Privacy Protection Analysis of Privacy Paradox on Social Media

Liu Tingyao and Dzaa Imma Abdul Latiff

Faculty of Communication and Media Studies Universiti Teknologi MARA, Shah Alam,
Malaysia
Email: 2021954663@student.uitm.edu.my
Corresponding Author's Email: dzaa17@uitm.edu.my

Abstract
Social media, modern information, and communication approach has created a platform for people to communicate and acquire information with close contact and a large amount of information, shaping a new form of interpersonal communication. However, there are growing public concerns about the privacy leak caused by social media, and the ensuing privacy paradox problem occurs one after another. Based on this definition of privacy in social scenarios, the research finds that the phenomenon of privacy paradox is related to self-disclosure psychology, privacy concern, and risk perception in the process of using social software, such as weibo, facetime, weixin, etc. And then from the perspective of users, the privacy paradox in this paper analyzes the current dilemma such as the contradiction between public and private boundaries, the contradiction between digital memory and deletion, the contradiction between communication situation and social identity, the contradiction between perceived risk and interest impact, and puts forward some suggestions on privacy protection in social media at the end of the article. It is hoped that it can serve as a reference for social media privacy protection work.
Keywords: Social Media, Privacy Paradox, Self-Disclosure, Privacy Protection.

Introduction
At present, social media has become the main means of instant communication between people, and the main body that generates and disseminates social media traffic has changed from others to social media users themselves. However, due to the low threshold and zero filtering mechanism of social media, there are many anomalies in the process of information dissemination. Taking Uniqlo's "July 14" video event in 2015 as an example. First, users actively diffused personal privacy information of the parties concerned, and secondly, the secondary diffusion through others led to larger uncontrollable diffusion, eventually leading to adverse social influence. The growing privacy leaks aggravate users' concerns about privacy. However, users are willing to share things about themselves on social platforms. The conflict between this privacy attitude and sharing behavior is called "privacy paradox". At present, social network has developed into a gathering place for information dissemination,

sharing, and search, but it also intensifies the expansion and generalization of the privacy paradox.

Problem Statement

With the popularity of social media, more and more people begin to use social media to share their lives, communicate with others and so on. As a result, incidents of personal information disclosure, illegal access and privacy infringement targeting social media users are increasing year by year. When we share our photos, our lives and even our privacy on social platforms, we need to be very careful. In daily life, personal information security problems caused by privacy disclosure emerge one after another. For example, in September 2018, Facebook discovered a security breach on its platform. Hackers could use the flaw to steal login codes, about 50 million of which were stolen. Thus, we must pay attention to the protection of privacy when using social media.

Study Motivation

With the development of big data and algorithms, privacy has become a global problem. It not only threatens the safety of personal property, but also has a great impact on the safety of human life. Therefore, in order to better safeguard the control of personal privacy and information security, it is necessary to enhance the awareness and ability of privacy protection from the perspective of personal behavior, so that users can enhance their awareness of privacy protection. This research needs to analyze and study the current privacy disclosure problem, so as to propose a feasible scheme to guide individuals to protect privacy, enhance the privacy protection awareness of social media users, create a safe social network environment, and protect users' personal information.

The research on implicit contradiction originated in the west. Spiekermann and Brown found in a 2001 study that although Internet users are very concerned about privacy leaks and privacy security issues on social media, in many cases they still choose to actively disclose their private information. This finding is inconsistent with our belief that, in our view, if a problem is detected, our privacy protection requirements will become higher, causing us to share and disclose personal information more carefully, but this also becomes a negative privacy attitude. The logical dislocation between active privacy disclosure behaviors is also a phenomenon of privacy paradox. Therefore, the researchers called the phenomenon that in social media, users still publish personal information online even though they are worried about the possibility of information leakage, which is called the privacy paradox.

Privacy Paradox

The paradox of "privacy" is put forward by the American scholar Susan Boehner, for the first time in 2006. In the research on user privacy attitudes and behavior, she found that people's concerns over privacy often present a kind of contradiction. On the one hand, users claim very much care about their privacy. Meanwhile, with little protection of personal information, it constantly gets leaked out. The so-called privacy paradox is the disconnect between privacy attitudes and actual behavior on social media.

With the rapid development of Internet information technology, social media, a content production platform based on user relations, has also developed rapidly and gradually become an indispensable part of daily life. As more and more users' personal information is made public through social media, the requirement of protecting users' privacy information

becomes more and more prominent. Internet survey data show that about 10,000 Internet users are worried about the leakage of private information, but users still post their personal information through social media. This contradictory phenomenon is the "privacy paradox".

Factors Influencing the Privacy Paradox on Social Media
a) Self-disclosure
Self-disclosure, originally a term used in psychology, expresses the process of honestly sharing one's private thoughts and feelings with others. Before the age of big data, self-disclosure is roughly divided into two categories: a kind is a person's will or ability, and the other kind in the process of social interaction or in certain scenarios. Therefore, people's performance to others should be considered according to the real situation as well as the relationship to consider, but a network of mimicry environment makes self-disclosure also appeared some new features: First, the content they post content tends to be more diversified. It includes gender, hobbies, birthplace, basic personal information such as phone number, and the user's location, photos, video, attitudes, and so on deeper private content. the absence of gatekeepers. The details of sensitive information and the lack of awareness of distinguishing are important factors of privacy for ordinary users; Secondly, compared with traditional interpersonal communication, people will reveal themselves more on the Internet. The anonymity and lack of visual cues of social platforms enable users to present their real selves, intentionally created selves, and even virtual selves to each other to obtain psychological recognition or satisfaction that cannot be obtained in reality (Linying, 2008)
Overall, the social media era self-disclosure is interpersonal relationships, the external environment, individual rationality, and multiple factors such as awareness of privacy protection constraints, but no matter what extent, how self-disclosure reflects user and through the information exchange of positive social behavior maintains the social relations and strong viscosity, which explains the paradox of privacy reason causes.

b) Privacy Concerns
Research on privacy attention in the social media environment mainly focuses on measuring users' cognition and attention to illegal disclosure and use of private information. Users with privacy concerns will take different protection measures due to individual differences, which has been proved by a large number of studies. For example, factors such as the user's age, gender, educational background, and Internet experience have different effects on privacy concerns. Social software trust and attitude have a certain impact on users. The trust factor is considered the antecedent variable of privacy concerns. Some scholars have conducted questionnaires and data mining on WeChat usage of college students in China and found that college students with higher privacy concerns are more inclined to implement privacy protection behavior. However, in the increasingly obvious privacy paradox, some scholars have found that there is no direct link between the level of privacy concern and self-disclosure (Xiaoxing, 2021). A survey on American college students using Facebook found that they would automatically create an account with a large number of personal information and will not show the degree of privacy concerns about differences in self-disclosure, and at the same time, a study shows a lot of people, who are concerned about privacy tend to show a strong consciousness, but in actual operation unable to reflect the proper measures. The underlying explanation for this is that human behavior is constrained by bounded rationality. When the

specific social environment affects rationality, privacy is ignored, which is the external factor causing the privacy paradox.

c) Risk Perception

The evaluation of Gains and losses affects people's perception of risk and imitation. When the benefit is greater than the risk, the protection measures and protection consciousness will decline. One reason for the high-risk perception is that everyone knows the harm caused by privacy disclosure but feels that privacy violation happens to others rather than to them. This existential psychological communication is called the "third-party effect"（Clinton Joseph Davission, 1983）. Risk perception lag, another reason is the widespread perception among users that Internet security cannot be trusted, therefore it is basic in the protection of privacy protection, such as modifying the login password and setting access, user privacy leak will pay more attention to the news events and more privacy protection measures are taken in the social platform, Such as using anti-virus software to clean your computer's cookies, checking websites about privacy policies and regularly asking for fee records. The consequence of low sensitivity is that the risk perceived by social users only lasts for a short time, and the long-term harm caused by privacy disclosure cannot be foreseen in advance. Even, it cannot be counted as privacy disclosure as long as personal property is not lost.

The phenomenon above is particularly prominent among the youth. Represented by the network generation, they show completely different characteristics from their parents' group, that is, they pursue individuality, are willing to show themselves, are eager to be recognized, and pursue a new wave of web applications. When vanity is satisfied or interest needs override privacy concerns, privacy protection will be in the last place.

5. Privacy Protection Dilemma based on Privacy Paradox
a) The boundary contradiction between "public" and "private"
Communication Privacy Management Theory (CPM) holds that private owners should draw boundaries for private information, and the free flow of information depends on the opening and closing of boundaries. Today's boundary division has become blurred with the expansion of media and technology, because "traditional privacy issues are mainly about the separation of private, sensitive and non-public personal information in the private domain, while new privacy issues are mainly about sharing, which is inherently insensitive and the separation of personal information in the public domain"(Gen, 2020). Compared with traditional privacy issues, semi-public information definition is on the rise of Internet privacy, and control, issues still need to explore, beyond the space limitations of big data technology to achieve the information release. Many people share storage in different virtual time-space cloud storage, which also makes the connection between the public-private boundaries by separating into overlapping each other at the beginning. In the era of big data, the segmentation between public and private boundaries eventually leads to a change in individuals' self-control over information.

Boundaries between "public" and "private" are fuzzy in that it's hard to tell if a user's post is part of the public or private domain. such as WeChat itself is a public social networking platform, voluntarily users to share personal information in "Moments" and this field is the public domain, WeChat users can also set up "visible to certain groups of friends only" to share different content, this behavior is also private sector boundaries. When social media is in the middle of the public and private sectors, the traditional definition of privacy cannot

ensure the rights and interests of privacy in datalization and highlights the complexity of privacy research in the era of big data.

b) The Contradiction between digital Memory and Deletion
Once users post their personal status to the Internet for sharing, information traces will be permanently retained, and anyone can find relevant information through search engines at any time. Although it causes privacy concerns, it will also affect the level of self-disclosure of social users. In recent years, many scholars have expressed doubts and worries about digital memory on the Internet. In his book Delete, data scientist Victor Mayer-Schoenberger called for an "Internet forgetting", in which meaningful information is retained, meaningless information is deleted, and the period of information is regulated. This is hailed as the choice and the virtue of forgetting in the era of big data. Facebook, Twitter, and other social media giants can wipe out any trace of minors using them, so they don't get into personal or work-related trouble because of a lack of cyber awareness, according to the "eraser" law signed by the state of California on September 23, 2013. Although the scope of protection of the law is limited and raw data does not disappear completely on the server, it is the world's first law specifically aimed at minors on online privacy, marking the rights of freedom and control game.

c) The Contradiction between Social Identity and Communication Situation
The individual's social status and the communication context affect self-disclosure, and the appropriate context plays a key role in privacy. The dramaturgy theory put forward by the famous American sociologist Goffman points out that an individual will design a self-image in advance and present it to others in a symbolic way. This is also true of the dramaturgy theory for online social communication. Social software provides a platform for users to show, while a virtual sharing platform is a platform to be recognized. It needs careful maintenance from individuals to make the audience see their well-designed personal image. But in real life backstage, covering up those who do not need to perform the link or others feel not easy to accept the picture, feelings, and opinions hidden in the heart. Virtual social platforms cannot be synonymous with real life, nor can they portray every person in time. Because it is not limited by time and space, users have to figure out how long it will take to send a state to be more easily accepted by others, and what language to use to convey their thoughts, etc., before posting a state. This backward process is also a process of self-image design for users. When the front desk is inverted from the background, it brings adverse consequences to individuals. Social media users usually reveal their individual identities and value orientation. When they share, leaving a stereotype about a certain major or a certain age for a long time. Once it is reversed, especially the positive image is overturned, it is difficult to be recognized by the outside world. Individuals will repeatedly speculate about the status when they publish it, and even publish the contents against their will in order to maintain interpersonal relations. True or false self-disclosure will also have a judgment impact on the privacy paradox behavior.

d) The Contradiction between Perceived Risk and Benefit Influence
Social media can be a double-edged sword. Everyone has the safety value evaluation. In the case of high risk, to avoid risk will inevitably give up income, risk, and income coexist, in order to obtain income has to take a high risk. For example, in the process of using WeChat, if you want the convenience of the mini program, you need to agree with Applet of Wechat to

obtain personal information; if you want the support of many people, you need to forward the voting activities. Perceived attitude and actual behavior are always in conflict with each other.

6. Suggestions on Privacy Protection Under Social Media
a) Strengthen the regulation of digital privacy
In the era of big data, excessive information has caused a variety of problems, and the requirement of legal norms for information division has become more and more urgent. The "Prism gate" incident pushed the issue of digital privacy to the climax, the United Nations also put forward a request for countries to strengthen the protection of digital privacy bill. In 2013, China issued the first personal information protection guidelines -- "Information Security Technology Public and Commercial Service Information System Personal Information Protection Guidelines", which clearly stipulates the collection and storage of personal information, but there are no special requirements for the use and release of data.
At present, Chinese network privacy laws and regulations need to be more systematic and operable. There are three problems: First, individual general information and sensitive information segmentation are insufficient in the network environment. Social users who upload personal information cannot distinguish which kind of information belongs to, and it is not clear how the dissemination of personal information in the public domain will affect personal life. Second, the scope of digital privacy and the definition of rights is not refined, especially the government and public administration of the use of personal information standards need to be strengthened. Most of the existing laws regulate the behavior of Internet service providers and users, and there is still no way to constrain the government and public administrative agencies. Third, there is lacking authoritative network information management institutions and a wide variety of social media. Take China as an example, instant messaging is dominated by WeChat and QQ, community Q&A is dominated by Zhihu and Douban, shopping consumption is dominated by Taobao and Jingdong, and video sharing is dominated by Meipai. Users need different social software due to the functional differences of social software. In this regard, there is the problem of user information matching. Information overload not only causes unnecessary waste of human and material resources on the website but also increases the possibility and way of personal information leakage with each registration. Therefore, the establishment of an authoritative information management organization contributes to reduce the waste of resources, but also purifies the user's personal information utilization channel at the source, so as to avoid the misuse of personal information by criminals.

b) Balance the Control of Personal Data
Personal privacy is uploaded to social networks by users. It seems that users have great power and control over the information initiative, but in fact, it is controlled by service providers. After the personal information is uploaded to the network, an individual can no longer control its spread and spread. Even after you delete it and the post turns invisible to you, the relevant information is still left in the Cookie of the server. To solve the problem thoroughly is the control of privacy information by network service providers. Information subjects can only passively accept that their privacy is controlled by service providers and expect themselves to rationally use and respect their personal data and information in accordance with industry norms. In case of any problem, privacy may be violated at any time.

For the control of personal data, it is necessary to achieve two goals: one is to rationally allocate the control of personal information and increase the processing of personal information of social media users. For example, you should have the right to request deletion of personal information registered on the website, the right to set the duration of information storage, the right to obtain notice and the right to license and consent in the process of personal information collection. Second, service providers should not only be regulated by industry standards, but also earnestly implement the responsibility of protecting users' privacy, strengthen the privacy setting function and privacy information reminder service. For example, when location services are used, service providers should inform users of which applications can share their location information, warn users of the dangers of some functions sharing their location, and set location requirements for authorized strangers. Each of these functions is further unraveling the dominance of personal data.

c) Building Appropriate Reasonable Expectations of Privacy
Public domain privacy can be divided into two categories: space privacy and information privacy. The so-called space privacy refers to the right of the user in the private space, his personal peace, and free activities from other people's interference; Information privacy means that personal information is forbidden to be collected, used or disclosed by others. Compared with space privacy rights, information privacy rights infringement is difficult to be confirm by quantitative means, and whether the recorded or filmed behavior in public places comes from the will of the parties is difficult to be guaranteed by law. Therefore, it is of great significance to clarify whether a specific expectation of privacy regarded as legitimate and reasonable.
The standard of reasonable expectation of privacy needs to meet two basic conditions. First, individuals should express their true feelings and expectations when protecting specific privacy. If there is no expectation, there is no harm. When the users do not think that the daily of the public and the life path known to others is privacy invasion, there is no so-called privacy leakage problem. Second, such expectations must be in line with the public interest and widely recognized by the society and the public. Only when they meet the above two requirements can they be called reasonable expectations. The standard of rational expectation of privacy breach through the inherent restrictions of the written word, extending the scope of individual privacy from the residence to the public place, and the subject of rights from the scene to the individual, paying attention to the subjective performance of individual privacy. Measures such as speeding up the introduction of reasonable expectation of privacy and bringing personal privacy in the public domain into the scope of legal protection can further clarify the boundary of Internet privacy, strengthen the respect of Internet service providers for users' privacy and enhance users' attention to their privacy.

d) Improve Users' Media Literacy
There are various reasons for privacy leakage in cyberspace. If personal information is exposed to public space, there are leakage risks. Users' and personal privacy are not controllable, as a result of secondary transmission and network technology, different legal norms such as external control, privacy, and security issues. The final analysis is social user privacy, because of positive spread risk problems, the conflict for self-disclosure and self-control, enhances the user ego to protect consciousness and media literacy is imminent.

Among them, users will disclose self-information in moderation according to the sensitivity of the content and the judgment of the disclosure object. This self-information management and control ability can not only effectively reduce the probability of privacy disclosure, but also is an important expression of media literacy. And develop the right privacy concerns to reduce the chances that privacy will be used by others. Legal protection is usually relief and compensation after the event. In order to avoid the harm caused by privacy disclosure, privacy protection measures need to be taken in advance. Only in this way can we better avoid various problems that may occur.

Conclusion
Since the birth of mobile networks, the development of social media in China is booming, and people spend more time between mobile terminals and social media. In order to ensure its better development, the solution of privacy issues has become an unavoidable problem. The phenomenon of the privacy paradox on social media is the result of a combination of various reasons. We should not treat it as a single act. We should not only raise awareness of privacy protection and change the way users treat privacy, but also make them develop correct privacy protection behaviors and prevent its occurrence in various ways.

References
Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. New Media & Society, 19, 579-596. doi:10.1177/1461444815614001.

Chaoqun, S. (2021). Study on the influencing factors of privacy paradox on Weibo Platform. 10.26991 /, dc nki. Gdllu. 2021.002306.

Wang Bowei. (2021). Social media users privacy paradox and digestion. 10.15997 / j.carol carroll nki QNJZ. 2021.16.045.

Huimin, W. (2021).Research on privacy protection of social media users in the era of big data .10.27426/d.cnki.gxtdu.2021.000540.

Xiaochen, Y. (2021). "Privacy Paradox" in Social media: A Case study of wechat Communication, Network Communication, 149-150.

Shu, Z., Junxiu, W. (2021). The Influence of Contemporary Youth's Privacy Concerns on their Privacy Protection Behavior: The Multiple Mediating Roles of Excessive Information collection and Privacy concerns. 10.26914 / Arthur c. nkihy. 2021.041903.

Xiaoxing, Z. (2021).The "Privacy Paradox" of College Students. 10.27167/d.cnki.gjinu.2020.000295.