Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries
DOI: 10.54254/2753-7048/14/20230924

Credibility, Privacy Concerns, Self-exposure, Engagement & Social Media: Discussion on I.P. Address Disclosure

Wenxin Tong[1,a,*]

[1]*Communication College, Boston University, MA, United States*
a. totwx@bu.edu
**corresponding author*

Abstract: This work is based on the current social media and Internet situation in China. Starting from 2022, China request all the social media platform to show I.P address for individual users. The exposure of IP address in China is inevitable, however, the author would like to see what will happen if this happens in another country. When TikTok is targeting a more international market, how will this exposure behavior influence user's action or habits? What kind of negative effects will exert on TikTok? How will the exposure of privacy correlate with users' behaviors? By conducting questionnaire in College students, the result shows people take privacy as a large portion of using an app but with limitations. Exposure of privacy is an important element, but as long as users build habits on the app, it will not affect users on a large scale. Credibility, Privacy, self-exposure, and engagement rate are all slightly influenced by the exposure of I.P address.

Keywords: IP address, TikTok, privacy

1. Introduction

An estimated 26% of U.S. adults under 30 get news regularly from TikTok, one of the most popular social media sites among young adults [1]. TikTok establishing itself as one of the top social media in the US mirrors the Chinese social media landscape where Douyin, the Chinese version of TikTok, has gained more than 400 million active daily users by January 2020.

TikTok, as a short video-sharing social media platform, is similar to its counterparts in encouraging content creation and building an online forum for public interactions. Such online communication allows users to interact with each other without necessarily disclosing personal information like names, ages, and locations.

Taking advantage of the natural experiment of a new feature on TikTok China, which mandatorily discloses all user's IP addresses since April 2022, people examine the relationship between IP address disclosure and the impacted users' engagement behaviors on TikTok. Specifically, the study proposes source credibility, users' privacy concerns, and self-exposure as three predictors and evaluates their predictive effects in determining users' engagement behaviors on TikTok. This research can shed light on the implication of disclosing IP addresses for policymakers and UX design practitioners in ByteDance, Ltd., the company that owns and operates TikTok.

DOI: 10.54254/2753-7048/14/20230924

2. Literature Review

2.1. Social Media Credibility

Credibility is an important source characteristic but not simply inherent to the source itself [2]. As McCroskey defined credibility as "the attitude toward a source of communication held at a given time by a receiver," it is a perception of, and judgment made by audiences regarding the source's believability, accuracy, and fairness [3]. Credibility is also a broad construct in communication and persuasion, among which expertise and trustworthiness are two of the most common dimensions [3]. A meta-analysis performed by Wilson and Sherrell indicated that while expertise leads to the largest attitude and behavioral changes, source manipulation exerts a small but consistent effect. In the extensive literature on credibility in the context of social media, researchers found that the distinctions among the nature of different social media sites can lead to different perceived credibility. While Facebook, Twitter, and TikTok are all examples of social media, the perceived credibility of Twitter differs from Facebook in the sense that the author's identity that indicates authority is not salient, leaving the burden of determining credibility on users [4]. Therefore, Twitter is perceived as less credible compared to Facebook and blogs [5]. There is also consensus that the assessment of credibility can be either objective, scrutiny of information quality, or subjective, relying on the perception of trustworthiness, expertise, attractiveness, and other source factors [6]. Either objective or subjective credibility assessment pertains to the Elaboration Likelihood Model (ELM), in which one's motivation and ability determine whether the information is processed centrally or peripherally [7]. Since social media, especially TikTok, are generally for entertainment purposes, users tend to take the peripheral route where the heuristic principle prevails [7]. Social locations, defined as "the location in time and space in a network of social relationships, is such heuristic cue that can impact credibility as an information quality factor [8]. When isolating the effect of location on credibility from the broader concept of social location, researchers found a positive relationship between users' perceived credibility and tweets that include event location [9]. As TikTok China took the lead in revealing its users' IP addresses, adding salient location tags next to their profiles, posts, and comments, it is unknown that such a relationship will still stand up when applying to TikTok.

2.2. Social Media Credibility and User Engagement

Blumler and Katz contend that users actively consume media content that best gratifies their needs. In the era of the explosive growth of online mis/disinformation, users' perceived source credibility becomes a crucial motivation for using social media because credibility and information quality are often positively related.

Studies find conflicting sequences regarding credibility and gratification. One was that gratification predicts credibility; another study suggested credibility predicts gratification [10]. However, a recent study found a strong predictive influence of credibility on motivations for using Twitter, which corresponds to the latter sequence [10]. As opposed to traditional media, social media like TikTok focuses not only on users' content consumption but also puts a heavy weight on their engagement behaviors. While engagement is a fragmentarily defined concept because of different conceptualizations across different contexts, in the context of social media, the behavioral dimension of public engagement prevails in existing research, which is often operationalized as practices including posting, liking, sharing, and commenting. As there are few studies examining such predictive influence of credibility on TikTok users' engagement behaviors, this study proposes the following hypothesis:

H1: The I.P. address disclosure will predict more user engagement in terms of posting, liking, and commenting.

DOI: 10.54254/2753-7048/14/20230924

2.3. Privacy and Social Media Engagement

In a social mobile era, information privacy is defined as one's ability to control what and when information can be released to the public. Internet development with social and mobile technologies of the last decade have significantly raised unprecedented issues regarding the degree of user engagement because of privacy violation by institutions. Thus, privacy concern, and worries about revealing one's personal information without permission to other parties, causes users' discontinuous usage behaviors.

Studies have shown that users will limit their engagement in some social media (e.g., Venmo) because every user activity might reveal personal information, such as transaction amounts, time, location, friends, and activities involved. They worry about information misuse by the social media platform, third parties, and other users who can see the information. In another study concerning Facebook, Facebook users are more likely to browse than actively posting and sharing information. Therefore, the following hypothesis is formulated:

H2: Privacy concerns regarding I.P. address disclosure will decrease user engagement.

2.4. Self-exposure and Social Media Engagement

Self-exposure is "the act of revealing personal information to others". It is an intentional act and fulfills one's needs for belonging and social connectedness. Self-disclosure can occur in interactions with strangers or close ones. People are most comfortable sharing information with either a stranger or a trusted person.

Based on this theory, studies have found that although social media users could share personal information within a selected group of recipients via group chat, private message, and close friends list, many of them still publicly share information on social media, reaching out to a wider range of audiences. People with the self-disclosive characteristic are more likely to share personal information in a public situation, and information disclosure would not concern them. Therefore, this study proposes the following hypothesis:

H3: The I.P. address disclosure will positively increase user engagement.

3. Research Methods

3.1. Research Objects

The study population is Boston University students currently using TikTok or Dou Yin. The author chooses this population because university students are the most active social media group. Thus, they could represent most users and express their ideas towards IP address exposure problems more effectively.

3.2. Research Technique

The sampling technique the author used is a certain sample because the author took what I could find to post my surveys. Another technique used is snowball sampling because author sent out the surveys and friends helped me send them to their friends, and the cycle continued. Techniques are also voluntary because the author cannot force anyone to do the survey but just send them into the group chat, and the population decides whether they want to participate.

The survey was sent out and author received 112 responses, with 60 effective and truthful responses on average for each question.

DOI: 10.54254/2753-7048/14/20230924

3.3. Research Procedure

The author first sent out the survey to friends individually because these friends will answer my survey carefully as they are close friends and understand the importance of the survey. Then, the author posted the survey link into the huge group chat. The author uses interactive and engaging wording and money to attract people to complete the survey. With the money they receive, they will answer the survey seriously and honestly. The questionnaire is divided into eight parts: the consent form, familiarity and frequency of using Tik Tok, assuming IP address exposure situation in Tik Tok, the independent variable of privacy, the independent variable of self-exposure, the independent variable of credibility, the dependent variable of uninstalled, and personal information.

After participants choose "I consent," they will answer questions about how often they use Tiktok, comment, and post on Tiktok. This could help to identify the response that said they never use Tiktok. The author needs to separate this group from people who are using Tik Tok really often because the author wants to continuously attract new users while retaining current users. Then the survey offers a situation of what it will be like to expose IP addresses while using Tiktok for the participants to understand the situation.

The author asks for privacy in the next part. For privacy, the author wants to investigate how much the participants treasure their privacy and to what extent they felt violated. By offering the Likert chart, the responders will rate their feelings depending on the situation. Self-exposure is another influential element because the author wants to know whether the participants have already done similar things, like providing and sharing their IP addresses on the platform. Then the author asked the participants whether they thought showing IP addresses could increase the credibility of the poster and also the platform. Last but not least, the author adds a separate part directly asking participants about their overall opinion. Engagement is one of the most important things for research, as the author want to keep and retain users. Finally, the author includes the personal information part for potential future investigation and research.

3.4. Variable

In this survey, the goal is to testify under what situations and conditions users will influence the engagement rate for users on TikTok. The dependent variable in the experiment is the engagement rate. The first dependent variable is Privacy concerns. In question 6, the author used the Likert scale to see how people measure the importance of privacy in different aspects. For example, the author wants to see how people value the control of personal information. "Being in control of who can get information about you" focuses on people's rights and willingness to show personal IP addresses and who the people have access to see it. Using the Likert scale for this question, the author could measure to what extent people are willing to show their privacy. Thus, the author could use linear regression to analyze the relationship between privacy and engagement. The second variable is self-exposure to the app. As more personal information (including IP address) is exposed on the app, people tend to rely on the app. Self-exposure will be measured by questions seven and question eight. Question seven is a multiple-choice question in which users choose what kind of information they are willing to expose on the internet spontaneously. By giving out information, the author has data to see how and what private information people value the most. If TikTok exposes more personal information against people's willingness, the engagement rate will be affected. The third variable is credibility. There is a certain possibility that with personal information, such as IP address, being exposed on the app, users will tend to add credibility to some information or content on the app. With credible information on the app, people are less likely to install the app. Questions nine and ten will measure credibility.

DOI: 10.54254/2753-7048/14/20230924

3.5. Linear Regression

Linear regression is able to estimate the relationship between one DV and multiple Ivs. Thus, in this study, the author decided to use linear regression to help interpret the result and relationship between three independent variables and one dependent variable. The first independent variable is privacy concerns (Question 6). Since it is a Likert chart. The author has to compute the average for each question and evaluate general privacy depending on each question's average. For question 7, since the author asked participants to click all information that they shared online, the author could set each element as 1 and add the number up. For example, if they shared "name" and "email address" through Tiktok, their self-exposure level will be noted as 2. Question 8 also evaluates self-exposure, and the author could use the question results from itself since it is a single question and could be considered as one of the variables for a later final evaluation of the dependent variable. Similar to question 8, question 9 and 10 are also the questions that could be taken into account in the final results directly. Moreover, for engagement, the author needs to transform the question data into 1 to 5 for later calculation. After the author get all the separate data, the author calculates the linear regression to see the relationship between independent variables and dependent variables.

4. Results

The author conducted separately for each element in question 6. The author has 57 effective answers for the first element. The author identified "Very Important" as 4, "Somewhat Important" as 3, "Not Very Important" as 2, "Not at all Important" as 1, and "Don't know/doesn't apply" as 0. Participants' attitudes towards being in control of who can get information about them are generally negative. With four as the maximum level and two as the minimum level, the average for this segment is 3.42, which is considered a high average. For the question "Not having someone watch you or listen to you without your permission," our participants also show negative about it with a maximum of 4, minimum of 1 and a 3.40 average. For questions about "controlling what information is collected about you," the average is 3.25, with a maximum of 4 and a minimum of 1. The average for the segment of "having individuals in social and work situations do not ask you things that are highly personal" is 3.31, with a maximum of 4 and minimum of 1. "Not being monitored at work/school" results in an average of 3.24, with maximum four and minimum 1. The average for "being able to go around in public without always being identified" is slightly lower, 3.18, with a maximum of 4 and a minimum of 1. Since we record "Don't know/doesn't apply" as 0 and clean the data from the answers, our maximum value is 4. Our conclusion on privacy concerns is that people care a lot about their privacy in general and value privacy in different situations in real life and through the internet.

For question 7, the author investigated self-exposure and collected 68 effective responses. The author set one element as 1. If the participants click two things, they shared through Tiktok, the number will be recorded as 2. The numeric data for self-exposure indicates that people generally share one or less information on Tiktok. Since it is skewed left, people tend to share less and less information on Tiktok. Thus, the self-exposure rate is generally low.

For question 12 about engagement, the author cleaned the data and recorded it into one representing "definitely no," 2 representing "probably no," 3 as "netural," 4 as "probably yes," and five as "definitely yes." Most participants think they will probably engage less or act neutral depending on the situation. people would generally engage less on Tiktok due to IP exposure.

The final result Is to see the relationship between independent variables and one dependent variable. The P value for privacy concern is 0.095 which is smaller than 0.1. This is stating that IV (Privacy concern) and the DV shows a relatively strong relationship. The independent variable privacy concern increases 1, then engagement rate averagely decreases by 0.387. The second IV is self-exposure. The p-value for self-exposure is 0.529, which is larger than 0.05. This proves that IV

DOI: 10.54254/2753-7048/14/20230924

and DV show a weak relationship. Meanwhile, as self-exposure increases by 1, the engagement rate will averagely decrease by 0.047. Question 8 also measures self-exposure. The p-value of question 8 is 0.08, which is smaller than 0.1. This represents that self-exposure and engagement rate has a very strong relationship. As self-exposure increases by 1, the engagement rate will also increase by 0.162. The third variable is credibility. Both Questions 9 and 10 measure the credibility of TikTok. In question 9, the p-value is less than 0.001. This indicates that there is a very strong relationship between credibility and engagement rate. It can also see if the credibility of TikTok grows by 1, the engagement rate will decrease by 0.311. Question 10 has a P-value of 0.904, which is larger than 0.1. This indicates that there is a weak relationship between the credibility of the author's content if showing their IP address and the engagement rate. If the credibility increases by 1, the engagement rate will also increase by 0.015.

If R2 shows 1, the regression explains all of the variability. The linear regression model for this survey, the R2 for this linear regression is 0.416. This represents that the regression explains 41.6% of the variabilities.

5. Discussions

The study uses privacy concerns, social media credibility, and self-exposure as the iVs of the research question to explore how social media platforms display IP addresses to affect user engagement. According to the results and analysis of the questionnaire, the user's privacy concern showed a correlation of -0.387 with a p-value of 0.095. It means that the privacy concern makes the public considerably reduce their engagement on social media after the platform exposes the user's IP address. Social media credibility as the second IV reveals that people believe that IP addresses can increase the overall trustworthiness of the media platform by increasing the author's credibility. Through the results, the research shows that the public's trust in the current Tiktok is very low. With a p-value of 0.94, the TikTok platform can increase user credibility and social media participation to a small extent by exposing the user's IP address. For self-exposure, according to the data, the respondents have a high acceptance of self-exposure, so it will not affect the user's participation in social media.

Forcibly exposing user' IP addresses will undoubtedly violate their privacy. Exploring the impact of privacy concerns on social media engagement is critical for deciding whether to display user IP addresses on social media platforms. According to the questionnaire survey, the regression relationship between privacy concern and social media engagement is -0.387 with a p-value of 0.095. Therefore, privacy concerns and social media engagement are strongly negatively correlated. In other words, social media engagement will be greatly reduced when users have strong privacy concerns. Based on the literature, privacy concerns regarding I.P. address disclosure will decrease user engagement. In short, the Privacy concern will cause the TikTok platform, which forcibly exposes the user's IP address, to lose a lot of user engagement.

According to the questionnaire data, respondents have a negative attitude toward the content and source credibility of social media platforms. Due to the impact of COVID-19 on the social media environment and misinformation, many media platforms cannot build a trusting relationship with users. Media platforms are currently working hard to re-establish the trust relationship with users. a user's perceived source credibility, then, becomes a crucial motivation for using social media because credibility and information quality are often positively related. IP Addresses of users could improve the source credibility of platform content. Based on the regression between the source credibility and social engagement, the data of 0.15 indicates that improving the source credibility through the IP address can increase the user's social engagement to a small extent.

Due to the rapid development of social media and the demand for personalized content, social media collects many personal identities. Through the integration of user information between different platforms, people voluntarily publish more and more personal information on the Internet.

DOI: 10.54254/2753-7048/14/20230924

Therefore, the public has fewer and fewer thresholds and concerns about self-exposure. Self-exposure: People with disclosure characteristics are more likely to share personal information in a public situation, and information disclosure would not be a concern to them. The TikTok platform allows more users to become authors and has user content generated. Therefore, users of the TikTok platform will have a higher degree of self-exposure in order to establish more connections with the platform and community. According to the questionnaire survey, participants also indicated that the degree of self-exposure will not affect the social media participation of movie users.

6. Conclusion

In conclusion, according to the hypothesis, the conclusion of the study is that the TikTok platform forcibly exposing users' IP addresses will reduce social media engagement. Although IP addresses can help platforms increase source credibility and thus increase user' social media engagement, privacy concerns have a greater impact on social media engagement based on static data from questionnaires. IP addresses have been used by many social media platforms to push personalized content for users to increase engagement. However, the public is still very resistant to exposing the IP address. More social media platforms tend to increase user social media engagement by increasing content credibility. Future research directions will be dedicated to studying the relationship between personal content credibility and social media engagement.

References

[1] *Berlo, D. K., Lemert, J. B., & Mertz, R. J. (1969). Dimensions for evaluating the acceptability of message sources. Public Opinion Quarterly, 33(4), 563.*
[2] *Gaziano, C., & McGrath, K. (1986). Measuring the concept of credibility. Journalism Quarterly, 63(3), 451–462.*
[3] *McCroskey, J. C., & Teven, J. J. (1999). Goodwill: A reexamination of the construct and its measurement. Communication Monographs, 66(1), 90–103.*
[4] *Kaye, B. K., & Johnson, T. J. (2004). A web for all reasons: Uses and gratifications of internet components for political information. Telematics and Informatics, 21(3), 197–223.*
[5] *Freeman, K. S., & Spyridakis, J. H. (2009). Effect of contact information on the credibility of online health information. IEEE Transactions on Professional Communication, 52(2), 152–166.*
[6] *Petty, R. E., & Cacioppo, J. T. (1986). Communication and persuasion: Central and peripheral routes to Attitude Change. Springer.*
[7] *Kaye, B. K., & Johnson, T. J. (2016). Strengthening the core. Electronic News, 11(3), 145–165.*
[8] *Wathen, C. N., & Burkell, J. (2002). Believe it or not: Factors influencing credibility on the web. Journal of the American Society for Information Science and Technology, 53(2), 134– 144.*
[9] *Aladhadh, S., Zhang, X., & Sanderson, M. (2014). Tweet author location impacts on tweet credibility. Proceedings of the 2014 Australasian Document Computing Symposium on–- ADCS''14.*
[10] *Johnson, T. J., & Kaye, B. K. (2014). Credibility of social network sites for political information among politically interested internet users. Journal of Computer-Mediated Communication, 19(4), 957–974.*