Investigating Privacy Perception and Behavior on Weibo

Clinton Amos
John B. Goddard School of Business and Economics
Weber State University
Ogden, Utah 94408
Tel: 801-626-7307
Email: clint.amos@gmail.com

Lixuan Zhang
Hull College of Business
Georgia Regents University
Augusta, Georgia 30907
Tel: 706-667-4525
Email: lixuan.zhang@gmail.com

Iryna Pentina
Department of Marketing and International Business
University of Toledo
Toledo, Ohio 43606
Tel: 419-530-2093
Email: Iryna.Pentina@UToledo.edu
Investigating Privacy Perception and Behavior on Weibo

Abstract

More than half of Chinese Internet users participate in Weibo, the most popular social media and microblogging platform in China. Weibo encourages members to voluntarily contribute personal information, leading to potential privacy invasion. This study examines how trust in other Weibo members and perceptions of government intrusion affect privacy-related attitude and behavior. Analysis of survey responses from 221 Weibo users confirm that perceived government intrusion is strongly correlated with privacy concern and self-protective behavior. Trust towards other Weibo participants is not significantly related to privacy concern; however it has a significant negative relationship with self-protective behavior. The study also reveals that privacy concern is positively related to self-protective behavior. Findings and their implications for future research and practice are provided.

Keywords: privacy concern, social media, Weibo, trust, protective behavior
Introduction

Microblogging is a form of social media that allows users to broadcast short messages via various platforms to friends and followers, ensuring frequent and immediate updates on their activities, opinions, and status (Barnes & Böhringer, 2011). The most popular microblogging platform is Twitter, which has numerous clones and competitors around the world. After China blocked Twitter in 2009, several Chinese media companies launched microblogging services that are rapidly gaining popularity. The two major microblogging service providers in China are Sina, with a market share of 56.6% and Tencent with a market share of 21.5% (iResearch, 2011). Microblogging in China is referred to as ‘Weibo’ (literal translation of microblogging). The China Internet Network Information Center (CNNIC) recently reported that 50.9% of the Chinese Internet population use Weibo, yielding 274 million microblogging participants (CNNIC, 2012a).

Much like Twitter, Weibo members post tweets or messages with 140 characters or less. Its members follow and are followed by others without the need to reciprocate the relationship. Every member’s Weibo page is publicly viewable, and mutual followers can exchange private messages. However, several distinct Weibo features differentiate it from Twitter. First, since each Chinese character represents a whole word, tweets written in Chinese communicate much richer content than English tweets. Additionally, Weibo users can post pictures and videos directly into their feeds. Weibo allows threaded comments on feeds, viewed under the original message and not broadcast to the user’s followers. Its Chat function provides a side-by-side alternative to the private messaging system. Furthermore, it provides virtual currency for purchasing virtual goods and services on the platform. The combined features of microblogging and social networking allow Chinese Weibo to provide greater possibilities of self-expression and relationship formation.

While Weibo users relish the opportunity to express themselves and establish unique identities (Zhang & Pentina, 2012), doing so inevitably requires personal information disclosure, leading to privacy violation risks such as stolen identity, potentially damaged reputation, harassing or cyberstalking. Additionally, government use of personal information posted on Weibo may have employment, financial, and political consequences, especially since recent legislation requires using real names for Weibo registration. Despite these risks, evidence shows that more and more young people in China do not mind disclosing personal information and enjoy sharing personal life on the Internet (CNNIC, 2012b). The CNNIC report indicates that 62.2% of social media users have never worried about social media privacy issues. Social media users may be aware of privacy violation risks, yet continue publishing public profiles with sensitive personal data.

Researchers have investigated the discrepancy among social media participants’ beliefs, attitudes and behaviors using multiple theories. However, most existing research uses U.S. and student samples, limiting the roles of cultural and contextual factors in privacy perceptions and behaviors (Waters & Ackerman, 2011). Moreover, few studies consider the role of government intrusion threat in affecting privacy attitudes and behaviors. Finally, although scholarly efforts identify drivers of privacy concern, few studies examine its behavioral consequences. The current study addresses these gaps by utilizing the communication privacy management theory to empirically examine privacy-protective attitude and behavior in a Chinese social media context. In what
follows, we develop our theoretical model and hypotheses, explain data collection procedures and analysis methods, and present and discuss the results. Subsequently, we suggest practical and theoretical implications of the findings.

**Theoretical Development and Hypotheses**

Communication privacy management (CPM) theory (Petronio, 2002) suggests that individuals believe private information is a possession that they have the right to control. Consequently, each person forms an informational space around oneself, and its individually-established boundaries determine information sharing behavior. Depending on the situational and personal factors, any attempt by others to penetrate these boundaries can represent a threat. In social media, due to ubiquitous access to information by anyone, situational factor such as the government policy and personal factor such as trust in other members may affect individual information boundary. The resulting perceived concern may lead limited information disclosure or the provision of false information.

**Trust Towards Other Members**

After individuals grant access to their private information, the information is collectively owned by the individual and other data recipients, representing an extension of privacy boundaries (Petronio, 2002). The data recipients are responsible for managing the information given and maintaining privacy. Since published information is not restricted, the personal information space in social media becomes co-owned by everyone who sees it. Once the information is collectively owned, a set of rules are negotiated for third-party dissemination (Child, Pearson and Petronio, 2009). Since people do not always effectively negotiate privacy rules for collectively held private information, *boundary turbulence* may occur, i.e. privacy violation (Petronio, 2002). On social media platforms, violations occur when one user’s posts are copied without providing credit, or one’s personal information is falsified and then published publicly. When social media participants distrust fellow members, they will perceive higher privacy risk (Krasonova et al., 2010).

In this study, trust is defined as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” (Mayer et al., 1995, p. 712). Trust often enables collaborative behavior and reduces harmful conflict. People trust others with similar characteristics, whom they have had longer interaction with and whom they may expect to have future repeated interactions with (Alesina & Ferrara, 2000). In social media, trust is salient because online relationship development is possible when every party is willing to open themselves to each other. Trust is critical for creating and maintaining online communities and virtual groups (Ridings et al., 2002), and it encourages information disclosure (Metzger, 2007). While the impersonality, anonymity and automation of electronic communications make trustworthiness evaluations of other members difficult for social media participants (Ferrazzi, 2012), trust can still be fostered by repeated interaction (Kanagaretnam et al. 2010) and mutual interests (Ridings et al., 2002). Research studies report that trust is a major factor influencing networking activity on social media (Debatin et al. 2009), as well as information sharing intensity (Dwyer et al., 2007; Ridings et al. 2002). Therefore, we propose:
H1a: Trust towards other social media participants is negatively associated with users’ perceived privacy concern.
H1b: Trust towards other social media participants is negatively associated with users’ self-protective behavior.

Perceived Government Intrusion Concern
Government censorship is a major characteristic of the Chinese Internet. Concerned about losing power or social control due to free information exchange on the Internet, the Chinese government enforces censorship on three levels: firewall devices at the border, government-mandated self-censorship by the Internet and content service providers, and self-restriction by individuals (Tan & Tan, 2012). Similarly, the government highly monitors and censors the microblogging space using human censors and software to monitor and update lists of sensitive words (Sullivan, 2012), likely increasing cautiousness of Weibo users when discussing certain topics. For instance, several accounts were banned for allegedly spreading political rumors (Reisinger, 2012), and according to a recent study, censors delete about 13 percent of China’s social media content (King et al., 2013). To hold Weibo posters accountable, on 16th December 2011, the Beijing municipal government announced the Rules on Microblogging, requiring users to register with real names. Anyone wanting to create a new Weibo account needs to submit their personal ID number. Existing subscribers who fail to register with real names can only read posts but cannot comment on or forward them. While at the moment the real name registration rule is inconsistently enforced, Weibo has introduced several mechanisms to encourage users to provide real identity information voluntarily. For example, anyone can become a “verified user” when reaching a minimum number of followers and followed accounts, use a real photo as profile picture and bind their cell phone to the Weibo account.

Although the alleged purpose of government surveillance is to nurture a healthy Internet environment, it brings many undesirable results, such as control of freedom of expression, unreliable data use, excessive intrusion into private behaviors and ambiguous definition of illegal and detrimental information. Much of the interactions occurred on online social media platforms can be subject to storage and later retrieval, compounding the concerns about privacy (Tufekei, 2008). Previous research has shown that government intrusion concern is negatively related to individuals’ e-commerce use (Dinev et al. 2006) and their willingness to disclose personal information (Dinev, Hart and Mullen, 2008). Since information posted on Weibo is monitored by the government, Weibo users may experience deletion of posts or accounts for communicating politically unacceptable messages. Therefore we propose:

H2a: Perceived government intrusion concern is positively related to privacy concern.
H2b: Perceived government intrusion concern is positively related to self-protective behavior.

Self-protective Behavior
Self-protective behavior is a set of users’ behavioral responses to privacy concern. According to CPM, users must serve a critical role in privacy protection by taking necessary actions to restrict personal information disclosure. CPM postulates that users create rules to maximize benefits and to minimize risks of information disclosure. When concern for privacy is high, boundary protection rules dominate and users withhold information. Withholding information is a common self-protection strategy for users in an e-commerce situation (Metzger, 2007; Son & Kim, 2008).
Users can abstain from participating activities leading to privacy concern. For Weibo users, they can withhold identifying information in two ways: both in their personal profile page and in the tweets they create.

To some extent, the survival and growth of social media sites depend on users’ disclosure of personal information so it is unlikely that the site operators will demotivate users to post personally relevant or identifying information. Users must control their own digital profile. However, due to the need for impression management, users often reveal extensive amounts of personal data. An analysis of over 4000 student Facebook profiles revealed that only a small percentage of users modify the default privacy setting (Gross & Acquisti, 2005). Another study found that over 90% of Facebook users disclose their real name, birth date, high school, profile picture and email address (Stutzman et al., 2011). Privacy paradox, defined as a discrepancy between privacy concern and actual privacy settings, often occurs in social media contexts (Barnes, 2006). However, evidence suggests that the gap between privacy concern and actual privacy-protecting behavior is closing. Utz and Kramer (2009) found that users with higher privacy concern have more restrictive privacy settings on social networking sites. The direct impact of privacy concern on ecommerce (Dinev & Hart, 2004) and e-banking (Jahangir & Begum, 2007) adoption behaviors was empirically supported. Additionally, privacy concern influences acceptance of technology and online purchase intentions (Smith et al., 2011).

Therefore:

H3: Privacy concern is positively related to self-protective behavior.

The research model for the study is presented in Figure 1. Based on CPM, the study focuses on two factors affecting Weibo users’ privacy attitude and behavior: perceived government intrusion concern and trust towards other Weibo users. We also hypothesize that Weibo users’ perceptions of privacy concern lead to the adoption of self-protective behaviors. Three variables are included as controls for both privacy concern and self-protective behavior: age, gender and number of followers. Research shows that older individuals are concerned about privacy (Bellman et al., 2004; Graeff & Harmon, 2002). In addition, previous research was inconclusive about the role of gender in privacy concern and self-protective behavior, since some studies suggest women are more concerned about the control of their personal information than men (Fogel & Nehmad, 2009; Youn & Hall, 2008), while others indicating female tendencies to disclose more about themselves than men (Petronio, 2002). This study will further examine the gender difference in privacy attitude and behavior by using gender as a control variable. Additionally, users with larger audiences may be more concerned about their privacy and consequently may safeguard their privacy more, therefore number of followers si also added a s a control. Since the variable number of followers does not follow a normal distribution, the natural log of the variable is used as the-acontrol variable.
Methodology

Scale Development
Hinkin (1998) suggested that survey items should be developed by specifying the content domain and developing items to evaluate that domain. An inductive approach to scale develop is appropriate and useful when conducting research in new contexts (Hinkin, 2009). Although there are early attempts to measure self-protective behavior (Youn, 2009; Youn & Hall, 2008; Son & Kim, 2008, Young & Anabel Quan-Haase, 2013), no established scale for self-protective behavior exist in the context of Weibo. In addition, the construct validity and reliability of previous scales are not measured. To develop the scale, we first gathered Weibo users’ opinion on how to protect privacy. An open-ended question was posted on a Chinese market research website: “How do you protect your privacy on Weibo?” Forty-eight Weibo users answered the question. Content analysis of the open-ended questionnaires revealed that the users mainly safeguard privacy by withholding their personal information. After evaluating the open-ended questionnaire and adapting the previous scales, five items were chosen to measure self-protective behavior on Weibo. The items were evaluated on their relevance, conciseness and clarity by an expert panel.

All other constructs were adapted from previous literature. The perceived privacy concern scale was borrowed from Xu et al. (2011). Government intrusion concern was measured by the Dinev et al. (2006) scale. Trust towards other members was adapted from Krasnova et al. (2010) which was measured on seven-point Likert scales with 1 being “do not trust at all” and 7 being “trust completely”. All the remaining constructs were measured on seven-point Likert scales with 1 being “strongly disagree” and 7 being “strongly agree”.

Data were collected from Weibo users by a market research firm. After removing the carelessly completed questionnaires, 221 questionnaires were retained for subsequent analysis. Table 1 displays the respondents’ demographic information along with tweet frequency and length of time using Weibo. The respondents have a median of 200 followers (min= 5, max = 119231) and
follow a median of 96 other accounts (min = 1, max = 1976). All respondents use the major two Weibo platform: 174 of them uses Sina Weibo while 47 uses Tencent Weibo.

Table1: Respondents’ Information

<table>
<thead>
<tr>
<th>Variable</th>
<th>Number of respondents</th>
<th>Percentage of total respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gender</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>126</td>
<td>43%</td>
</tr>
<tr>
<td>Female</td>
<td>95</td>
<td>57%</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18-23</td>
<td>13</td>
<td>6%</td>
</tr>
<tr>
<td>24-29</td>
<td>112</td>
<td>51%</td>
</tr>
<tr>
<td>30-35</td>
<td>63</td>
<td>29%</td>
</tr>
<tr>
<td>36-40</td>
<td>21</td>
<td>10%</td>
</tr>
<tr>
<td>41-50</td>
<td>12</td>
<td>5%</td>
</tr>
<tr>
<td><strong>Frequency of Tweets</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Several times every day</td>
<td>129</td>
<td>58%</td>
</tr>
<tr>
<td>Once every day</td>
<td>57</td>
<td>26%</td>
</tr>
<tr>
<td>Several times every week</td>
<td>27</td>
<td>12%</td>
</tr>
<tr>
<td>Once every week</td>
<td>5</td>
<td>2%</td>
</tr>
<tr>
<td>Several times every month</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Rarely</td>
<td>1</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Time Since first use</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Less than six months</td>
<td>1</td>
<td>0%</td>
</tr>
<tr>
<td>Six months to a year</td>
<td>31</td>
<td>14%</td>
</tr>
<tr>
<td>One year to one year and a half</td>
<td>58</td>
<td>26%</td>
</tr>
<tr>
<td>One year and a half to two years</td>
<td>59</td>
<td>27%</td>
</tr>
<tr>
<td>More than two years</td>
<td>72</td>
<td>33%</td>
</tr>
</tbody>
</table>
Results
Partial Least Squares (PLS), specifically SmartPLS 2.0 (Ringle, Wende and Will, 2005), was used to assess the psychometric properties of the measurement model and to test the hypotheses. Utilizing a component-based approach, PLS is designed to not only explain the variance, i.e. to examine the significance of the relationships and variance explained, such as in linear regression, but also to simultaneously model the structural paths and measurement paths (Gefen et al., 2000). PLS was chosen over covariance-based Structural Equation Modeling for two reasons. First, it is not contingent upon data having normal distributions and interval nature (Fornell & Bookstein, 1982), which makes PLS suitable for handling variable such as number of followers. Second, it is appropriate for exploratory studies in the early stages of theoretical development (Fornell & Bookstein, 1982).

Perceptual measures provide the potential for common method variance. In order to minimize this potential, the survey was arranged such that the dependent variables followed the measurement of the independent variables. Salancik and Pfeffer (1977) argue that this approach helps in reducing the effect of common method variance. In addition, in order to empirically test for this potential, Harman’s one-factor test was performed by using all items in a principal component factor analysis (Podsakoff et al., 2003). A substantial amount of common method variance is present when a single factor emerges from the factor analysis, or one factor accounts for the majority of the covariance among measures. In our data, four factors emerged from the factor analysis, and each factor explains roughly equal variance. Therefore, common method bias does not appear to be a foremost issue.

Assessment of Measurement Model
The adequacy of the measurement model is demonstrated through measures of convergent and discriminant validity. Convergent validity is assessed by examining composite reliability of constructs and average variance extracted (AVE) [see Table 2]. The data shows that the constructs demonstrate satisfactory internal reliability. The composite reliabilities range from 0.87 to 0.93, exceeding the recommended value of 0.70 (Gefen et al., 2000). The AVEs are above 0.5 as recommended by Fornell and Larcker (1981).

Table 2: Reliability and Discriminant Validity of the Constructs

<table>
<thead>
<tr>
<th></th>
<th>Variance Extracted</th>
<th>Composite Reliability</th>
<th>Cronbach Alpha</th>
<th>GOV</th>
<th>TRUST</th>
<th>PRIVACY</th>
<th>BEHAVIOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOV</td>
<td>0.80</td>
<td>0.92</td>
<td>0.88</td>
<td>0.89</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TRUST</td>
<td>0.73</td>
<td>0.91</td>
<td>0.88</td>
<td>-0.06</td>
<td>0.85</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRIVACY</td>
<td>0.77</td>
<td>0.93</td>
<td>0.90</td>
<td>0.70</td>
<td>-0.06</td>
<td>0.88</td>
<td></td>
</tr>
<tr>
<td>BEHAVIOR</td>
<td>0.57</td>
<td>0.87</td>
<td>0.82</td>
<td>0.50</td>
<td>-0.10</td>
<td>0.52</td>
<td>0.75</td>
</tr>
</tbody>
</table>

*Numbers in bold are square roots of average variance extracted.*
Discriminant validity was assessed by two criteria: 1) each item should have a higher loading on its hypothesized construct than on other constructs and 2) the square root of each construct’s AVE should be higher than its correlation with other constructs. Table 3 shows the factor and cross-loading results from the principal component factor analysis. All items have much higher self-loadings than cross-loadings. We also compared the square root of the AVE of each construct with its correlations. As Table 2 indicates, the AVE’s square root is greater than the construct intercorrelations.

Table 3: Loadings and Cross-Loadings of the Constructs

<table>
<thead>
<tr>
<th>CONSTRUCTS BEHAVIOR</th>
<th>GOV</th>
<th>TRUST</th>
<th>PRIVACY</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERCEIVED GOVERNMENT INTRUSION</td>
<td>gov1</td>
<td>0.1344</td>
<td>0.8688</td>
</tr>
<tr>
<td></td>
<td>gov2</td>
<td>0.1815</td>
<td><strong>0.9226</strong></td>
</tr>
<tr>
<td></td>
<td>gov3</td>
<td>0.1629</td>
<td><strong>0.8933</strong></td>
</tr>
<tr>
<td>TRUST TOWARDS OTHER MEMBERS</td>
<td>trust1</td>
<td>-0.0923</td>
<td>0.0351</td>
</tr>
<tr>
<td></td>
<td>trust2</td>
<td>-0.0188</td>
<td>-0.041</td>
</tr>
<tr>
<td></td>
<td>trust3</td>
<td>-0.0847</td>
<td>-0.1103</td>
</tr>
<tr>
<td></td>
<td>trust4</td>
<td>-0.071</td>
<td>-0.0373</td>
</tr>
<tr>
<td>PRIVACY CONCERN</td>
<td>privacy1</td>
<td>0.2788</td>
<td>0.2549</td>
</tr>
<tr>
<td></td>
<td>privacy2</td>
<td>0.2201</td>
<td>0.2693</td>
</tr>
<tr>
<td></td>
<td>privacy3</td>
<td>0.2482</td>
<td>0.2693</td>
</tr>
<tr>
<td></td>
<td>privacy4</td>
<td>0.3594</td>
<td>0.2655</td>
</tr>
<tr>
<td>PROTECTIVE BEHAVIOR</td>
<td>behavior1</td>
<td><strong>0.6885</strong></td>
<td>0.2863</td>
</tr>
<tr>
<td></td>
<td>behavior2</td>
<td><strong>0.7664</strong></td>
<td>0.2251</td>
</tr>
<tr>
<td></td>
<td>behavior3</td>
<td><strong>0.7983</strong></td>
<td>0.2287</td>
</tr>
<tr>
<td></td>
<td>behavior4</td>
<td><strong>0.7467</strong></td>
<td>0.2501</td>
</tr>
<tr>
<td></td>
<td>behavior5</td>
<td><strong>0.7412</strong></td>
<td>0.3704</td>
</tr>
<tr>
<td></td>
<td>behavior6</td>
<td><strong>0.7490</strong></td>
<td>0.4167</td>
</tr>
</tbody>
</table>

Assessment of Structural Model

With an adequate measurement model, the hypotheses were tested by examining the structural model. The PLS algorithm and the bootstrapping re-sampling methods were used with the 221 cases, and 1000 re-samples were used to estimate the model. Figure 2 shows the results. The model accounts for 50.3% of variance in privacy concern and 34.4% of variance in self-protective behavior.

In contrast to H1a, trust towards others is not significantly related to perceived privacy concern. There is a significant negative relationship between trust towards others and self-protective behavior, lending support to H1b (b=-0.07, p<0.01). Perceived government intrusion is positively related to perceived privacy concern (b=0.70, p<0.01) supporting H2a. As hypothesized, perceived government intrusion is significantly related to self-protective behavior, supporting H2b (b=0.24, p<0.01). Privacy concern is positively related to self-protective behavior (b=0.37, p<0.01), supporting H3. For the control variables, age is not significantly related either to privacy concern or self-protective behavior. Gender is significantly
related to privacy concerns and self-protective behavior. Females have a higher level of privacy concern ($b=0.06$, $p<0.05$), however, they are less likely to engage in self-protective behavior ($b=-0.06, p<0.05$). Number of followers is not significantly related to privacy concerns but Weibo users with large number of followers reported higher engagement in self-protective behavior ($b=0.08$, $p<0.05$).

To evaluate the impacts of two antecedents on perceived privacy concern and three antecedents on self-protective behavior, an effect size analysis was completed. Effect sizes can be evaluated via Cohen’s $f^2$ (Cohen, 1992), which is calculated using the formula ($R^2$ included - $R^2$ excluded)/(1 - $R^2$ included). $R^2$ included was the $R^2$ value with the independent construct included, and $R^2$ excluded was the $R^2$ value with the independent construct omitted. The guidelines for assessing the Cohen’s $f^2$ are 0.02 for small effect, 0.15 for medium effect and 0.35 for large effect (Cohen, 1988). Perceived government intrusion is found to have a large effect on perceived privacy concern ($f^2=0.46$) and a small effect on self-protective behavior ($f^2=0.04$). Privacy concern has a small effect on self-protective behavior ($f^2=0.11$). Trust towards others does not have a significant effect on self-protective behavior.

![Figure 2: PLS Model](image)

**Discussion**

The study empirically tests the applicability of CPM theory (Petronio, 2002) in the context of the Chinese microblogging service Weibo. In particular, relying on the CPM’s cornerstone principle of privacy management dialectics, which postulates a behavioral tension between concealing and revealing private information, we propose and test the attitudinal mechanism that regulates this behavior. Results indicate that increases in privacy concern motivate Weibo users to choose self-protecting coping behaviors. This finding is consistent with previous studies that privacy concern substantially affects information disclosure (Derlega et al., 2008). Finally, we examine the roles of the two factors trust in other Weibo members and governmental intrusion in affecting Weibo users’ perceived privacy concern.

Contrary to expectations, an insignificant relationship between trust towards others and perceived privacy concern was found. Hence, trust in other Weibo users does not appear to
heighten privacy concerns. In contrast, findings suggest that perceived government intrusion is positively and substantially related to both perceived privacy concern and self-protective behavior. Constant government censorship of Weibo, as well as the strategies to control its content, such as real name registration, credit system, and deleting accounts, objectively removes or minimizes privacy from the platform and, consequently, increased users’ privacy concerns and the actions taken to protect privacy.

In addition, findings show that Weibo members with more followers do not have greater privacy concerns while engaging in more self-protective behavior. Finally, this results of the study show that the females seem to demonstrate paradoxical behavior in privacy. They have a significantly higher level of privacy concern than females, yet they are less likely to engage in self-protective behavior than males. Other research also finds that women generally are more concerned about the effect the privacy invasion practice, but they are less likely to adopt behaviors to safeguard and protect their privacy (Sheehan, 1999). The discrepancy between attitude and actual behavior among females deserves future research investigation.

Theoretical and Practical Implications

The study makes several contributions to online privacy research and practice. First, the study is among one of the early studies to examine privacy in microblogging platforms in China. We propose and test a model of antecedents of privacy concern and self-protective behavior based on CPM theory. Our findings show that presence of government censorship is strongly correlated with privacy concern, limiting information disclosure on Weibo. Surprisingly, the degree of trust in other Weibo members is not associated with privacy concern. Past research would dictate that as an individual’s lack of trust towards others would increase his/her privacy concern. The insignificant relationship between trust towards other members and privacy concern may result from the strength of the perceived threat from government intrusion since the government is perceived to pose a major threat with possibly severe sanctions. Chinese Weibo users may perceive other members as posing minimal threat relative the government, explaining their lack of concern. Another possible explanation for the insignificant relationship between trust and privacy concern could be the nature of network ties among Weibo members. It was previously noted that, although experiencing lower trust, members of the MySpace online network (characterized by weak ties and greater exposure to strangers), form more relationships than members of Facebook (characterized by stronger ties of university peers) (Dwyer et al., 2007). Apparently, for such a public network as Weibo, where anyone can follow anyone else without permission or reciprocity, lack of trust does not necessarily mean greater privacy concern. The so-called “third-person effect”, when users perceive others to be more at risk for privacy violations than themselves (Debatin et al. 2009), may also mitigate perception of risk in social media. Finally, a false sense of anonymity whereas one perceives that there are appropriate safeguards to maintain anonymity (Friedman et al., 2004) or that they can terminate a relationship at any given time (Dwyer et al., 2007) may explain a weaker role of trust in privacy concern on Weibo. Clearly, future research is needed to investigate the role of trust further and identify other potential Weibo community-related factors that may reduce privacy concerns. From past research, such variables as internalization of community norms and codes of conduct, as well as social identification with the community may be considered (e.g., Mazar et al., 2008).
Third, the findings that Weibo members with more followers do not have greater privacy concerns while engaging in more self-protective behavior are intriguing. It is possible that more popular Weibo users may have psychological traits such as narcissism, leading them to be overconfident, explaining the lack of privacy concern (Campbell et al., 2004). Alternatively, those with more followers may have a prominent social status offline (e.g. celebrities) and thus accept the public nature of their private lives and recognize that they need to engage in some self-protective behavior despite not feeling a heightened sense of privacy concern. These assertions may warrant further investigation.

Fourth, answering the call for investigation of privacy concern outcomes (Xu et al., 2011), the study proposes and tests the self-protective behavior construct. A careful examination of the items shows that users mainly use avoidance strategies. They avoid revealing anything identifiable, provide incomplete profile information and change default privacy settings. These items provide a foundation for the development of comprehensive self-protective behavior measures on Weibo.

Characterized as a hybrid of Twitter and Facebook, Weibo is deeply integrated into Chinese life and represents an important medium of marketing communication and research. Access to personal information, such as demographic and psychographic characteristics, can help online marketers create personalized messages and products. Therefore, understanding what drives Weibo users to disclose or protect their private information is of great interest to marketers. The identified role of government censorship in increasing privacy concerns and protective behaviors needs to be taken into account by marketers, necessitating potential adjustment of market research data with the provision of incomplete or false profile information. Marketers should be sensitive to Weibo members’ preferences regarding information disclosure and would be better served using inbound marketing tactics (such as creating Weibo brand accounts and providing content and entertainment). Given greater efforts of the UN and other governments to control the Internet, future research can test the influence and magnitude of perceived government intrusion on privacy concerns and self-protective behavior across cultures and in other political contexts.

The substantial relationships between perceived government intrusion, privacy concerns and self-protective behavior suggests that Weibo site operators should further enhance users’ privacy settings and choices. Recently, Sina Weibo has given more control to users regarding their tweet visibility. For example, in 2011, tweets can be designated as public (visible to all) or private (not visible to others). In September, 2012, the new version 5 of Sina Weibo provided users the ability to group their followers and then choose to post a tweet that only specific groups can view. Sina Weibo needs to promote its Community Management Center to enhance perceptions of it as a legitimate channel for privacy protection. By establishing and enforcing community norms, Weibo can ensure that members’ deviant behaviors are significantly reduced. Similar privacy adjustments are applicable with respect to advertising: users should be able to regulate their exposure to advertising or the use of their private browsing or purchasing information for advertising. By voluntarily regulating advertising and marketing on the site, Weibo can increase its credibility among its members.
References


Utz, S., & Kramer, N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms, *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 3*(2), article 1.  


Appendix: Measurement Items and Descriptive Statistics

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust towards other members (Mean=5.18, Std.Dev=0.90)</td>
<td>Other Weibo members will do their best to help me. Other Weibo members do care about the well-being of others. Other Weibo members keep their promises. Other Weibo members are trustworthy.</td>
</tr>
<tr>
<td>Perceived government intrusion concern (Mean=4.60, Std.Dev=1.39)</td>
<td>I am concerned about the power that government has to monitor Weibo. I am concerned my personal information on Weibo will be more open to government. I am concerned that my personal information on Weibo could be investigated by government.</td>
</tr>
<tr>
<td>Privacy concern (Mean=5.36, Std.Dev=1.21)</td>
<td>I am concerned that information submitted to Weibo can be misused. I am concerned that others can find private information about me on Weibo. I am concerned about providing personal information on Weibo, because what others might do with it. I am concerned about providing personal information on Weibo, because it could be used in a way I did not foresee.</td>
</tr>
<tr>
<td>Self-protective behavior (Mean=4.44, Std.Dev=1.29)</td>
<td>I do not use my real name as my Weibo nickname. I changed the default privacy setting of Weibo. I deleted some of my tweets to restrict others from reading/viewing them. I provided some fake or inaccurate personal information. I never mention anything on Weibo that others could identify me.</td>
</tr>
</tbody>
</table>