Ethics and Information Technology (2018) 20:279–289
https://doi.org/10.1007/s10676-018-9480-6

ORIGINAL PAPER

Privacy perception and protection on Chinese social media: a case study of WeChat

Zhen Troy Chen[1] · Ming Cheung[2]

Published online: 5 September 2018

Abstract

In this study, the under-examined area of privacy perception and protection on Chinese social media is investigated. The prevalence of digital technology shapes the social, political and cultural aspects of the lives of urban young adults. The influential Chinese social media platform WeChat is taken as a case study, and the ease of connection, communication and transaction combined with issues of commercialisation and surveillance are discussed in the framework of the privacy paradox. Protective behaviour and tactics are examined through different perceptions of privacy in the digital age. The findings of this study suggest that users possess certain amount of freedoms on WeChat. However, users' individual privacy attitudes and behaviour in practice suggest they have a declined sense of their own freedom and right to privacy. A privacy paradox exists when users, while holding a high level of concerns, in reality do little to further the protection of their personal information on WeChat. We argue that once a user has ingrained part of their social engagement within the WeChat system, the incentive for them to remain a part of the system outweighs their requirement to secure their privacy online as their decision-making is largely based on a simple cost-benefit analysis. The power and social capital yielded via WeChat is too valuable to give up as WeChat is widely used not only for private conversations, but also for study or work-related purposes. It further blurs the boundaries between the public, the professional and the private, which is a rather unique case compared with other social media around the world.

Keywords Privacy paradox · Privacy protection · Social media · WeChat · Young adults · China

Digital technology has changed the lives of people in China profoundly in recent years, particularly with the Internet + initiative put forward by the government. Social media platforms such as WeChat and e-commerce mobile apps such as Taobao coordinate and mediate the social, economic and political aspects of users' everyday life with increasing quality and quantity (Kokolakis 2017). The boundaries of the public, the professional and the private have become blurred, which raises questions concerning the Internet privacy protection of users, who can be easily identified through the very technology that makes the exchanges of information possible (Walsh and Baker 2017). Users are threatened by an expanding surveillance society, where their private information and practices are traced and recorded cumulatively and often out of context (Fulton and Kibby 2017). The phenomenon of the privacy paradox has been well-documented in the literature, and it indicates how people can be extremely concerned about online privacy while disclosing their personal information for relatively small rewards and doing little to protect themselves or adjust their privacy behaviour (Büchi et al. 2017; Lee et al. 2013; Young and Quan-Haase 2013; Zarouali et al. 2017). The debate concerning privacy threat has received considerable attention in the West but has not been thoroughly discussed in China, as no stand-alone privacy law has yet been developed and social media platforms have only relatively recently gained popularity. The aim of this study is to examine the nature of the privacy threat posed by digital technology and to further contribute to the debate on privacy protection using the case of WeChat, the most popular social media platform in China. Based on in-depth interviews together with WeChat profile analyses of

✉ Ming Cheung
m.cheung@griffith.edu.au; drmingcheung@gmail.com

Zhen Troy Chen
zhen.chen@xjtlu.edu.cn

[1] Xi′an Jiaotong-Liverpool University, Suzhou, China and University of Nottingham-Ningbo, Ningbo, China

[2] Griffith University, Brisbane, Australia

40 urban young Chinese adult users, we investigate their perceptions of online privacy along with the concerns and tactics they use to protect their privacy.

In this article, we first discuss the development of the relevant philosophical, legal and technological concepts with regards to privacy in China. We also review the terms, concepts and protective measures concerning social media privacy. In particular, we propose a dialectic approach to study the complex issues regarding privacy perceptions and protective tactics under a privacy paradox framework. We then focus on presenting a case study of WeChat, where users' private data might be collected by the platform operator for retargeted marketing, services and other purposes.

Privacy in China

The modern concept of privacy, exemplified in various national and international laws, can be understood as the right to be left alone, free from unwanted intrusion (Westin 1967 as cited in Zarouali et al. 2017). It normally comprises territorial privacy (physical space), personal privacy, and informational privacy. The focus of this study is primarily on informational privacy on social media. In China, people may often be asked about their hometown, salary, age, and marital status by those they have just met in professional settings or even by strangers. Some argue that *guanxi* (connections and networks) in Chinese society is built on close acquaintances (*shuren shehui*, in Fei 1992, pp. 47–48) and was established long before the networked society came into being. Chinese culture thus is somewhat vague and ambiguous in terms of the boundaries of the public and private spheres (Du 2015; Fei 1992). However, the development of networks with the advancement of Internet technology has intensified concerns about privacy. Privacy issue is gradually transforming from the cultural sphere to the commercial and legal sphere, as modern technologies increasingly pose a threat to privacy in China, resulting in financial crimes, telephone and email spam, online trolling, etc. Yet the Chinese legal system as part of the codified institutions is insufficiently developed in terms of privacy protection and struggles to deal with these new challenges. The term 'privacy right' was not used in Chinese law until 1992, when the Law on the Protection of Women's Rights and Interests was introduced, and it is still not a stand-alone right recognised by Chinese civil or tort law. It is protected in principle by the Constitution, the 1982 General Principles of the Civil Law and a number of departmental laws under the rights of personality and reputation. On the other hand, the awareness of privacy rights is increasing in the social media age, partially due to the construction and coordination through mass media and online platforms such as WeChat. The platforms require users to agree to terms and conditions that include privacy policies when signing up.

As mentioned, it is traditionally acceptable in China to enquire about personal and private information such as age and salary due to the benefits of exchanging such information. For example, age can indicate seniority, which can in turn earn respect, and salary can be used as a signal to indicate capability and social status. Studies taking a uses and gratifications perspective have well addressed this (see for example, Fulton and Kibby 2017; Raacke and Bonds-Raacke 2008). Yet these traditional practices are gradually changing. The distinct structural functions and effects of different social media can satisfy the diverse motivations of their users (Jeong and Kim 2017). Similar to Facebook and Twitter, WeChat in China works as a juxtaposition of traditional and new social media, enabling users to create individual accounts and personal profiles and to share selected information (text, images, and videos) with friends and connections. It is a combination of an instant messaging tool and a personal blog, both of which support multimedia contents. Social media affordances or functionality have been identified through investigations of college student users on Facebook, Instagram, and Twitter. These include: communication, convenience, curiosity/information seeking, popularity, and building and maintaining relationships, in addition to commerce (Al-Kandari et al. 2016; Jeong and Coyle 2014; Yang et al. 2014). Among these positive benefits, the function of communication serves as a key criterion for privacy calculus (Jeong and Kim 2017). The functionalist view tends to argue that social media users weigh affordances over privacy concerns. However, privacy as a basic human right is necessary to maintain certain standards in people's interactions and relationships to keep aspects of their lives free from intrusion (Rachels 1975). This is achieved through the careful management of personal boundaries that determine levels of privacy in relation to others (Zlatolas et al. 2015).

Privacy on social media

Rachels (1975) identified two key concepts of privacy: accessibility and control. Accessibility is the ease of access by others to individual personal information, whereas control is the ability to set and maintain boundaries for such information and is a mechanism for deciding to whom and to what extent it is accessible. These concepts are important for individuals to maintain relationships with others. In terms of social media privacy, visibility is another important concept widely discussed (see for example, Fox and Moreland 2015). It refers to the reception of information, including profiles, posts, and other personal information (the result of access control). Typically, there is a positive association between privacy control and visibility, but this is not always the case with social media. Some platforms such as Facebook and Twitter allow users to view the personal information of others without direct access, as some of the information is made publicly accessible by default without the knowledge of the users. One consequence is that even with strict self-control, unwanted privacy breaches could still be possible. This raises concerns to users who may regret certain posts and activities when they later realise the potential loopholes (Dhir et al. 2016).

The openness and interactive nature of social media have led to privacy concerns among users, primarily over social privacy and institutional privacy (Hodkinson 2017; Young and Quan-Haase 2013). The data posted by users could be monitored, collected and used by corporations (advertisers and marketers) to retarget them for commercial purposes. Surveillance from the government and other public institutions as well as from individuals could also be a concern to users. Based on a study of privacy concerns on Facebook, Debatin et al. (2009) found that some users are afraid of reputation damage caused by gossips and rumours. Other concerns include unwanted contacts, stalking, hacking, trolling, and identity theft, in addition to third-party access and utilisation of personal data. Studies of social media such as Facebook, LinkedIn, Myspace, and Twitter have found an interesting privacy dilemma or paradox. While users show a clear and strong desire to keep their personal information private, they are at the same time expecting exposure, affirmation, and admiration from their followers (Büchi et al. 2017; Kokolakis 2017; Zarouali et al. 2017).

Jeong and Kim (2017) identified the type and content of postings (particularly the sensitivity of content) and audiences (external and internal) as factors influencing users' attitudes towards privacy on social media. These involve trust and risks (Norberg et al. 2007), as identified in a comparative study of user activities on Facebook and Twitter. The findings echo Kokolakis' (2017) comprehensive review of the recent literature on privacy attitudes and behaviour on social media. Despite the often self-reported concerns over privacy on social media, users were found to remain largely positive towards using them. This situation has been described as an accepted norm by several scholars (see for example, Hodkinson 2017; Spottswood and Hancock 2017; Young and Quan-Haase 2013).

However, this does not mean that no action is taken by social media users; rather, it demonstrates that the intentions and attitudes towards privacy concerns do not necessarily lead to strict protective behaviour. Research on various social media in the West suggests that numerous measures and strategies are used to balance the privacy control and visibility of users' personal information. According to the communication privacy management theory (Dhir et al. 2016; Spottswood and Hancock 2017), information withheld and disclosed is influenced by the intimacy of relationships (e.g., family, friends, colleagues, and acquaintances), accessibility (likelihood of individual or public access), post-control over published content, trust in and reliability of the platform, and psychological pressure.

In addition, the concept of voluntarism further complicates the paradox; this refers to the willingness and desire to disclose private information on social media regardless of the often predicted negative consequences (Jeong and Kim 2017). This is particularly evident with young college students, who are more active in terms of online self-expression and identity representation. Debatin et al. (2009) found that even though measures were taken (privacy setting and falsification of personal information) to protect privacy, young college students were generally less concerned about corporate and marketing efforts on the commercialisation of personal information. Extreme cases have been identified, in which users were willing to jeopardise their rights to privacy due to the fear of being forgotten, ignored or missed out (Fox and Moreland 2015). Research in that direction tends to shift away from privacy concerns to instead focus on pleasure and satisfaction.

In summary, the acceptance of the 'norm' under the privacy paradox involves various factors. The efficacy of various protective measures is affected by digital literacy (Internet and technical skills), privacy literacy (both technical and legal), and the correlations between privacy protective behaviour on the one hand and technical familiarity, awareness of surveillance techniques, and privacy policy knowledge on the other (Bartsch and Dienlin 2016). The theories examining privacy paradox on social media are discussed in the following section.

The privacy paradox

Kokolakis (2017) provided a comprehensive review of the privacy paradox phenomenon based on 51 recently published papers. He suggested that privacy should be understood from different aspects, including territorial privacy (physical space), personal privacy, and informational privacy. The focus of this current study is on informational privacy on social media. The privacy paradox denotes the inconsistency or divergence between privacy concerns/attitudes and privacy protective behaviour. The former refers to more generic attitudes and the latter to more context-specific behaviour (Morando et al. 2014). Privacy concerns and behaviour have been studied in various contexts, including social and transactional situations (e.g., e-commerce) (Bae et al. 2016). Kokolakis (2017) identified interpretations from five research areas: privacy calculus theory (uses and gratifications approach); social theory; psychology (cognitive bias and heuristics in decision-making); behavioural economics (bounded rationality, incomplete and asymmetric information); and quantum theory (indeterminacy). These theoretical frameworks all have merit in explaining the privacy paradox phenomenon. However, we draw on the privacy calculus approach to offer a nuaced case study on privacy paradox in a Chinese context. Social media as a technology is a relatively new phenomenon in China, and users tend to decide whether to use a given social media primarily according to its affordances. Therefore, what we are trying to argue is that the adaptation of social media as a technology first starts as an economic and pragmatic calculus process. Users test, learn and socialise on social media primarily based on the funtionality and affordances of the available platforms. Privacy becomes a concern at a later stage when a platform has garnered significant network effect. In addition, we regard social media as symbolic spaces in which actors such as users, platforms, and institutions can engage with each other. The privacy paradox consists of a dialectic that cannot be dissolved or eliminated; rather, the two oppositional aspects co-exist without contradictions. That is, disclosing information is necessary for building up and maintaining relationships (Al-Kandari et al. 2016; Jeong and Kim 2017) and gaining social capital (Fulton and Kibby 2017). However, this must be coordinated and negociated within constantly shifting boundaries that serve the needs of users in specfic contexts (Hodkinson 2017; Walsh and Baker 2017).

Research questions

This study aims to identify and investigate the privacy paradox among users of WeChat, the most popular social media platform in China. In particular, we are interested in how users perceive and behave towards privacy in their everyday use of the platform. As examinations on privacy protective measures and tactics in China are scarce, we aim to address the following questions:

> **RQ1** Do the users express different levels of concern for privacy in terms of self-disclosure activities on WeChat?
> **RQ2** Within the privacy paradox, how do the users behave taking into consideration their concerns on WeChat?
> **RQ3** What strategies and tactics do the users use to protect their privacy on WeChat?

Methodology

To answer the research questions, we used semi-structured interviews as our primary research method. Compared with questionnaire and survey, which largely rely on self-reported data, this qualitative method is good at answering not only 'what' but also 'how and why' type of questions. We recruited 40 young Chinese adults in Shanghai, Guangzhou, Dalian, and Ningbo, including undergraduate and postgraduate students. They are aged between 20 and 30, with a balance in genders. We used snowballing as a method to approach informants and stopped interviewing more as the data we collected had started to reach stratification. The informants formed a representative sample of 'typical users' of WeChat—urban young adults and mostly from Tier 1 and Tier 2 cities of China (Smith 2018). During the interviews, we also observed and analysed the informants' WeChat Moments (profile and posts of each informant) with their consent to validate their strategies and tactics in protecting privacy on the social media platform. In-depth interviewing is an effective method for finding out what is happening in this new social media era given that there is limited research into privacy protection in the Chinese context. Profile and posts analysis is also a good complementary method, as it reveals more first-hand and reliable data and insights than a self-reported survey. This combined approach is intended to generate richer substance and details than the rigid and limited answers obtained through surveys.

The interviews were conducted according to a list of questions derived from the literature review and put in three sections: WeChat affordances, privacy perception and concerns, and privacy protection behaviour on WeChat. For section one, we asked why the informants use WeChat and what affordances and services they use with a focus on personal and private information exposure. These include how they get connected, communicate and engage with individuals or in groups. For section two, we asked about their awareness of privacy terms and conditions as well as their general privacy concerns on WeChat. Questions ranged from privacy breach incidents to their evaluation on privacy exposure in exchange of benefits. For section three, we asked how they protect their privacy on WeChat, with regard to their behaviour and tactics.

WeChat: a case study

A number of common themes around the privacy paradox phenomenon have emerged from our interviews. However, before going into details about the themes, we would briefly introduce WeChat, a very popular social media platform established by China's Internet giant, Tencent. Unlike Weibo (the Chinese equivalent of Twitter) which is a microblogging and broadcasting service where all profiles and posts are publicly accessible unless users self-amend certain privacy settings, WeChat adopts a different approach in attracting users, which is narrow-casting oriented. It was created as an enhanced version of the instant messaging desktop-based software QQ (similar to ICQ and MSN), to attract new users on mobile Internet. Unlike Weibo, which adopted a key opinion leader strategy by inviting celebrities and public intellectuals to be their first cohort of users, WeChat allow users who are already friends offline to send instant texts and voice messages to each other. With a series of updates, it now supports video conferencing (similar to FaceTime) as well as WeChat Moments (literally 'friends circle' in Chinese) that enables the posting of text, pictures, and short videos. WeChat has now penetrated into almost every aspect of users' daily and professional life in China (Fulco 2017). Clover (2017) provides a vivid summary of WeChat,

> It is hard to overstate the pervasiveness of WeChat in Chinese life – the app is a phone, messenger, video conference, e-commerce platform and gaming console, not to mention noodle delivery service… Many a new relationship is sealed with the ritual smartphone 'scan' of one anothers' WeChat QR code.

Increasing privacy concerns with connection expansion

Based on the data we collected, the privacy concerns revealed by the informants were categorised into a few themes. The first identified theme covers social, organisational, institutional and technological concerns. Other contributing factors are investigated as these privacy concerns evolve over time. We illustrate the significant points shared among the informants through representative quotations derived from the interviews. Some of the informants reported that they left their WeChat Moments unguarded, that is, made them completely accessible to anyone who is a friend. Those expressing little concern tended to trust connections developed from their real-life friendships. Connections on WeChat are initially based on established relationships offline, but these expand over time. There appears to be a consensus among users that they at first did not realise their privacy exposure on WeChat, as their established circle of friends was familiar and trustworthy. As their social connections expanded from their core relationships (e.g., family and close friends) and functional relationships (e.g., classmates and colleagues) to casual relationships (e.g., acquaintances and those met through occasional, social and professional settings), increasing concern about privacy emerged. This is a dynamic process. The following statement from a female informant is not uncommon among other informants:

> I tend to trust my WeChat friends as I have already known most of them when we first got connected. They could see most of my posts from the very beginning. However, as the time I spent on WeChat increases, my personal information will nonetheless be revealed. Now it is a concern for me because I have around 500 connections, and a lot of them are people I barely talk to. (Personal communication, informant 8, 2017)

For the clarify of analysis, we will now discuss the social, organisational, institutional and technological concerns one by one. Even though these concerns can overlap with each other and often work in flux, the differences are categorised based on how informants viewed them from different angles.

Social concerns

Social concerns relate to general social life and include text messages and posts regarding major life events, personal information, and mundane day-to-day occurrences that reveal social cues, digital and real-life footprints. Cases reported by informants include but are not limited to online threats, identity theft, online trolling, and malicious attacks. Some revealed concerns in terms of their professional lives. Informants generally distinguished between their personal and professional lives, although with a lesser concern on the latter as most were university students and had not yet embarked on professional careers. The interviews also showed that 'professional life' was understood and interpreted rather broadly. The students drew more or less clear lines between themselves and the university, internship providers, and employers. They were concerned about connections in the organisations they worked for or belonged to, for example, their teachers, managers, and colleagues. Some informants had issues when the organisation was part of their social cues if it used WeChat as a work-facilitating tool. They saw it as an invasion of their privacy and personal lives. One informant said:

> I really have issues with colleagues and team leads who use WeChat for work. We are dragged into a group, and the work is updated constantly. It's like having someone watch over your shoulder. The worst scenario would be notices sent to the group outside of work hours or during weekends. I tend to block certain posts from my colleagues, especially those from my team lead. (Personal communication, informant 22, 2017)

This reveals a mixture of privacy concerns in terms of personal space (though virtual) and information. The blocking tactic utilised is a counter-action against such invasion and is further investigated in the section on protective behaviour.

Organisational concerns

Organisations may collect, store and exploit the data of social media users. The ownership and power of the big data generated by users over WeChat as a social network is a cause for concern, as it can come with the potential of abusing such power. Two levels of concern are identified in our interviews: towards the platform itself and towards the government. While the platform works within a relatively independent commercial environment, it is subject to governmental supervision through legal and administrative mechanisms, particularly evident in China. One informant provided a vivid example of how users coordinate their daily lives through WeChat and how powerful the platform can be:

> When I get up in the morning, I will routinely check WeChat Moments. At the student canteen, I will pay for my breakfast with WeChat wallet. I will probably ask my classmates where the lecture will take place, and we will discuss the schedule of the lecture on WeChat on my way to the classroom. We even have WeChat groups set up for group discussion in class. At lunchtime, we may order take-away through WeChat or share real-time locations with friends if we decide to eat out. And we may post food pictures and selfies while we have dinner together. All of these are communicated through WeChat. I am not sure if our conversations on WeChat are stored or monitored. But I know that articles posted by public WeChat accounts (*gongzhong hao*) get censored and sometimes taken down by Tencent and/or the authorities. (Personal communication, informant 36, 2017)

This concern is not mere speculation, as algorithm-based technology has enabled WeChat to post retargeted advertisements to users for commercial gain. This was well documented in the report compiled by *Tengyun* (Tencent Cloud), a research institute of Tencent based at its Beijing office. Cases of digital games, animation, TV drama, and films are reported to have used user-generated data (Tengyun 2017).

Institutional concerns

WeChat as a social network has developed into a multifunctional platform, which is a convergence of the social, the political, and the transactional. The data obtained and stored have been a concern for many users. Data generated in real life are not easily captured, stored or taken advantage of (it will be eventually forgotten), while online data can be. Online data penetrate into nearly every aspect of a user's life, probably in ways that the user does not even notice. Institutional concerns are closely related to the control and access of power, which could be problematic if not managed properly. Governments worldwide have tightened Internet governance over the years through codified or institutionalised laws and regulations within the legal and judicial systems. Legitimate yet debatable reasons are Internet security and anti-terrorism. WikiLeaks and the Snowden incident have been well documented and analysed in the literature. Alerting the general public to crime and getting it controlled before disastrous attacks occur can be beneficial to society as a whole. However, much of the information about what people think and like is not meant to be controlled or used against the general public. It is a balance hard to strike. Yet, despite overwhelming concerns about (potential) government surveillance, some informants said that they were fine with it. As one informant stated, 'I am not that important to be watched over. I have done nothing wrong to be singled out' (Personal communication, informant 1, 2017). The dystopian view of profit-seeking corporations and a totalitarian government was a lesser concern for some informants, and they were generally positive about the convenience and benefits brought by the technology. This is where opinions diverge, which is further discussed below.

Technological concerns

Technological concerns are closely linked to moral panic reported by informants who had doubts about the ever-advancing digital technologies. Informants with these concerns generally believed that tighter controls should be exercised on the platforms. They recognised the benefits of such technologies, but a fear over privacy loss sometimes prevailed, as immersion in the digital and virtual world could have left too many unnecessary footprints on such platforms. One informant contended that a balance must be achieved when using such platforms:

> I have concerns about posting too much information on WeChat. I think the regulations should be tightened. The platforms are like power. They should be shut in cages. If not, I will do my part. I hardly post anything (on WeChat) nowadays. If you have a concern, just don't do it. (Personal communication, informant 33, 2017)

We first thought that this was simply an overreaction to privacy invasion on social media. However, we later found that some other informants expressed similar views and used the withdrawal strategy to protect their online privacy. WeChat has developed as a platform where users' real identities can be traced to an individual registered with a mobile phone number, which in China is linked to a national ID. The anonymity of the Internet has been undermined if compared to the Internet forum/BBS era, when the older generation had little concern about privacy, as personal information was generally not required to surf the Internet.

Evident privacy paradox: calculus and dispositions

The second theme is developed around the notion of the privacy paradox, contributed by several factors. Our interviews confirm that the privacy paradox exists in Chinese social media. Two distinct and interrelated concepts about privacy paradox, namely privacy calculus and privacy dispositions, are worth some explanation. Both concepts have been regarded as heuristic and psychological processes, where individuals struggle to process overloaded information with limited cognitive resources in evaluating a privacy calculus. Therefore, users tend to be less careful in evaluating such information and become vulnerable in the face of heuristic and cognitive bias (Choi et al. 2015). This has consequences when users conduct a privacy calculus. They may use mental shortcuts to bypass the heuristic and cognitive challenges. Privacy calculus refers to a pure economic analysis of the benefits (e.g., gaining social capital and resources) and risks of privacy exposure on social media. In contrast, privacy disposition refers to users' overall concerns about opportunistic behaviour against privacy exposure online (Smith et al. 1996) which involves psychological shortcuts and depends on people's propensities. Therefore, it has a moderating effect on privacy calculus. Those who have high dispositional privacy concerns tend to be sensitive and protective of their privacy. On the other hand, those with low dispositional privacy concerns are less sensitive about privacy exposure.

In the information systems literature, calculus theory is largely accepted as a rational evaluation process based on the cost-benefit analysis of privacy exposure (Kokolakis 2017). The interviews suggest that many informants allowed some level of privacy exposure so that people could know and remember them and from which they could gain social respect and affirm other types of social capital. However, we do find different levels of privacy concerns depending on privacy dispositions. The dynamic and ambiguous management process of privacy exposure also involves trust fostered through the reciprocal information exchange on social media over time.

Network mutuality and reciprocity

The concepts discussed above indicate that people are rational (although bounded or with limitations) when making decisions about whether to allow a connection to review their posts and personal information on WeChat. However, it is difficult to know whether users are rational and consistent with their self-affirmed principles. Network mutuality and reciprocity play a role in assessing privacy risks between connections on WeChat and concisely represent commonality and similarity in a social relationship. According to McPherson et al. (2001), this fosters a similarity effect indicating that network mutuality has a positive association with liking and is a perceptual bias creating a cohesion force. That is, a high degree of network mutuality leads to high network cohesion, which maintains socially rewarding relationships. Walther et al. (2008) identified that a highly comprehensive profile contributes to network mutuality, which is perceived by users as socially rewarding. One informant confirmed how network mutuality assuaged her concerns over privacy when talking about her intimate and private WeChat usage:

> My sister and I have nothing that cannot be talked about on WeChat. We became close in high school and now are at different universities. We use WeChat to talk to each other regularly. We share our secrets on WeChat, and we do video chats as well. She would not block any posts from me because she trusts me. I would not treat (trust) others like I do to her. (Personal communication, informant 19, 2017)

Mutuality and reciprocity do not necessarily lead to privacy exposure. Some informants suggested that even though some of their connections were very open about their privacy with easy accessibility and diagnosticity, they would not do the same in return. This indeed reflects a careful calculus process, in which privacy risks can have more weight than social capital gains. However, the cost-benefit calculus is sometimes dominated by economic interests. For example, the popularity of live-broadcasting apps has made it a lucrative business with immense privacy exposure. The business model of these platforms and services is primarily based on the commercialisation of privacy, and some scholars have been positive about how such platforms celebrate the enabling nature of the return to self-expression and representation (Li 2016). Whether this opens a potential new public sphere or is further captured by exploitive capitalism is still debatable (Rubinstein 2013), but the blurring of the private and the public is evident and it poses increasing privacy concerns.

Trust within the established and expanding 'friends circle'

The privacy setting depends on the boundary evaluated by the user. It consists of both calculation and ambiguous and blurry impression on a person's friendship. However, relational framing theory has suggested that the accessibility and diagnosticity of a user's profile can be used to assess and foster trust between two communicators (McLaren et al. 2014). Yet, there may not be a clear-cut distinction between rational calculation and general impression as it relies on the changing dynamics within a mutual and reciprocal relationship which could keep changing over time.

For example, we found that most of the informants categorised their friends into different groups. According to Fisk and Neuberg (1990), immediately available category-based information and attribute-based information play an important role in shaping how impression of a friend is formed, maintained and changed. Category-based information may include age, race, appearance, profession, and beliefs. Once such a mechanism is activated, the impression tends to be stereotypical and stable. Impressions may change over time because of attribute-based information (sometimes category-based information is limited or not available), which needs careful observation and analysis. It is a mutual process that partly explains why our informants must expose selected private information for people to get to know them. Attribute-based information can include interests, political views, and social status. Therefore, it is hard to stabilise impressions within a short time, particularly towards a newly added connection (on WeChat, in the form of a label or a group). Most of the informants we interviewed had more than 10 labels whose group members overlapped. A male student with 45 labels/groups for his WeChat connections commented,

> When I post something, it might be context-specific (thus trivial). So I would create a new group to determine who can or cannot see my particular post. I ended up with 45 groups set up. I did not realise this until you asked me to count the groups. (Personal communication, informant 24, 2017)

Users may include or exclude different connections primarily for reasons of trust, particularly when their circles of friends are growing. Family members do not care much about privacy in terms of personal information, as they have already known the details and would not normally use it for threatening purposes. However, this does not mean that users will let their family members see each and every post on their WeChat Moments. University students may want to maintain the image of ‘being a good kid and student’, so posts concerning skipping morning classes, having fun in nightclubs or complaints about their tutor are often excluded and blocked from their family members and relatives. This privacy paradox thus triggers various protective tactics used by users who are willing to manage and control their privacy exposure on WeChat.

Protective tactics: managing privacy on social media

In this section, protective behaviour and tactics are investigated as ‘the other’ aspect of the privacy paradox. The behaviour consists of a series of actions developed over time from a request of new connection to the establishment and cancellation of a connection.

Ex-ante: ignore or accept new connection requests

One type of protective behaviour is a strategy that works as an overarching principle for users to control their personal information from the very beginning and to reject or allow access as an antecedent mechanism. The interviews show that category-based information and attribute-based information are first used to decide whether to accept a new request on WeChat. WeChat allows users to locate a specific account by QQ account or mobile phone number in addition to WeChat ID, which is the default privacy setting when a user registers. Users can choose to opt out of certain search criteria so that not every method is activated. This provides an initial level of control for users to manage the visibility of their account. When a user receives a new friend request, a message containing the requester’s self-introduction will be sent. This is the primary category-based information a responder relies on to decide whether to accept or not. The requester’s profile will simultaneously be viewable by the responder; it usually consists of the name, nickname, location, origin (request from a shared group, from scanning QR code, etc.), self-introduction, profile picture, and posts. WeChat’s post settings range from all posts for the public to view, 10 posts for non-connections, or none. One recent update in the latest version of WeChat is to allow all users to view posts from the past 3 days, 6 months, or all posts. Depending on the settings of a requester, a responder can therefore use all or limited posts as attribute-based information to get an impression of the requester. If the requester’s profile looks suspicious and untrustworthy, the request will usually be declined. If the requester is persistent, his or her request can be blocked and put on a blacklist. The informants were generally aware of these functions and used them in various ways. However, as some informants suggested, most requests were from established real-life social networks, so they would try to map them online and offline to determine whether to accept a friend request. From the above analysis, we understand that even within established real-life relationships, there is a spectrum and hierarchy based on how trustworthy a relationship is, which will affect the privacy settings accordingly. For requests outside the established friendship, such as new classmates, colleagues, and contacts necessary for transactional and professional purposes, the level of privacy exposure varies, and the privacy setting is available for users to exercise control.

A dynamic management process

The above section examined the accessibility and diagnosability (both category-based information and attribute-based information) of a requester as antecedent mechanisms, which constitute the first step towards the management of privacy on WeChat. Once the connection and the information (including privacy) exposure are established, users have various tactics to protect their privacy using functions afforded by WeChat.

The first set of tactics employed by users is *information screening: grouping, labelling, and blocking*. They used technology-based controls and screening of their own information on WeChat. As mentioned, WeChat has developed over time a set of opt-out privacy settings for users to manage their posts by groups, labels, and timelines. There are options such as to let connections see all posts, those within 6 months, or those within 3 days. Users can also change the accessibility of their posts by including or excluding certain groups. If they have changed their impression towards certain connections, they can block them and put them on a blacklist or simply delete them. The blocking takes two forms: either blocking the access of a connection from viewing a post or refusing to view a connection's posts. This tactic is based on the control of accessibility. Another tactic works on the visibility of a user's information, which is primarily focused on the diagnosability of the information.

The second set of tactics is *de-identification and persona construction*. To manage the diagnosability of the information posted, a user must work on the content posted online and how these posts are crafted to avoid easy identification. As one informant pointed out, 'never trust your friends' posts on social media' (Personal communication, informant 6, 2017). This indicates the suspicion concerning information circulated on WeChat Moments. This does not mean that the posts are all fake, but they have never been raw data. Thus, they should not be taken at face value. The information has been carefully crafted, screened, engineered, or manufactured. It requires media literacy to understand it and is open to interpretation. Persona construction by Chinese youths on social media is another factor identified in the interviews. Most informants agreed that the Moments they posted were what they wanted to show to others, images or personas carefully rehearsed and curated over time, although with some exceptions. These included selfies, lifestyle and emotions, trips and check-ins, and important life events, in addition to other everyday occurrences. The crafted personas were particularly evident in the pictures and selfies posted, which were heavily manipulated with the help of a number of beautifying apps and filters. Some informants used mosaics or emojis to blur or cover pictures that had personal information. Some who were highly aware of privacy exposure would never post selfies or photos with their faces on WeChat. Instead, they used animated avatars, animals, or other pictures as their profiles. They even checked-in at different locations or provided the wrong geo-location information to confuse their connections. These de-identification tactics were considered to be helpful in creating a safer environment for their online privacy, at least psychologically.

The third tactic we found through our interviews is *ex-post: abstinence, deletion, and withdrawal*. It involves a set of *ex-post* measures to control the flow of information. Radical views on privacy protection are about trying not to leave any traces of personal information on social media, and some informants even suggested stop using WeChat. However, this is not a constructive measure, as most users would make full use of the platform, and the strategy shall be about how to avoid privacy exposure rather than exercising a complete withdrawal. This tactic is therefore proposed as a damage-control measure. Some informants suggested that posts containing personal information should be deleted. In line with the concerns about expanded connections over time, WeChat released a new test version that supports user identification of connections with weak social ties as determined by the frequency of engagement within the past 6 months. The three criteria include private chat, shared group, and comments on Moments. Once identified, such connections can be deleted in bulk. One postgraduate studying computer science held a more relaxed view when interviewed together with his friend:

> It is good to be cautious, and I have no problem with that (function). But I don't think we should worry too much about information we posted a long time ago, even for the friends whom we engage with less. They probably just don't care and thus will not violate our privacy. I understand the dark side of big data and all that. But there is a boundary of big data, too. Just imagine: Tencent has to invest a lot to store the 'junk talks' we produce every day. At a certain point, they have to delete them from their servers if that junk does not bring any profits. (Personal communication, informant 16, 2017)

This view is not at all surprising, and generally among the informants, a lower level of concern was found over corporate control and surveillance of users' privacy compared with potential privacy breaches by their connections. The informants were aware of and even appreciated the retargeted advertisements if they found them helpful. If not, they tried to ignore the advertisements and would sometimes click 'likes' to show that they were targeted by a certain brand or company to attract affirmation and admiration among their various social circles.

Conclusion

In this study, we investigated how urban young Chinese adults perceived and protected their privacy on the popular social media platform WeChat. Concern over privacy exposure on social media within a growing and expanding social network is on the increase. Specific social, organisational, institutional and technological concerns were examined. The sensitivity of content, audiences, and trust and attitudes stemming from privacy calculus and privacy dispositions were also discussed. Using the framework of privacy paradox, the different levels of concern in an increasingly surveillance-based and exploitive social media and big data era were investigated. Users used different tactics such as *ex-ante*, de-identification and persona construction, and *ex-post* measures to manage the accessibility, control, visibility, and diagnosability of their posts and profiles in a changing dynamic. We contribute to the literature by providing a richer and more up-to-date approach to privacy perception and protection in China. *Ex-ante* measures have not been fully investigated in the existing literature, and privacy protection is assumed to only become an issue when the connection is established. However, our interviews show that privacy management starts long before that, with the development of sophisticated analytical and psychological processes, and we thus make a specific contribution to the literature.

To sum up, we have four observations based on our empirical study. First of all, in the online environment of WeChat, users possess certain amount of freedoms. However, when it comes to users' individual privacy in the online environment, it appears as if users have or at least behave in such a way that would suggest they have a declined sense of their own freedom and right to privacy. The widespread acceptance of WeChat as an integral part of modern social communication in China and beyond has bestowed on the platform a unique and highly influential form of power: it has the power to control users' privacy and construct new privacy norms.

Secondly, the amount of coverage that WeChat privacy issues have received in the media in the past few years means it would be difficult for users to not have become aware, to some degree, that they should harbour concerns about personal information and privacy on WeChat. It would be logical to assume that the natural response to such concerns would be to seek a means to improve the security of one's personal information. However, a privacy paradox exists when users, while holding a high level of concerns, in reality do little to further the protection of their personal information on WeChat. An important reason may be that WeChat is one of the most influential social media platforms available in China, while its competitors such as WhatsApp, Facebook, Tumblr, and Twitter are blocked.

Thirdly, to try and understand the cause of this paradox, the interviews conducted in this study indicate that it appears to come down to a simple cost-benefit analysis by WeChat users. Once a user has ingrained part of their social engagement within the WeChat system, the incentive for them to remain a part of the system outweighs their requirement to secure their privacy online. In response, the incentive for WeChat to willingly improve the privacy for its users is not nearly as strong, as the platform understands the social investment its users have will drive the majority to stay regardless of the improvements that it calls for. Not to mention the fact that WeChat's success is sustained through the commodification of user-generated content (Tengyun 2017). The network externality accumulated via this particular platform is what the users cannot afford to lose. The social, economic and arguably political power WeChat has now acquired drives more and more people to become involved, and stay involved, in the effort to avoid social exclusion. This also confirms the importance of social bonding in China as discussed at the beginning of this paper.

Last but not least, this translates to users' continued use of the social media platform, despite privacy concerns. This reality bestows on WeChat a unique form of power. While WeChat, of course, does not wield this power by directly threatening to cut its general users off from the social interaction available through its platform, it needs not do so, as the social capital investment that users have made appears to be too valuable to simply give up despite the existence of any privacy concerns. To reiterate, users now use WeChat not only for private conversations, but also for study or work-related purposes. This is quite a unique phenomenon in the use of WeChat that we identified in a Chinese context. It further blurs the boundaries between the public, the professional and the private which is a rare case compared with other social media around the world.

However, our findings are based on a limited number of informants on WeChat, who were predominantly urban young university students. They were tech savvy and well educated and might be biased in terms of their social media usage. Although we have touched upon privacy violations such as identity theft, further investigations into severe and unusual cases in other more public and privacy-free social media platforms are warranted. These cases may be intertwined with online security and crime, which is out of the scope of this study, but these are important aspects in need of further scrutiny and investigation to inform current privacy policy. It might not be immediately possible to generalise our research findings to the wider international social media landscape, but our nuanced investigation provides necessary updates and empirical data for the careful examination of privacy perception and protection online among urban young adults in China. WeChat is one of the most influential social media platforms in China, but it is worth noting that although around 800 million people are online (Tengyun 2017, p. 6), the other half of the population is not. The gaps between the digital haves and have-nots and between digital natives and migrants, in addition to the nuances between rural and urban, as well as male, female and LGBT (lesbian, gay, bisexual, and transgender) users, require further investigation.

References

Al-Kandari, A., Melkote, S. R., & Sharif, A. (2016). Needs and motives of Instagram users that predict self-disclosure use: A case study of young adults in Kuwait. *Journal of Creative Communications*, *11*(2), 85–101.

Bae, Y. H., Jun, J. W., & Hough, M. (2016). Uses and gratifications of digital signage and relationships with user interface. *Journal of International Consumer Marketing*, *28*(5), 323–331.

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154.

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of Internet skills for online privacy protection. *Information, Communication & Society*, *20*(8), 1261–1278.

Choi, B. C., Jiang, Z., Xiao, B., & Kim, S. (2015). Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. *Information Systems Research*, *26*(4), 675–694.

Clover, C. (2017). Overloaded China users battle 'WeChat fatigue'. *Financial Times*. https://www.ft.com/content/51dfa598-0189-11e6-99cb-83242733f755.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108.

Dhir, A., Kaur, P., Chen, S., & Lonka, K. (2016). Understanding online regret experience in Facebook use—effects of brand participation, accessibility and problematic use. *Computers in Human Behavior*, *59*, 420–430.

Du, P. (2015). *Intercultural communication in the Chinese workplace*. Basingstoke: Palgrave Macmillan.

Fei, X. (1992). *From the soil, the foundations of Chinese society: A translation of Fei Xiaotong's Xiangtu Zhongguo* (G. G. Hamilton & Z. Wang, Trans.). Berkeley: University of California Press.

Fisk, S. T., & Neuberg, S. L. (1990). A continuum of impression formation, from category-based to individuating processes: Influences of information and motivation on attention and interpretation. *Advances in Experimental Social Psychology*, *23*, 1–74.

Fox, J., & Moreland, J. (2015). The dark side of social networking sites: An exploration of the relational and psychological stressors associated with Facebook use and affordances. *Computers in Human Behavior*, *45*, 168–176.

Fulco, M. (2017). The WeChat economy, from messaging to payment and more. *Cheung Kong Graduate School of Business*. http://knowledge.ckgsb.edu.cn/2017/08/28/mobile-commerce/wechat-economy-messaging-wechat-pay/.

Fulton, J. M., & Kibby, M. D. (2017). Millennials and the normalization of surveillance on Facebook. *Continuum-Journal of Media & Culture Studies*, *31*(2), 189–199.

Hodkinson, P. (2017). Bedrooms and beyond: Youth, identity and privacy on social network sites. *New Media & Society*, *19*(2), 272–288.

Jeong, Y., & Coyle, E. (2014). What are you worrying about on Facebook and Twitter? An empirical investigation of young social network site users' privacy perceptions and behaviors. *Journal of Interactive Advertising*, *14*(2), 51–59.

Jeong, Y., & Kim, Y. (2017). Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. *Computers in Human Behavior*, *69*, 302–310.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134.

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on social network services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human Computer Studies*, *71*(9), 862–877.

Li, H. S. (2016). Narrative dissidence, spoof videos and alternative memory in China. *International Journal of Cultural Studies*, *19*(5), 501–517.

McLaren, R. M., Dillard, J. P., Tusing, K. J., & Solomon, D. H. (2014). Relational framing theory: Utterance form and relational context as antecedents of frame salience. *Communication Quarterly*, *62*(5), 518–535.

McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a feather: Homophily in social networks. *Annual Review of Sociology*, *27*, 415–444.

Morando, F., Iemma, R., & Raiteri, E. (2014). Privacy evaluation: What empirical research on users' valuation of personal data tells us. *Internet Policy Review*, *3*(2), 1–11.

Norberg, P. A., Horne, D., & Horne, D. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Raacke, J., & Bonds-Raacke, J. (2008). MySpace and Facebook: Applying the uses and gratifications theory to exploring friend-networking sites. *Cyberpsychology Behavior*, *11*(2), 169–174.

Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, *4*(4), 323–333.

Rubinstein, I. S. (2013). Big data: The end of privacy or a new beginning? *International Data Privacy Law*, *3*(2), 74–87.

Smith, C. (2018). 110 amazing WeChat statistics and facts (January 2018). *DMR*. https://expandedramblings.com/index.php/wechat-statistics/.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196.

Spottswood, E. L., & Hancock, J. T. (2017). Should I share that? Prompting social norms that influence privacy behaviors on a social networking site. *Journal of Computer-Mediated Communication*, *22*(2), 55–70.

Tengyun. (2017). *Creator economy: A new era of the 'Internet + Cultural and Creative'—social reception, industry ecology and policy system*. Beijing: Development Research Centre of the State Council, Tencent Social Research Centre.

Walsh, M. J., & Baker, S. A. (2017). The selfie and the transformation of the public–private distinction. *Information, Communication & Society*, *20*(8), 1185–1203.

Walther, J. B., Van Der Heide, B., Kim, S. Y., Westerman, D., & Tong, S. T. (2008). The role of friends' appearance and behavior on evaluations of individuals on Facebook: Are we known by the company we keep? *Human Communication Research*, *34*(1), 28–49.

Yang, C.-C., Brown, B. B., & Braun, M. T. (2014). From Facebook to cell calls: Layers of electronic intimacy in college students' interpersonal relationships. *New Media & Society*, *16*(1), 5–23.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, *16*(4), 479–500.

Zarouali, B., Ponnet, K., Walrave, M., & Poels, K. (2017). "Do you like cookies?" Adolescents' skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing. *Computers in Human Behavior*, *69*, 157–165.

Zlatolas, L., Welzer, T., Hericko, M., & Holbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*, *45*, 158–167.