Chinese context. This study thus attempts to expand upon prior research by examining concerns about GSNAs, as well as attitudes and strategies to address these concerns among Chinese university students. By conducting 47 semi-structured interviews, this study finds that although participants are generally concerned about the privacy risks of GSNAs, a few of them have taken steps to address their concerns. Five types of social privacy concerns, including information leakage/misuse, location tracking, malicious personal attacks, sexual harassment, and individual-targeted advertising, and three types of institutional privacy concerns, including information leaks, information tracking, and surveillance by apps and the Chinese government, have been identified in this research. Most participants have taken little action to address their privacy concerns and display an attitude of trust, ignoring and accepting the privacy risks of GSNAs. Comparatively, few participants have developed active strategies to mitigate their concerns, such as abstaining from or exercising caution when using apps and functions, and reporting privacy threats to app platforms. Significantly, this study offers new insights into users’ privacy concerns that are specifically associated with Chinese social and cultural contexts. However, as this research mainly focuses on privacy concerns and strategies from users’ perspectives, future studies are encouraged to delve into solutions and strategies to mitigate users’ privacy concerns in the global context of social media.

Keywords
privacy concerns, geosocial networking applications, dating apps, Chinese university students, strategies

Introduction
Currently, most smartphones are embedded with a Global Positioning System (GPS) which enables them to calculate relatively accurate location information (Hoang et al., 2016). This location-aware capability has thus facilitated the development of geolocation-based applications (Ding et al., 2014). Among all the geo-location-enabled apps, geosocial networking applications (GSNAs) have become prevalent and enjoy widespread popularity (Smith, 2016). A recent study revealed that 15% of US adults have used an online dating site or a GSNAS (Smith, 2016). The rate is even higher among people aged 18–24, at 22% (Smith & Anderson, 2016), demonstrating the popularity of GSNAs among young adults (Gatter & Hodkinson, 2016; Neuts, 2016). Many young people use social media in China; a report published in 2018 shows that 61% of social media users in China are aged 15–34 (Guo, 2018). GSNAs are typically used for socializing and dating (Ding et al., 2014; Farnden et al., 2015). Some popular GSNAs are social apps such as WeChat, Facebook, and LINE and dating apps such as Tinder, Grindr, Momo, Tantan, and Happn. Chinese GSNAs have grown markedly

Corresponding Author:
Haili Li, Digital Media Research Centre, Creative Industries Faculty, Queensland University of Technology, Kelvin Grove, Brisbane, QLD 4059, Australia.
Email: haili.li@hdr.qut.edu.au
during the past several years; WeChat is now used by 97% of all of the Internet users in China (Guo, 2018), and the number of its monthly active users reached 10.8 billion in 2018 (L. Peng & Ye, 2019). Another GSNA, Momo, has been reported to have around 1.033 billion monthly active users as of March 2018 (Momo, 2018). GSNA has obvious advantages such as portability, availability, locatability, and multi-mediality (Schrock, 2015), which provide users with the ability to connect with each other in a more immediate, accessible, and convenient way (Choi et al., 2016), and thus appeal to more people.

However, with the rapid development and widespread prevalence of GSNA, some potential risks associated with these apps’ special functions and features (e.g., location-aware functionality) have gradually emerged and induced severe problems. One of these significant issues is the potential for privacy invasion, for example, the leak of users’ locations and the surveillance of private and sensitive information by the app platforms which may be intentionally exploited by attackers for illegal purposes (Farnden et al., 2015; Hoang et al., 2016; Polakis et al., 2015). In the recent Facebook data breach case in 2018, nearly 50 million users’ accounts were compromised after an attack by hackers (Carrie, 2018). The Chinese GSNA WeChat and Momo have been reported to leak users’ data as well; 364 million user profiles on WeChat monitored by the Chinese government were reported to be compromised by data leakage (Huang & Soo, 2019), while 30 million Momo users’ data were reportedly being sold online for about RMB 200 (≈US$30) per profile (Lee, 2018). Although Facebook, WeChat, and Momo offered explanations for the data breaches, the endlessly emerging cases of privacy concerns around GSNA have caused apprehension and distrust among users (Griffin et al., 2018).

The development and prominence of Chinese GSNA in recent years along with the increasing privacy issues of these apps (Ding et al., 2014; J. Peng et al., 2015) call for immediate scholarly attention. However, while users’ privacy concerns of using GSNA have become a serious research focus in media and communication studies (e.g., Lutz & Ranzini, 2017; Masur & Scharkow, 2016), a sizable amount of the scholarship has mainly concentrated on Western contexts (e.g., Farnden et al., 2015; Griffin et al., 2018; Lutz & Ranzini, 2017). Limited attention has been paid to this issue in the Chinese context. Thus, this research attempts to extend the previous research by focusing on China. In this sense, Chinese university students have been chosen as the research subjects for the following two reasons. First, university students are heavy users of social media (Lenhart & Madden, 2007; Zickuhr, 2010), that is, 94% of university students use social media (Junco et al., 2011), a rate higher than the general population (Guo, 2018; TalkingData, 2016). Second, university students participate in more diverse activities on social networking sites (SNSs) compared to the general population, and the frequency that they engage in these activities is also higher due to their flexible schedules (Zickuhr, 2010). A report also shows that Chinese university students use a wide range of mobile social media and are active users on these platforms (TalkingData, 2016). The more activities that university students engage in, the more experiences and thoughts on subjects like privacy concerns they will likely have regarding the use of GSNA. Thus, this study aims to explore how Chinese university students perceive the privacy issues surrounding GSNA as well as their attitudes and actions taken regarding these concerns. Based on this objective, two main research questions have been designed:

**RQ1.** What are Chinese university students’ privacy concerns regarding the use of GSNA?

**RQ2.** What are Chinese university students’ attitudes and actions taken regarding their privacy concerns?

In this article, I will first discuss the existing literature on privacy risks that have been posed by GSNA, users’ privacy concerns, and their strategies to mitigate the privacy risks. In the following methodology section, I will explain how the semi-structured interview method was employed in this research to answer the aforementioned research questions. The results will demonstrate the findings regarding participants’ privacy concerns and attitudes/strategies to address their concerns, followed by the conclusion and a discussion focusing on how privacy risks might be addressed in the context of social media.

**Literature on Users’ Privacy Concerns of Using GSNA**

The popularity of GSNA and the substantial amount of users’ private information in their possession have exacerbated these apps’ vulnerability to privacy leaks (Hoang et al., 2016). Among GSNA, dating apps such as Happn (Luzio et al., 2018; Ma et al., 2017), Tinder (Lutz & Ranzini, 2017), and Grindr (Corriero & Tong, 2016), and mobile social apps such as WeChat (Ding et al., 2014; J. Peng et al., 2015; X. Wang & Gu, 2016) and Momo (M. Li et al., 2014) have been revealed to have a high risk of compromising users’ private information and has thus triggered privacy concerns. Currently, most dating apps rely on location-tracking functions to provide location-based real-time dating, facilitating people seeking “local and immediate” (Brashers, 2001) dates. Users are easily located and are thus exposed to serious physical threats such as rubbery, stalking, and kidnap- ping (Furini & Tamanini, 2015; Hoang et al., 2016). For example, Luzio et al. (2018) argue that the detailed private information of users including their accurate real-time locations, daily routines, and social relationships with other users on the dating app Happn could be exploited by an attacker intentionally to seriously jeopardize users’ privacy and security. Similarly, other dating apps such as Grindr, Skout, and
Tinder have been shown to have similar risks (Farnden et al., 2015). In addition, users’ data on these dating apps have not been properly protected. For example, deleted user accounts along with users’ relevant information can be easily recovered on some dating apps (Farnden et al., 2015). Apart from Western dating apps, Chinese GSNAs such as WeChat and Momo have also been found to potentially risk leaking users’ location information via the location-tracking function (Ding et al., 2014; H. Li et al., 2018; M. Li et al., 2014; J. Peng et al., 2015; R. Wang et al., 2015; X. Wang & Gu, 2016). Privacy risks of GSNAs have spawned users’ concerns (Furini & Tamanini, 2015; Masur & Scharkow, 2016; Sarikakis & Winter, 2017), and users have thus developed diverse strategies to alleviate their concerns and protect their privacy (Lankton et al., 2017; Vishwanath et al., 2018; Young & Quan-Haase, 2013).

Aside from privacy which has been identified as a top concern of using GSNAs, other concerns include security, identity theft involving personal profiles on dating apps, and recognition/social stigma associated with using gay dating apps (Corriero & Tong, 2016; Gibbs et al., 2010; Griffin et al., 2018). Compared to men, women demonstrate more privacy and safety concerns regarding the use of GSNAs and are in particular more cautious in using location-tracking functions (Furini & Tamanini, 2015; Griffin et al., 2018; Madden et al., 2013). While studying Facebook users’ privacy concerns, Raynes-Goldie (2010) proposed the concepts of social and institutional privacy concerns. Social privacy concerns revolve around privacy violations by other users of SNSs and apps, for example, being hacked, stalked, or receiving inappropriate content from other individual users (Lutz & Ranzini, 2017; Raynes-Goldie, 2010). Institutional privacy concerns include the use of users’ private data against users’ wills for certain purposes (e.g., for commercial purposes) by app providers, other institutions, and governments (Lutz & Ranzini, 2017; Raynes-Goldie, 2010). Based on Raynes-Goldie’s (2010) differentiation between these two concepts, several studies have compared users’ social and institutional privacy concerns (Lutz & Ranzini, 2017; Masur & Scharkow, 2016; Quinn & Epstein, 2018; Young & Quan-Haase, 2013). For example, young Facebook users such as university students have been found to be more concerned about social privacy than institutional privacy (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). Similarly, greater concern about social privacy has also been demonstrated among other social media users (Masur & Scharkow, 2016; Quinn & Epstein, 2018). On the contrary, Lutz and Ranzini (2017) suggest that compared to social privacy, Tinder users appear to be more concerned about institutional privacy. Users are more worried about how Tinder will use their personal data and how Tinder tracks and sells their private data to other institutions. The above studies provided the impetus for this research to differentiate between Chinese university students’ concerns about social versus institutional privacy. However, these studies have largely concentrated on Western users, and this research will thus expand on prior knowledge by providing a non-Western context, specifically a Chinese context.

To mitigate their privacy concerns, users have developed diverse strategies according to the specific features of different GSNAs (Albury & Byron, 2016; Lankton et al., 2017; Masur & Scharkow, 2016; Vishwanath et al., 2018). Several studies have concentrated on how users manage their privacy on Facebook. Compared to institutional privacy, Facebook users are more concerned about their social privacy; thus, they have mainly taken actions to protect their social privacy (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). These strategies encompass disclosure management such as deleting/removing posts, photo tags and contact information, and accessibility management (i.e., restricting other people’s access to the user’s private information) such as using a fake user name and limiting friend requests (Lankton et al., 2017; Raynes-Goldie, 2010; Vishwanath et al., 2018; Young & Quan-Haase, 2013). In terms of disclosure management, Masur and Scharkow (2016) suggest that trust is a significant factor that influences SNS users’ disclosure management strategies. If users have a high level of trust in the recipients of their information, they are more likely to disclose information with little concern about the consequences. A privacy paradox (Barnes, 2006) has been discovered to exist in relation to users’ privacy concerns and the actions they adopt to deal with these concerns. That is, although users are concerned about privacy, they typically take little to no action to mitigate privacy risks. Users are worried about their privacy, yet they do not stop sharing information on social media (Fogel & Nehmad, 2009; Mihailidis, 2014). The privacy paradox has also been revealed to exist among Chinese university students in this research, which will be analyzed in the “Results” section.

Several research gaps have been identified through the analysis of the previous studies. First, most studies on GSNAs, particularly on their privacy risks and users’ privacy concerns, have primarily focused on a Western context, while non-Western apps and user groups remain understudied. Second, although university students are heavy users of GSNAs (Yang et al., 2016), limited scholarly attention has been paid to this group to examine their privacy concerns (Griffin et al., 2018; Lankton et al., 2017; Young & Quan-Haase, 2013). Third, specifically in the Chinese context, existing research has mainly concentrated on the Chinese GSNAs such as WeChat and Momo to examine their potential privacy risks while overlooking users’ privacy concerns and attitudes toward using these apps. Therefore, this research aims to extend the previous studies by offering insight into the understudied research domain with a specific emphasis on Chinese university students’ privacy concerns and the strategies they have developed to mitigate these privacy risks.
**Method**

A semi-structured interview method was employed in this study. The semi-structured interview allows researchers to discuss topics that have been pre-determined while remaining open to alternative issues that participants may want to discuss (Bryman, 2012). It provides a flexible method for organizing the interview schedule and questions, as well as an ability to investigate participants’ thoughts and experiences. The semi-structured interview is therefore a suitable method for this study to explore participants’ privacy concerns regarding their use of GSNAs in an open and flexible way. The interview process primarily incorporates two phases: recruiting participants and conducting the interviews with participants. Participant recruitment information was disseminated through multiple channels including displaying posters in four universities in Beijing and distributing information through emails, online forums, and social media platforms (e.g., Weibo and WeChat) since May 2017. Within 1 month, more than 70 potential participants expressed interest in participating in an interview. Taking into consideration the gender ratio of the participants, 47 participants, including 25 female and 22 male university students, were randomly chosen from the respondents. An interview guide was designed based on the knowledge gained from relevant literature, three pilot interviews, and personal experience of using GSNAs. The interview guide includes four sections. The first section is demographic information, including age, gender, sexual orientation, educational background, and major. Following this is the participants’ basic information regarding their use of GSNAs, for example, which GSNAs participants have used, how long they have used these apps, their frequency of using these apps, and their ranking of GSNAs in terms of their perceived trustworthiness. The third part focuses on participants’ privacy concerns regarding their use of GSNAs, how these concerns have been shaped and developed, and their experiences of encountering privacy threats. Finally, the fourth section looks at participants’ attitudes toward these privacy risks and actions they have taken to mitigate their concerns. It should be noted that specific questions in each of the above sections were sometimes tailored according to different participants’ individual responses. The semi-structured interviews were conducted from June to September 2017: nine face-to-face talks and 38 WeChat audio/video calls. These interviews were audio-recorded, transcribed, and translated from Chinese to English for data analysis. Thematic analysis, “a method used for identifying, analyzing and reporting patterns (themes) within data” (Braun & Clarke, 2006, p. 79), was applied in this study to identify, classify, and analyze different themes regarding participants’ privacy concerns, and their attitudes and strategies toward these concerns.

Table 1 shows the demographic information of the 47 participants. The average age of the participants is 24.2. The percentage of female participants is slightly higher than that of males. Most participants identified themselves as heterosexual, while three male participants identified themselves as homosexual. More than half of the participants were undergraduate students, while others were involved in higher degree programs including master’s and PhD programs. Participants majoring in science, technology, engineering, and mathematics (STEM) disciplines account for a higher proportion than participants from Arts and Humanities majors. Building on the statistics of Table 1, the influence that the demographic information has on different groups of participants’ privacy concerns and their attitudes toward privacy risks will be revealed in the “Results” section.

**Results**

GSNAs participants mainly used include WeChat, Momo, Tantan, Bolalu, Youjia, Paipai, and Blued, most of which are social and dating apps. Among these GSNAs, WeChat, as a multi-purpose social app, was perceived as the most important and most frequently used app by participants. Some participants suggested that they check WeChat messages “very often” even when there is no new message notification. The second most-popular GSNAs among participants is Momo, which is reported to be used for entertainment (e.g., watching live streams, playing games), socializing, and finding dates. The frequency of the participants’ use of GSNAs was reported to depend on the types of the apps and participants’ individual habits. For example, WeChat is the app used most frequently, while dating apps such as Paipai and Youjia were reported to be “occasionally” used by participants.

| Major (discipline) | Numbers | Percentage |
|--------------------|---------|------------|
| Arts and Humanities | 19 | 40.4 |
| STEM | 28 | 59.6 |

**Table 1.** Demographic Information of the Participants.

| Age (years) | Numbers | Percentage |
|-------------|---------|------------|
| 18–20 | 12 | 25.6 |
| 21–25 | 23 | 48.9 |
| 26–30 | 7 | 14.9 |
| 31–35 | 5 | 10.6 |

| Gender | Numbers | Percentage |
|--------|---------|------------|
| Female | 25 | 53.2 |
| Male | 22 | 46.8 |

| Sexual orientation | Numbers | Percentage |
|--------------------|---------|------------|
| Heterosexual | 44 | 93.6 |
| Homosexual | 3 | 6.4 |

| Education background | Numbers | Percentage |
|----------------------|---------|------------|
| Undergraduate student | 26 | 55.3 |
| Master’s student | 14 | 29.8 |
| Doctoral student | 7 | 14.9 |

STEM: science, technology, engineering, and mathematics.
The ranking of GSNAs by participants, according to their level of trust toward these apps, demonstrates that WeChat was viewed as the most trustworthy app; participants perceived it as "indispensable" and was more important than other apps, fulfilling a range of purposes. However, although Momo is a popular app among participants, it was perceived as the most untrustworthy app as most participants regarded it as a hookup app and described its main function as "looking for casual sex and relationships":

WeChat is an indispensable app for me. I use it for almost everything, so I trust it very much. But I don't trust Momo as I think it's a hookup app although it claims that it is a social app. (Female 8, 25)

WeChat is such an important app for me which can be used for so many purposes: financing, maintaining connections with my family and friends. I have an intimate feeling with WeChat. Although I also use Momo, it's more like a tool for entertainment and finding casual dates. (Male 4, 23)

**Chinese University Students’ Privacy Concerns**

Some studies have pointed out that users are generally unaware of or not concerned with the privacy risks that exist with their use of mobile and social media (Almuhimedi et al., 2015; Karanja et al., 2018). In contrast, other research has suggested that users care about privacy and perceive it as "very important" to know who can get information about them on social media (Rainie, 2016). While participants were asked “Have you realized that there are privacy problems regarding using GSNAs?” and “What do you think about the privacy issues?,” this study found that not only were most participants aware of privacy threats, they also viewed these potential privacy risks as significant issues:

I know there are a lot of privacy risks about using these apps and some of them are big issues. If these privacy problems are not treated seriously, they will have serious consequences then. (Female 1, 29)

Participants’ privacy concerns are shaped and developed by their individual experiences, especially the privacy threats they have personally encountered: hearing from other people’s, such as their parents’ and friends’, experiences; and news reports about the privacy problems of GSNAs. Compared to getting information from news reports and hearing other people’s accounts, participants’ own experiences of privacy threats appear to be more likely to exacerbate their privacy concerns.

Social privacy concentrates on the privacy violations by other users of GSNAs, while institutional privacy targets the privacy threats from app platforms, governments, and other organizations (Lutz & Ranzini, 2017; Raynes-Goldie, 2010). With this differentiation, this study has classified participants’ concerns into two types, as shown in Table 2.

**Table 2. Participants’ Social and Institutional Privacy Concerns.**

| Social privacy concerns | Institutional privacy concerns |
|-------------------------|-------------------------------|
| The leakage of personal information by other users | The leakage of personal information by apps |
| Location tracking by other users | Users’ information tracking by apps |
| Malicious personal attacks | Surveillance of personal information by apps and the Chinese government |
| Sexual harassment | |
| Individual-targeted advertising | |

Five types of social privacy concerns were proposed by participants, which mainly focus on the misuse and tracking of personal information by other users and negative information received from others on GSNAs. For example, participants mentioned that sometimes their personal information was published by other users without their consent and thus made them feel that their privacy was violated, which echoes the Lutz and Ranzini’s (2017) finding on Tinder users’ privacy concerns. Compared to acquaintances, participants expressed more concerns about the misuse of their private information by strangers:

Sometimes my friends forwarded our private chats to a big WeChat group which made me feel embarrassed. But compared to this, I would be more worried if the chat messages were forwarded by a stranger. (Female 2, 25)

Once I was asked to show a personal photo by a user on Momo while we were chatting. I didn’t think too much and sent a photo to him. Later I found that he posted my photo to one of our Momo groups which attracted other group members’ attention and discussion about my photo. That made me so afraid, as anyone in that group could then forward my photo to others if they want. After that I never sent any photo to any stranger on Momo. (Female 25, 19)

Apart from the misuse (e.g., unwanted publication) of their personal information such as photos and messages, participants also worried about the leak of their financial information (e.g., bank accounts) when they transferred money to other users, especially strangers on GSNAs. It is worth mentioning that compared to participants who identify as heterosexual, participants who identify as homosexual are more concerned about the leakage of information associated with their identity and sexuality on gay social and dating apps such as Blued:

Every time I used Blued to talk to people, I always worried, what if I am identified by others, like nearby users, as some of them might be my classmates or people who know me. (Male 1, 21)
Participants commented that being tracked and located by other users on dating apps was “scary” and expressed concerns about using this function:

There were several times while I was chatting with nearby users on Momo, they could almost accurately estimate my location. It was so scary that if they wanted, they could track and stalk me at any time. (Female 20, 20)

Malicious personal attacks were also identified as a privacy threat of using GSNAs by participants, which were reported as messages received from strangers in most cases. Participants showed different attitudes toward malicious messages, including other users’ unfriendly comments on their posts and other activities (e.g., live streaming). Some participants chose to “ignore” these comments without any reaction, while others thought that the malicious messages damaged their personal reputation and invaded their privacy, so they reported these malicious messages to the app platforms:

I always post information on Momo, including my selfies and texts. Sometimes I do get the unfriendly comments from some strangers. Some of those comments are very malicious, but anyway, they are just from people I don’t know. So, I don’t care much and just ignore them. (Male 8, 19)

Once we (my friend and me) were live streaming on Momo. There was a user who kept posting malicious comments, like “You are so ugly. Get out of the live streaming room.” I was very angry and also responded against him. We were, like, having a battle. Finally, I reported this user to Momo administrators, and they kicked him out of our live stream. (Male 22, 24)

Some female participants reported that they have been sexually harassed by “bad guys” on dating apps, especially on Momo, for example, being asked to have one-night stands and send erotic photos. These experiences caused their concerns and also affected their attitudes and perceptions of specific dating apps. For example, several participants said that using dating apps such as Momo to find true love and serious relationships is “impossible” and “ridiculous”, as they thought most male users on Momo are only interested in “flirting” and “casual sex” based on their experiences of encountering sexual harassment:

Receiving harassing messages like nasty words on Momo happens quite often. Most of them are from “bad guys” who just want to have one-night stands with me. (Female 18, 21)

Promotion of individual businesses has become increasingly popular and prevalent on multiple Chinese app platforms in recent years (Na, 2018), such as WeChat Business and Momo Business, which means users take advantage of the app platforms to advertise products and sell them to other users. The targeted advertising on apps was seen as a violation of their private time and space by participants. Particularly, participants showed more discontent with individual advertising by people who they know like friends than strangers:

I don’t care if strangers posted some advertisements in some big WeChat groups. But what I don’t like is that some of my friends always posted advertisements in Moments and our private WeChat groups. They didn’t respect other people’s privacy as they never asked whether we wanted to see these advertisements. (Female 19, 33)

Participants’ institutional privacy concerns mainly revolve around the collaboration between apps and other organizations, and the surveillance by apps and the Chinese government. Unlike the social privacy concerns which primarily arise from the participants’ experiences in real life, some of these institutional privacy risks have never happened to participants. Instead, their concerns about institutional privacy have mainly been shaped by news reports relevant to the privacy risks of apps, such as Momo’s data breach (Lee, 2018):

These kind of news reports about information leakage, like Momo’s user data being sold online, always made me worry a lot. (Female 13, 27)

Participants’ privacy concerns in terms of information leakage by apps primarily focus on intentional and unintentional information leaks. Intentional information leakage includes app platforms selling users’ data to third parties purposefully (e.g., for commercial trade), which was found to be the most significant privacy concern among Tinder users by Lutz and Ranzini (2017). Unintentional information leakage means app platforms leaking users’ information unintentionally due to their technical vulnerabilities. Compared to intentional data leakage, participants appear to be more concerned about unintentional privacy leaks. Additionally, participants also expressed their distrust of GSNAs’ capabilities of protecting users’ data privacy:

I am more concerned about unintentional data leakage. Because it means they [apps] are unaware of their own technical problems, and thus couldn’t be able to protect users’ data privacy and safety. (Female 16, 24)

Rapid technological development is always accompanied by all kinds of technical issues. I’m afraid that currently these apps have not been developed very well in terms of preventing risks. (Male 12, 27)

GSNAs’ information-tracking behavior was reported as another concern by participants, similar to Lutz and Ranzini’s
Li et al. (2017) findings about users’ concerns regarding Tinder tracking and analyzing their personal data. This study reveals that participants are not entirely aware of what data-tracking behavior GSNAs conduct as they have no resources to know this information. However, participants identified different apps’ data-tracking behavior from some of their daily experiences. For example, participants found that sometimes when they browsed WeChat Moments (posts from WeChat contacts), commercial advertisements matching with their interests came up, which are labeled “marketed by WeChat.” Participants then realized that WeChat tracks their data and analyses user behavior such as search histories (Karanja et al., 2018), and thus gain information about their interests and user habits. In this way, WeChat could post advertisements targeting different users’ tastes. Some participants showed understanding of data tracking and analysis by apps, and they worried that this personal information, including their location history, search history, and personal preferences, may possibly be hacked or used for “bad things” such as illegal purposes:

As I always travelled while I was working for a public relations company, I got advertising information promoted by WeChat about flight tickets and hotel bookings quite often. I don’t mind that WeChat tracked my information in this way, but I worry that what if my personal information is used for some bad things. (Male 7, 27)

Participants’ concerns about surveillance of private information conducted by app platforms and the Chinese government echo Karanja et al.’s (2018) findings regarding users’ worries about surveillance by governments while using social media. Among the institutional privacy concerns, this was the gravest concern of participants, who spoke of personal messages and public news on apps such as WeChat and Momo being censored and deleted. Many participants mentioned a common phenomenon: they were notified that a subscribed account (i.e., a public or self-media account on WeChat) posted new information, but later when they opened the account, the information had already been deleted and replaced with a warning sign that “the content could not be checked as it violates the rules of WeChat”:

I noticed that this warning sign came up quite frequently on WeChat. If the news included sensitive words or was against the government, it would be quickly deleted and, as I know, sometimes even subscribed accounts will be closed by WeChat. (Male 22, 24)

In recent years, the Chinese government has conducted a strict Internet censorship policy on all social media platforms to censor and monitor users’ posts (Liao, 2019). For example, according to the government’s requirements, mobile social apps such as WeChat and Momo established their own censorship system to censor users’ posts on their platforms (Lee, 2018; Liao, 2019; L. Peng & Ye, 2019). Participants commented that some posts are deleted by WeChat because of the “sensitive keywords,” especially political and “radical” keywords or they are found to be against the voice of the government. Although some participants said that they never participated in any political discussion or posted any political comments, they still have concerns about the censorship systems on GSNAs as they feel insecure and unfree, and believe that their conversations are under continuous surveillance. Several participants mentioned that their freedom of expression is “restricted” and “deprived” due to the censorship system, and that there are “arrangements” by censors regarding what can be seen or not:

Compared to other concerns, being monitored by the app is the biggest privacy concern for me. It makes me feel unfree and as though I lost my rights to speak my own opinions if they are not “politically right.” (Male 12, 27)

Previous studies have pointed out that compared to institutional privacy, users of Facebook (Raynes-Goldie, 2010; Young & Quan-Haase, 2013) and other social media (Masur & Scharkow, 2016; Quinn & Epstein, 2018) care more about social privacy, while Lutz and Ranzini (2017) suggested that users of Tinder are more concerned about institutional privacy compared to social privacy. However, this study finds that although participants expressed more concerns about social privacy than institutional privacy in general, clear differences in responses between genders, sexual orientations, educational backgrounds, and majors have been noted. Male participants showed more concerns about institutional privacy, while females reported more worries about social privacy threats. Particularly, in terms of social privacy, female participants expressed more concerns about sexual harassment and location tracking by other users. Regarding institutional privacy, male participants’ main concerns focus on the surveillance of users’ personal information and activities by apps and the Chinese government, while pronounced concerns regarding institutional privacy threats were not found among female participants. Sexual orientation is another element that affects participants’ concerns. The three participants who identify as homosexual showed much more concerns about social privacy risks, especially the leakage of information with regard to their identity and sexuality on Blued. Educational background also influences participants’ privacy concerns. This study reveals that the participants who engaged in higher degree programs including master’s and doctoral programs expressed more concerns regarding institutional privacy, while undergraduate students cared more about social privacy.

**Attitudes and Actions Toward Privacy Concerns**

Participants broadly expressed two types of attitudes and actions toward addressing their privacy concerns in this research. The first type is understanding and accepting the
Concerns. Strategies for app developers to better understand user habits and platforms’ behavior of tracking and analyzing users’ data will not do anything purposefully to harm users. The app they still claimed to trust that the apps and the government pants felt deprived of a part of their privacy and freedom, attitudes toward the privacy risks. Although some participants “trust” were frequently mentioned while talking about their and trust in the app platforms as the words “understand” and “hard,” and “impossible”:

cerns by participants, while taking action to change other view as “the best strategy” to deal with social privacy con-
or accepting other users’ behavior without taking action was viewed as “the best strategy” to deal with social privacy con-
cerns by participants, while taking action to change other users’ behavior on GSNAs was deemed “embarrassing,” “hard,” and “impossible”:

I felt embarrassed to tell my friends to stop posting advertisements on WeChat, so what I did is ignoring their messages purposefully. There is no appropriate way to solve this issue. (Female 12, 23)

It’s hard to avoid all of the unwanted forwarding of my personal posts by my friends as they don’t think they violate my privacy by doing so. It’s just like strangers don’t think they harassed you when they sent you sexually harassing messages. It’s hard to stop people doing this, so I just accept these behaviours. (Female 4, 25)

In terms of institutional privacy, most participants who hold the first type of attitude expressed their understanding and trust in the app platforms as the words “understand” and “trust” were frequently mentioned while talking about their attitudes toward the privacy risks. Although some participants felt deprived of a part of their privacy and freedom, they still claimed to trust that the apps and the government will not do anything purposefully to harm users. The app platforms’ behavior of tracking and analyzing users’ data was regarded as “legitimate” and “normal” commercial strategies for app developers to better understand user habits and behavior, while surveillance by apps and the Chinese government was perceived as a method to establish a “healthy” and “secure” online environment. Participants also commented that it is “impossible” to take action regarding these institutional privacy threats and that they have no idea what kinds of actions they could adopt if these threats, such as information leakage by the app companies, happen one day. Participants also reported that they could only “accept” these institutional privacy risks as they do not think users have enough capability to develop strategies to solve these complicated and professional technical issues:

I know all of the apps are tracking and analysing our data for their own benefit. Although I worried, I could still understand their behaviour. Also, I trust them as I think every app has its own rules for protecting user data and “bottom lines” in analysing user data legally. (Female 12, 23)

I think it’s hard for us to take effective measures to prevent any risk as we are not IT experts. If the app company wants to sell or leak our data purposefully, we couldn’t do anything unless you give up using that app. (Male 5, 26)

Other participants spoke of taking active actions to mitigate the privacy risks of GSNAs, including three specific types of strategies as shown in Table 3. Compared to participants who took little to no action, fewer participants reported taking active actions. These active actions were mostly developed to deal with social privacy concerns. Being more cautious while using GSNAs was perceived as the most “suitable” and “effective” means to mitigate privacy concerns. Unlike completely abstaining from using an app or some of its functions, participants preferred to use the app with adjusting their strategies and being more cautious. For example, most participants reported that normally they do not look at the default settings while registering their information on an app, as they think it is “troublesome” and “a waste of time” to read these items. This corresponds to Jedrzejczyk et al.’s (2010) finding that users lack patience reading privacy guidelines and are not good at applying appropriate privacy settings. However, some participants reported that after realizing or experiencing the privacy risks, they changed their behavior around using GSNAs. They became more cautious and began to use active strategies to prevent risks, for example, checking the default settings while installing an app, reading the terms of use before registering on an app, ensuring the security of the environment before using the location function, not sending personal photos to strangers before establishing their trustworthiness, not having “too personal” conversations with other users in case the information is misused, and not participating in politically sensitive discussions in case of surveillance:

I know Momo has a lot of privacy issues, but I still want to use it. So, to use it in a safe way, I become very cautious in using the location function now. I never opened the location when I am

---

**Table 3. Participants’ Attitudes and Actions Toward Privacy Concerns.**

| Taking little to no action                                      |
|----------------------------------------------------------------|
| Trusting users and apps without taking any action              |
| Ignoring privacy concerns with taking little to no action      |
| Accepting privacy risks with taking little to no action         |

| Taking active actions                                          |
|----------------------------------------------------------------|
| Abandoning using specific apps and functions                  |
| Being more cautious while using GSNAs                         |
| Reporting privacy threats to app platforms                     |

GSNAs: geosocial networking applications.
alone, outside [of campus] or at night. I only used it after I make sure the nearby environment is safe. (Female 12, 23)

After I knew WeChat has issued some new rules for censorship and surveillance of users’ messages, I became very careful. I never posted or forwarded any radical or sensitive things as I don’t want to be censored and put on the “blacklist”. (Male 11, 24)

Abandoning using specific apps or some functions was perceived as the “safest strategy” to completely eliminate privacy concerns by four participants. Although they described this strategy as a radical method, they asserted that not using the apps or some functions is the only way to ensure complete safety and privacy. This study also finds that participants who adopted this strategy had more privacy concerns and perceived GSNAs as untrustworthy:

I heard from the news reports that some young girls used Tantan and then met bad guys which caused serious consequences. I felt so scared so I didn’t use it anymore after watching these news. But the app was still on my phone and I felt unsafe. Then one day I just uninstalled it and I feel much more comfortable now. (Female 13, 27)

I used WeChat Shake (i.e. shaking the phone to get a random chance to talk with a stranger) to look for people nearby and had very terrible experiences. Since then I never trusted the function. I have to use WeChat but I never used WeChat Shake after that. (Female 25, 19)

Reporting privacy issues to the app platforms was identified as a strategy that the fewest participants (only three Momo users) have adopted. Participants reported that they adopted this strategy while encountering privacy risks such as sexual harassment and malicious comments from other Momo users. However, reporting privacy issues to administrators on Momo was viewed as a method “only useful for once” by participants, and they suggested platforms such as Momo should develop a system to automatically detect harassment and malicious texts or to issue clear administrative regulations to tackle these privacy risks and protect users’ benefits:

I received sexually harassing messages from a stranger nearby on Momo and I reported him to the administrator. The administrator solved the problem very quickly and told me that the user got a warning and his account would be suspended if he sent similar messages to me again. But after that I still got harassing messages from other users. It’ll be troublesome if I report these messages every time. Momo should think about an efficient way to work this out. (Female 25, 19)

Gender and major are two variables that affect participants’ attitudes and actions toward their privacy. Most male participants showed an understanding of these privacy risks and they preferred to either accept these risks or trust other users and app platforms without taking action. For example, male participants frequently responded “it doesn’t matter to me,” “it doesn’t bother me,” and “I don’t care” when asked about privacy issues. Female participants appeared to be more active in developing strategies to tackle privacy problems, especially in terms of being more cautious while using GSNAs. In addition, female participants expressed less trust in GSNAs and a stronger desire for app platforms to take more responsibility to protect users’ privacy. Participants from STEM disciplines, especially information technology and Internet security, were found to be more active in taking actions to deal with their privacy concerns.

Conclusion and Discussion

This study explores Chinese university students’ concerns about using GSNAs, as well as their attitudes and actions toward mitigating these concerns through conducting 47 semi-structured interviews. Privacy issues have become significant (Farnden et al., 2015; Hoang et al., 2016) with the rapid development of GSNAs worldwide (Smith, 2016; Smith & Anderson, 2016), as represented by the privacy concerns raised by the recent Facebook data breach case (Carrie, 2018). Particularly, Chinese GSNAs such as WeChat and Momo have become increasingly prevalent, which has also caused serious privacy issues (Ding et al., 2014; Lee, 2018; Liao, 2019; J. Peng et al., 2015). However, a majority of the existing studies have concentrated the privacy risks of GSNAs and users’ privacy concerns in Western contexts (Griffin et al., 2018; Lutz & Ranzini, 2017), yet little is known about this issue in the Chinese context. This study aims to enrich the prior studies by focusing on exploring users’ concerns in a Chinese context. As the major user group of GSNAs (TalkingData, 2016), Chinese university students have been chosen as the research subjects for this study due to their active and frequent use of GSNAs (Guo, 2018; TalkingData, 2016; Zickuhr, 2010).

Results showed that participants were largely concerned about the privacy risks of GSNAs and perceived them as significant issues, yet only a handful of them have taken active actions toward mitigating these risks. Participants’ privacy concerns were revealed to have been primarily shaped by their and other people’s experiences of encountering privacy threats on GSNAs as well as news reports relevant to privacy problems. Building on Raynes-Goldie’s (2010) differentiation of social and institutional privacy concerns and other studies on these two types of concerns (Lutz & Ranzini, 2017; Young & Quan-Haase, 2013), this study has classified participants’ privacy concerns thusly. Five types of social privacy concerns, including information leakage/misuse, location tracking, malicious personal attacks, sexual harassment, and individual-targeted advertising, and three types of institutional privacy concerns, including information leakage, information tracking by apps, and surveillance by apps and the Chinese government, have been identified through the interviews. Notably, although this study has a small sample of participants, the results demonstrate conspicuous differences in privacy concerns and strategies between participants who have different gender, level of education, major and sexual identity. Women,
undergraduates, and homosexuals are more concerned about social privacy, while men, master’s and doctoral students, and heterosexuals reported more worries about institutional privacy. Similar to prior research (Shklovski et al., 2014; Zurbriggen et al., 2016), a privacy paradox was seen in users’ privacy concerns and their actions toward these concerns in this study: although some participants showed significant concerns, they did not take action to mitigate their concerns. Instead, they chose to trust the GSNAs, or either ignore or accept the privacy risks. Other participants actively developed strategies to deal with their privacy concerns, for example, abstaining from using apps and functions, being more cautious in their use of apps and functions, and reporting privacy threats to app platforms. Women and students in STEM majors were more active in taking actions to deal with their concerns, while men and Arts and Humanities majors took little action.

This study enriches previous research regarding users’ privacy concerns, especially in a Chinese context which has not been paid much attention. Due to the objective differences between Chinese and Western societies, and the uniqueness of GSNAs’ development in the Chinese context, some of the users’ concerns have hardly been addressed in prior studies in Western contexts. For example, the individual advertising on GSNAs was identified as a primary social privacy concern by Chinese users because of the emergence and prevalence of “WeChat Business” in Chinese society (Na, 2018). Similarly, the prominent concern of institutional privacy regarding surveillance of user information by apps and the Chinese government is also associated with the unique Chinese context, particularly the Chinese Internet censorship policy (Liao, 2019). However, this study also has some limitations. First, this study only interviewed 47 participants, which is a relatively small sample and thus limits the kind of results (e.g., gender and age differences in privacy concerns) to be generalized. Second, as this study primarily focuses on exploring users’ privacy concerns and their strategies, the results are restricted to user perspectives. It has not provided knowledge about how these privacy problems could be addressed from other perspectives, such as the app developers and the Chinese government. Given that privacy issues have become increasingly significant with the rapid growth of GSNAs, future studies are encouraged to delve into possible solutions and strategies to mitigate users’ privacy concerns in the global context of social media.

As an attempt to partly remedy the second limitation, combined with the strategies that participants have revealed in this research, this study tries to provide some suggestions regarding how users’ privacy concerns could be addressed in the context of social media, mainly from the perspectives of users. For example, before deciding to download an app, users are encouraged to spend some time examining and evaluating the information relevant to the app, such as users’ comments in app stores and online forums, news reports about privacy and safety problems, and privacy policies/guidelines on the app’s official website. While installing an app, users could take advantage of the permission system of their smartphones to meticulously decide which permissions to give to the app’s capabilities in collecting and transmitting user data (e.g., access to location and photo taking) (Do et al., 2014). When registering their information on the app, users are encouraged to read the terms of use which often include how the app protects users’ privacy and how users could protect their own privacy (e.g., reporting privacy violations by other users to administrators) if they encounter any problems while using the app. The targeted methods to tackle specific privacy risks need to be developed according to different apps’ functions and features, but several general strategies to deal with users’ privacy concerns are proposed here. First, users should be careful with the use of the location functions on their phones to prevent location tracking by other users and app platforms. Location is best enabled only when users need it. After finishing the use of location services, users should close them to prevent their location information being continuously tracked. In addition, anti-tracking apps such as AVG PrivacyFix and Xprivacy could be installed on users’ phones to block mobile tracking (Karanja et al., 2018). Second, to mitigate the risk of information leakage, users should be careful about exposing their real personal information (e.g., names, date of birth, age) and financial information (e.g., bank accounts, card numbers, and passwords) while engaging in activities on the app. Instead, it is better to use unidentifiable information (Hoang et al., 2016). Third, instead of ignoring or accepting the privacy risks like most participants reported in this study, users are suggested to take action when encountering privacy issues. For example, reporting inappropriate behavior (e.g., sexual harassment, malicious comments) to the app platform is a positive strategy not only of protecting users’ privacy but also of helping the app platform improve their management and establish a safer and healthier user environment. Apart from users, other parties such as app developers and governments should also take steps to protect users’ privacy. For example, app developers should be aware of the privacy risks and users’ privacy concerns, and thus make efforts to update and improve their technical systems (e.g., detecting and restoring technical vulnerabilities) and management policies (e.g., collecting, storing, and analyzing user data legally and properly). Governments should also play a role in making laws and policies to supervise and regulate app developers’ behavior and protect users’ privacy. In this way, the privacy risks of GSNAs and users’ concerns regarding using these apps could be mitigated through the efforts of different parties.

Declaration of Conflicting Interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) received no financial support for the research, authorship, and/or publication of this article.
Gibbs, J. L., Ellison, N. B., & Lai, C.-H. (2010). First comes love, then comes Google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research, 37*, 70–100.

Griffin, M., Canavello, A., & McAnulty, R. D. (2018). Motives and concerns associated with geosocial networking app usage: An exploratory study among heterosexual college students in the United States. *Cyberspsychology, Behavior, and Social Networking, 21*(4), 268–275.

Guo, M. (2018, November 7). 2018 Kantar report of the influence of Chinese social media. *Kantar China Insights*. https://cn.kantar.com/%E5%AA%92%E4%BD%93%E5%8A%A8%E6%80%81/%E7%A4%BE%E4%BA%A42018/2018%E5%B9%B4%E5%87%AF%E5%BA%6E%E4%B8%AD%E5%9B%BD%E7%A4%BE%E4%BA%A4%E5%AA%92%E4%BD%93%E5%BD%B1%E5%93%8D%E6%8A%A5%E5%91%8A/

Hoang, N. P., Asano, Y., & Yoshikawa, M. (2016, January 31–February 3). Your neighbors are my spies: Location and other privacy concerns in dating apps [Conference session]. The 18th IEEE International Conference on Advanced Communication Technology (ICACT 2016), PyeongChang, Korea.

Huang, Z., & Soo, Z. (2019, March 5). Data leak exposes 364 million Chinese social media profiles tracked by police surveillance programme, security researcher says. *South China Morning Post*. https://www.scmp.com/tech/enterprises/article/2188662/data-leak-exposes-364-million-chinese-social-media-profiles-tracked

Jedrzejczyk, L., Price, B. A., Bandara, A. K., & Nuseibeh, B. (2010). On the impact of real-time feedback on users’ behaviour in mobile location-sharing applications. In L. F. Cranor (Ed.), *Proceedings of the Sixth Symposium on Usable Privacy and Security* (pp. 1–12). New York, NY: Association for Computing Machinery.

Junco, R., Heiberger, G., & Loken, E. (2011). The effect of Twitter on college student engagement and grades. *Journal of Computer Assisted Learning, 27*, 119–132.

Karanja, A., Engels, D. W., Zerouali, G., & Francisco, A. (2018). Unintended consequences of location information: Privacy implications of location information used in advertising and social media. *SMU Data Science Review, 1*(3), 1–22.

Lankton, N. K., McKnight, D. H., & Tripp, J. F. (2017). Facebook privacy management strategies: A cluster analysis of user privacy behaviors. *Computers in Human Behavior, 76*, 149–163.

Lee, E. (2018, December 3). Updated: Thirty million users of Chinese dating app Momo reportedly had their data exposed. Technode. https://technode.com/2018/12/03/momo-data-leakage/

Lenhart, A., & Madden, M. (2007). Teens, privacy & online social networks: How teens manage their online identities and personal information in the age of MySpace. Pew Internet & American Life Project.

Li, H., Zhu, H., Du, S., Liang, X., & Shen, X. (2018). Privacy leakage of location sharing in mobile social networks: Attacks and defense. *IEEE Transactions on Dependable and Secure Computing, 15*(4), 646–660.

Li, M., Zhu, H., Gao, Z., Chen, S., Yu, L., Hu, S., & Ren, K. (2014). All your location are belong to us: Breaking mobile social networks for automated user location tracking. In J. Wu & X. Cheng (Eds.), *Proceedings of the Fifteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc ’14)* (pp. 1526–1528). New York, NY: Association for Computing Machinery.
Liao, S. (2019, March 4). Over 300 million Chinese private messages were left exposed online. The Verge. https://www.theverge.com/2019/3/4/18250474/chinese-messages-millions-wechat-qq-yy-data-breach-police

Lutz, C., & Ranzini, G. (2017). Where dating meets data: Investigating social and institutional privacy concerns on Tinder. Social Media + Society, 3(1), 1–12.

Luzio, A. D., Mei, A., & Stefa, J. (2018). Uncovering hidden social relationships through location-based services: The Happn case study [Conference paper]. In INFOCOM 2018—IEEE Conference on Computer Communications Workshops, Honolulu, HI, USA, 15–19 April 2018.

Ma, X., Sun, E., & Naaman, M. (2017). What happens in Happn: The warranting powers of location history in online dating. In C. P. Lee & S. Poltrock (Eds.), Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (pp. 41–50). New York, NY: Association for Computing Machinery.

Madden, M., Lenhart, A., Cortesi, S., & Gasser, U. (2013, August 22). Teens and mobile apps privacy. Pew Research Center. http://www.pewinternet.org/2013/08/22/teensand-mobile-apps-privacy/

Masur, P. K., & Scharkow, M. (2016). Disclosure management on social network sites: Individual Privacy perceptions and user-directed privacy strategies. Social Media + Society, 2(1), 1–13.

Mihailidis, P. (2014). The civic-social media disconnect: Exploring Ideological as well as technical aspects of social media. Information, Communication & Society, 17, 1059–1071.

Momo. (2018, May 29). The revenue of 2018 Q1 is 27.6 billion RMB and the pure profit is 9 billion RMB of Momo. Momo. https://www.immomo.com/newroom/14832.html

Na, N. (2018, June 19). How to use WeChat for business: Interact with your audience. SAP. https://blogs.sap.com/2018/06/19/how-to-use-wechat-for-business-interactive-with-your-audience/

Neuts, D. E. (2016, June 7). Tinder hopes to double paid members to 2 million by year end. Subscription Insider. https://www.subscriptioninsider.com/news/tinder-hopes-to-double-paid-members-to-2m-by-year-end-4999-1.html

Peng, J., Meng, Y., Xue, M., Hei, X., & Ross, K. W. (2015). Attacks and defenses in location-based social networks: A heuristic number theory approach [Conference paper]. In The 2015 International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec), Hangzhou, China, 16–18 November 2015.

Peng, L., & Ye, D. (2019, January 10). 450 billion WeChat messages have been sent everyday. South Daily. http://tc.people.com.cn/n1/2019/0110/c183008-30513620.html

Polakis, I., Argyros, G., Petsios, T., Sivakorn, S., & Keromytis, A. D. (2015). Where’s Wally? Precise user discovery attacks in location proximity services. In I. Ray (Ed.), Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security Denver (CCS 2015) (pp. 817–828). New York, NY: Association for Computing Machinery.

Quinn, K., & Epstein, D. (2018). #MyPrivacy: How users think about social media privacy [Conference paper]. In The 9th International Conference on Social Media and Society (SMSociety ‘18), Copenhagen, Denmark, 18–20 July 2018.

Rainie, L. (2016, September 21). The state of privacy in post-Snowden America. Pew Research Center. https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. First Monday, 15(1). https://firstmonday.org/ojs/index.php/fm/article/view/2775/2432.

Sarikakis, K., & Winter, L. (2017). Social media users’ legal consciousness about privacy. Social Media + Society, 3(1), 1–14.

Schrock, A. R. (2015). Communicative affordances of mobile media: Portability, availability, locatability, and multimedia. International Journal of Communication Systems, 9, 18.

Shklovski, I., Mainwaring, S. D., Skuladottir, H. H., & Borghorsson, H. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In M. Jones & P. Palanque (Eds.), Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2014) (pp. 2347–2356). New York, NY: Association for Computing Machinery.

Smith, A. (2016, February 11). 15% of Americans have used online dating sites or mobile dating apps. Pew Research Center. https://www.pewinternet.org/2016/02/11/15-percent-of-american-olds-have-used-online-dating-sites-or-mobile-dating-apps/

Smith, A., & Anderson, M. (2016, February 29). Five facts about online dating. Pew Research Center. https://www.pewresearch.org/fact-tank/2016/02/29/5-facts-about-online-dating/

TalkingData. (2016). The 2016 investigation report of Chinese university students’ mobile life. Talking Data. http://mi.talkingdata.com/report-detail.html?id=314

Vishwanath, A., Xu, W., & Ngoh, Z. (2018). How people protect their privacy on Facebook: A cost-benefit view. Journal of the Association for Information Science and Technology, 69(5), 700–709.

Wang, R., Xue, M., Liu, K., & Qian, H. (2015). Data-driven privacy analytics: A WeChat case study in location-based social networks. In K. Xu & H. Zhu (Eds.), Wireless algorithms, systems, and applications (pp. 561–570). Springer.

Wang, X., & Gu, B. (2016). The communication design of WeChat: Ideological as well as technical aspects of social media. Communication Design Quarterly Review, 4, 23–35.

Yang, K. C. C., Pulido, A., & Kang, Y. (2016). Exploring the relationship between privacy concerns and social media use among college students: A communication privacy management perspective. Intercultural Communication Studies, 25(2), 46–62.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. Information, Communication & Society, 16(4), 479–500.

Zickuhr, K. (2010). Generation 2010. Pew Internet & American Life Project.

Zurburggen, E. L., Ben Hagai, E., & Leon, G. (2016). Negotiating privacy and intimacy on social media: Review and recommendations. Translational Issues in Psychological Science, 2(3), 248–260.

Author Biography

HaLi Li (MA, University of Chinese Academy of Sciences) is a PhD candidate at Digital Media Research Centre (DMRC), School of Communication, Queensland University of Technology. Her research interests include social media, digital intimacy, and diaspora.