doi: 10.29843/JCCIS.202007_(39).0006

嘗試建構一個臉書使用者的隱私風險係數：臉書使用者的態度與行為關係

江淑琳、張志堯

摘要

本研究旨在嘗試建構一個社交媒體隱私揭露的風險係數，以了解臉書使用者在網路社會中隱私揭露的的敏感程度。本研究聚焦於兩類線上隱私揭露行為（三個面向），以檢驗線上使用者看重並在乎隱私的程度。這兩類隱私分別為靜態隱私與動態隱私，前者包括使用者在臉書提供真實姓名與個人資訊，後者指的是打卡動態。問卷收集自 305 位台灣大學生，並建構出每一位受試者的隱私風險係數，高風險係數表示使用者較容易在臉書洩露個人資訊，反之則否。本研究進一步採用此係數檢測受試者對隱私的態度與行為之關係。研究發現，在靜態隱私上，受試者的態度與行為之間沒有顯著差異；不過，低風險係數的受試者較高風險係數者在乎動態隱私的揭露。隨著臉書等社交平台提供更多個人隱私設定功能，隱私風險係數相關變項將更複雜，未來當社交媒體提供更多使用者揭露隱私功能時，研究者可以本研究所發展之風險係數為基礎，加入更多變項以建構與時俱進的使用者隱私風險係數，檢測使用者態度與行為之間的關係。

⊙ 關鍵字：臉書、隱私矛盾、隱私風險係數、靜態隱私、動態隱私

⊙ 本文第一作者江淑琳為中國文化大學新聞系副教授；第二作者張志堯為法鼓文理學院人文社會學群社區再造碩士學位學程副教授。

⊙ 通訊作者為江淑琳，聯絡方式：Email ：CShulin@googlemail.com；通訊處：11114 台北市士林區華岡路 55 號大成館二樓。

⊙ 收稿日期：2018/10/30　接受日期：2019/07/08

An Exploratory Index For Facebook Users’ Privacy Concerns: The Relationship Between Attitude and Behavior

Shu-Lin Chiang, Chih-Yao Chang

Abstract

This study proposes an exploratory index of risk to privacy leakage on social media. The purpose of proposing this privacy risk index (PRI) is to understand widely people’s sensitivity toward their personal information explosion in this highly connected network society. We mainly focus on two types of online privacy disclosure with three measures and examine the extent to which online users value and concern the right of privacy: static privacy (personal information including real names, fans page the users join in), and dynamic privacy (location-tagged). Data collected from 305 university students in Taiwan who were recruited to answer the questionnaire. We measured each respondent’s PRI, and the higher score means one’s Facebook behaviors make her or him more vulnerable to online social media privacy leakage, and vice versa. Furthermore, we use PRI to examine the relationship between individuals’ attitude and their behaviors on Facebook. The results show there is no significantly different between the participants’ attitudes and behaviors toward privacy concerns in terms of disclosing their static privacy. However, lower PRI users cared more about dynamic privacy leaking than higher PRI users. In sum, the PRI is a simple but straightforward tool to assess one’s risk of online privacy leakage. As the function settings of the FB platform become more complicated, the related variables of the PRI are also more diverse. We suggest that more online privacy concerns could be melt into PRI to evaluate one’s vulnerability of privacy leaking along with the technical tools developed to collect personal information without full acknowledgment.

⊙Keywords: Facebook, Privacy Paradox, Privacy Risk Index (PRI), Static privacy, Dynamic

Privacy

⊙ The first author, Shu-Lin Chiang is an Associate Professor in Department of Journalism at Chinese Culture University. The second author, Chih-Yao Chang, is a an Associate Professor of Graduate School of Humanities and Social Sciences at Dharma Drum Institute of Liberal Arts.

⊙ Corresponding author: Shu-Lin Chiang, e-mail: cshulin@googlemail.com, address: 55, Hwa-Kang Road, Yang-Ming-Shan, Taipei , Taiwan 11114, R. O. C.

⊙ Received: 2018/10/30 Accepted: 2019/07/08

Introduction

Facebook was created more than two decades ago, becoming one of the most popular social network sites (SNSs). It was first circulated by students throughout US universities and then extended to the general public. Facebook boasted more than 2.23 billion monthly active users by the second quarters, 2018.[1] Taiwan has over 18 million users, which means that over three quarter of Taiwanese people have registered Facebook accounts, with a penetration rate of 88%.[2] With the development and design of the functions that share personal information, Facebook has attracted academia's attention to observe the privacy attitudes, and the patterns of information revelation among the younger generation (Acquisti & Gross, 2006).

Based on the past studies of online privacy and security, it would be expected that those who desire more control over their information would engage in less disclosure. Yet, researchers did not find this association between information control and less disclosure on Facebook (Christofides, Muise, & Desmarais, 2010). The existent findings show that Facebook users leave a lot of information about themselves on their webpages, but not being sensitive to their information settings nor aware of everyone has access to them (Acquisti & Gross, 2006). Ironically, when users are asked if they are concerned about their privacy on Facebook, the answer is usually positive. The contradiction that the users value privacy but still disclose their personal information is the so-called "privacy paradox" (Barnes, 2006; Norberg, Horne, & Horne, 2007).

However, the "privacy paradox" seems to be too arbitrary to explain Facebook users' attitudes and behavior. Scholars (boyd & Hargittai, 2010) used longitudinal data and found that there were significant increases in the frequency with which users modified Facebook's settings between 2009 and 2010, as users perceived online privacy issues. An incomplete notion of privacy in the context of Facebook may be responsible for the aforementioned perceived "privacy paradox" (Raynes-Goldie, 2011). Thus, researchers may need to delineate

[1] Source: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[2] Source: https://www.internetworldstats.com/stats3.htm

nuanced privacy-related activities under the big umbrella of "privacy" along with the ongoing development of disclosure tools on Facebook.

Our research is inspired by the idea of "personalization technology," which divided Facebook activities into three dimensions— social-based personalization, behavioral profiling, and location-based personalization (Toch, Wang, & Cranor, 2012). The research also draws on the variables adopted in Acquisti, Brantimarte, and Loewenstein (2015) while discussing users' disclosure behaviors in online media and the trend users defaulting profile settings over time. In Toch and his colleague's research, they proposed three dimensions of personalization in Facebook—social-based personalization, behavioral profiling & data aggregation, and location-based personalization. These two insightful research findings also remind us that privacy concerns are context-dependent. Thus, we modify and further adopt five variables—real names, personal information, joining fan pages (static privacy), photo tag, and check-in (dynamic privacy)—to assess Facebook users' reconstruction of "privacy." More detailed explanations of the variables tested in the research will be provided later in the "Methodology" section.

The main research question in this study is: Is any consistency between Facebook users' attitudes and actual behaviors on privacy concerns? In order to answer this question, we first operationalize two types of "privacy" on Facebook, static privacy (personal information including real names, joining fan pages) and dynamic privacy (location-tagged) to investigate the "privacy paradox" phenomenon that has been proposed in existing Facebook research literature. The static privacy refers to use real names in Facebook registration to provide addresses, mobile numbers, joining fan pages, and so forth. While the dynamic privacy one is about the activities of "location check-in." We argue that the inconsistency between attitude and behavior on privacy is personal profiles left on Facebook while Facebook users should concern and protect their privacy in terms of activity tracks consistently. Specifically, in this study, we intend to present a nuanced explanation of the "privacy paradox" going beyond the common understanding "users say they are worried, but they don't care."

Literature Review

At present, the literature on social media privacy has a wide range of topics, which can be roughly divided into two perspectives. One is from a macroscopic point of view to look at the privacy protection of users from national or regional institutions (Raynes-Goldie, 2010; Marsoof, 2011; Romanou, 2018), such as the EU General Data Protection Regulation (GDPR) to protect the privacy of users (Aysem & Mehemt Bilal, 2017). In this case, user privacy is an object protected by national laws and platforms. The other is from the microscopic point of view to believe that the user can decide which personal information to be disclosed and who can or cannot see this disclosed information (Child, Haridakis, & Petronoi, 2012). That is, users have the ability to take privacy control actions, and have relative rights in privacy control. This paper is mainly based on the second perspective.

This section is divided into three parts. Since privacy is the core concept in this study, the first part will deal with the definition of privacy, including traditional and changing definitions. The second part provides a definition of privacy paradox and some examples. The third part discusses why social media users still want to disclose their personal information even if their privacy may be leaked, and synthesizes main reasons via reviewing current literature.

Privacy

Most traditional conceptions of privacy are based on the notion of privacy as total withdrawal–the right to be let alone (Norberg, Horne, & Horne, 2007), otherwise it will cause violation of privacy. With the advent of social network sites (SNSs), in particular, Facebook in this research, privacy has been a contested terrain; it is currently facing renewed and increasing challenges. Some argue that privacy within social networking sites is often not expected or is undefined (Dwyer, Hiltz, & Passerini, 2007). New media application, i.e., check-in for deals (a platform for local stores and places to offer deals to nearby Facebook users), brings along so-called "mobile privacy," and context needs to be considered while research privacy online (Hartmann, 2013). That is, in highly contextual spaces such as SNSs, privacy should be considered as a fluid process where individuals selectively control access to information about themselves by regulating their social interactions (Altman, 1975-cited from Stutzman et al., 2012). Privacy online is about being selective and optimizing access to the self (Raynes-Goldie, 2011). Researchers need to take privacy as a dynamic and dialectic process to explain the perceived changes in privacy behaviors on social networking sites (Tufekci, 2008). The existing literature reminds us that the basic challenge that privacy research faces is the combination of person, location, and activities (Hartmann, 2013).

Regarding the categories users disclose on Facebook, the existing literature (Christofides, Muise, & Desmarais, 2010) found that the majority of students disclose information such their relationship status, email address, and birthday, to an average of 297 “friends” and countless other networked connections through the site. It is also found that the majority of users provide real names, complete birthdays, and clear photo images of themselves in their profiles (Christofides, Muise, & Desmarais, 2010).

Privacy Paradox

Based on traditional privacy literature, it would be expected that those who desire more control over their information would engage in less disclosure. Yet, researchers did not find this association between information control and disclosure on Facebook (Christofides, Muise, & Desmarais, 2010). Some of the earliest work on privacy and social networking sites (SNSs) identified a disconnection between users’ privacy concerns and their disclosures on the site (Acquisti & Gross, 2006 ; Spiekermann, Korunovska, & Bauer, 2012), in what some have labeled a “privacy paradox” (Barnes, 2006). “Privacy paradox” in existing literature shows that Facebook users disclose a lot of information about themselves, and are not very aware of privacy settings or decide who can actually access to their profile (Acquisti & Gross, 2006).

Researchers found that even potential attacks are highlighted on various aspects of users’ privacy, for example, the information posted on a student’s profile may prevent that student from getting a job, enable campus police to crash that student's party (Lewis, Kaufman, & Christakis, 2008), but only a minimal percentage of users change the highly permeable privacy preferences' (Gross & Acquisti, 2005). Awareness did not increase privacy. "Even though individuals express concerns and awareness about Internet privacy, they still will intend to engage in risky online activities" (Campbell et al., 2001). The overwhelming majority of survey participants knowing that they are able to limit who views their personal information; participants did not take the initiative to protect their information (Govani & Pashley, 2005).

Why Users Disclose Privacy Online

"Privacy paradox" causes researchers' curiosity, and a great amount of literature seeks to explain this phenomenon. The point is not to ask why the users are not concerned about their privacy, but why they want to disclose and how they manage their online privacy settings and to uncover the online cultural value concerning privacy (Child & Petrinio, 2011; Osatuyi, Passerini, Ravarini, & Grandhi, 2018; Heravi, Mubarak, & Choo, 2018; Ortiz, Chih, & Tasi, 2018).

To explain this paradox existing/non-existing, a growing body of research mentions the following reasons: privacy control policy provided by FB, user's self-efficacy, and cost-profit trade-off (Birnholtz, Bruke, & Steele, 2017; Young & Quan-Haase, 2013; Chen & Chen, 2015; Chen, 2018) Facebook, unlike other online networks, offers its users very granular and powerful control on the privacy (in terms of searchability and visibility) of their personal information (Acquisti & Gross, 2006). Facebook allows substantial opportunity for computer-mediated communication (CMC) and variables in privacy management practices through the upgraded feature of status updates that took place in 2006. Users of Facebook took some strategies to protect their privacy, e.g., taking camouflage as a privacy protection strategy, aliases (Child & Petronio, 2011). The goal of using aliases is to make it difficult for people to find them via search, or to attribute their Facebook activities to heir "real" identities (Raynes-Goldie, 2010).

More recently, researchers (Chen & Chen, 2015; Chen, 2018) propose the concept of privacy self-efficacy is another concept related to privacy management, privacy concern, and self-disclosure. This concept indicates “the perception of ones’ ability to protect one’s privacy” (Chen, 2018). Since users believe in and feel confident they have the ability to control who can access their private information, they do utilize FB privacy policy to manage their profile and limit profile visibility. In this case, privacy concern does not discourage their self-disclosure.

The latest research on the privacy paradox comprehensively synthesize seven activities to ask her participant to account for the methods of “limiting profile visibility”: (a) deleting something you posted on social media, (b) editing something you posted on social media, (c) avoiding commenting on or liking other people’s posts or pictures, (d) asking someone to remove something posted about or related to you on social media, (e) asking someone to untag, (f) giving inaccurate or misleading information about yourself on social media, (g) creating differen/additional profiles on social media (Chen, 2018, p. 1401). Research shows that participants concern their privacy would limit their profile visibility, but may not influence their intention of self-disclosure. In this case, limiting profile visibility plays a mediating role in bridging the gap between privacy concerns and self-disclosure in the privacy paradox (Chen, 2018). That is, the privacy paradox may not appear while other factors mediate.

FB users are not naïve in providing their personal information without any calculations. Having a FB private profile is associated with a higher level of online social activity (Lewis, Kaufman, & Christakis, 2008), and this may bring along not only risk, but also some gratifications, such as sociability, pleasure, and social capital, etc. For FB users, they recognize privacy is a series of trade-offs as well as a collective information practice (Dourish & Anderson, 2006). SNSs facilitate and encourage mass self-reporting of everyday activities in exchange for convenience and social benefits (Raynes-Goldie, 2011). Researchers apply a theoretical privacy calculus model to suggest that “the extent to which people exercise privacy practice is based on a cost-benefit trade-off” (Chen, 2018, p. 1393; Culnan &

Armstrong, 1999; Dinev & Hart, 2006). Chen (2018) extends the privacy calculus model to consider social capital as the benefits factor and privacy concerns as the cost factor. While users weigh perceived benefit more than the risk to privacy, they would disclose more information instead of self-withdrawing from FB (Chen, 2018).

From the aforementioned, an inadequate notion of privacy in the context of Facebook may be responsible for the perceived privacy paradox (Raynes-Goldie, 2010). "Privacy paradox" seems to be too rough an idea to explain Facebook users' attitudes and behavior. Scholars (boyd & Hargittai, 2010) use longitudinal data and find that there were significant increases in the frequency with which users modified Facebook's settings between 2009 and 2010. They found that users do perceive online privacy issues. Therefore, this research proposed the need to delineate nuanced, relevant privacy-related activities under the big umbrella "privacy" along with the ongoing development of Facebook. That is, to differentiate between privacy activities. To bridge the gap in the existing literature, we try to develop an index to understand the complicated concept of privacy via a semi-constructed questionnaire. The following section will explain the methodology of how this study adopts to create an index to examine Facebook users' risks of privacy leakage.

The current study tries to answer the abovementioned questions via (1) creating an index for the individual users, and (2) applying and testing the index to examine the concerned privacy among the college students in Taiwan. We asked participants to fill in the semi-structured questionnaire including measurements of privacy. We further propose an index to investigate the relationship between participants' attitudes and behaviors. We finally discuss the reasons why the participants care or care not the private information they provide on Facebook.

Methodology

This study is conducted to further "privacy paradox" research on Facebook via (1) proposing an exploratory Privacy Risk Index (PRI) for each individual user; and (2) applying and testing this PRI to examine what are the concerns of privacy issues among college students in Taiwan. Accordingly, the hypothesis of “privacy paradox” on Facebook is to be tested.

Hypothesis: There is a negative association between privacy concerns and privacy disclosure of Facebook users.

The setting

Respondents were recruited from students who were taking courses instructed by the authors at the time of implementing this exploratory project. Since this is an exploratory study of college students’ privacy concerns on SNSs, the survey population is intended to cover this group. Moreover, a convenience sample may be suitable for preliminary research to build an index, though the results might not be properly inferred to the general population. Therefore, with the aforementioned concerns and referring to the existing literature, the authors adopted the purposive sampling method to recruit volunteers from their classes for the sake of time efficiency and budget limitation (Oliver, 2006).

A total of 307 college students completed the questionnaire. After screening out two unqualified respondents, the sample comprised 305 college students. The semi-structured questionnaire in this study was composed of four types of Facebook information, including student’s demographic and socioeconomic background, motivations to use, disclosure of personal information, activities: joining fan pages, using “location check-in” and “photo tag” functions. In addition, respondents were also asked to assess their awareness and sensitivity of privacy protection when using Facebook as the realm of their online social activities. The descriptive statistics are shown in Table 1 and present a snapshot of the whole picture of the respondents in this study.

The age range is between 19 and 27, with an average of 20.524 years. Among them, using Facebook for about two to three years is 66.55%, and for over four years, 19.35%. More specifically, 61.89% started using Facebook in high school, and 45.90% reported their main motivation was due to peer influence. Other motivations included “contact friends” (22.62%), “play games” (19.67%), and “follow friends’ updated status” (11.48%). It reflects that Facebook, as an online social site, attracts its potential users through existing users' diffusion.

As to the frequency of usage, 81.64% reported they stuck on Facebook seven days a week for an average of 3.92 hours a day. This result implies at least two phenomena: one is that using Facebook has been a common activity among college students to share and/or follow friends' updated status and information; the other is the rapid growth of smart mobile devices with Internet access which makes digital life much easier, so that online social media is heavily used, at least among the college population.

Table 1
Descriptive Statistics of Respondents

Variable name	Description	Coding	Mean (s.d.)
Age	Age in measurement occasion	Interval scale	20.524(1.299)
Grade	Grade in college	Ordinal scale:1.sophomre;2. junior;3.senior	
fb_use	Use Facebook or not	Nominal scale: 0.no;1.yes	
fb_age	Years of using Facebook	Interval scale	2.771(1.135)
fb_day	Average days of a week using Facebook	Interval scale	6.564(1.071)
fb_hour	Average hours of a day using Facebook	Interval scale	3.633(3.449)
fb_name	Sign up Facebook account with real name	Nominal scale: 0.no;1.yes	
fb_name_privacy	Degree of valuing name privacy on Facebook	5-point Likert Scale: from 1(much concerned) to 5 (less concerned)	
fb_inform	Number of personal information disclosed on Facebook	Interval scale	3.384(1.812)
fb_fanpage	Join fan pages on Facebook	Interval scale	2.793(1.298)
fb_tag	Allow friends to tag you on Facebook	Nominal scale: 0.no;1.yes	
fb_checkin	Use "check in" function on Facebook	Nominal scale: 0.no;1.yes	
PRI	Privacy Risk Index	See equation 1	
Number of cases:		307	

Note: s.d.: standard deviation

Key variables

To best capture the privacy issues on Facebook, we collect several major functions related to privacy issues as our key variables modified from the previous research (e.g., Toch, Wang, & Cranor, 2012; Acquisti, Brandimarte, & Loewenstein, 2015). They are discussed as follows.

Real name on Facebook

This variable is to measure how many respondents signed up using their real names. The original question is stated as, “Did you sign up for your Facebook account with your real name?” and it was found that 78.69% of the respondents signed up using their real names, and among them, 74.79% selected their Chinese name as their primary account name. Basically, nearly 80% of college student samples used their real names so that other Facebook users could identify them correctly if they are known by someone else, has a connection to, or is interested in.

Personal information disclosure

The questionnaire asked the respondents to check a list of personal information as to whether or not they had disclosed it on Facebook. The personal information included home address, home landline number, cellphone number, graduate school name, current school name, workplace, relationship status, email, gender, leisure habits, and birthday. It was found that the most common personal information disclosed on Facebook is the respondent’s current/previous school (about 85%), followed by workplace (52.79%), and relationship status (38.03%). On the other hand, the less common personal information disclosed is email (7.21%), home address (12.46%), and cellphone number (12.46%). Comparing the more and less common disclosed personal information, these respondents are willing to share which school they attended, where they do their part-time job, and somewhat their relationship status, while private contact information is less likely to be disclosed. It reflects an interesting observation that Facebook makes users visible among friends and their friends, which is one of the unique features of such online social sites; however, Facebook users can be active on their own social page without any unnecessary contacts. The authors found the respondents tended not to disclose their private contact information, but other social activities were acceptable; therefore, it would be interesting to ask follow-up questions or qualitative interviews about reasons of disclosure or not wanting to compare with their Facebook behaviors for a much bigger picture of their sensitivity and awareness of privacy issues on SNSs.

Joining fan pages

Respondents were asked a series of Facebook behaviors. The first one was “Which fan groups did you join?” The results showed that star fan pages (both domestic and foreign) are the most popular ones (Table 2). In addition, shopping stores are also popular among respondents (32.13%). As observed in Table 2, the types of fan pages that over 20% of the respondents joined are highly related to entertainment and fashion activities, showing that Facebook provides many opportunities for its users to follow updated news and information, as well as being able to make friends with others who have interests in common.

Table 2

Types of Respondents' Joining Facebook Fan Pages

Rank	Fan pages	%
1	Domestic stars	54.10
2	Shopping stores	32.13
3	Foreign stars	28.52
4	Music	27.54
5	Medicine	24.26
6	Magazine/news media	23.28
7	Sports	14.43
8	3C products	13.11
9	Arts & culture	12.79
10	College clubs	12.46
11	Novels	11.80
12	Restaurant	11.48
13	Tourism	9.51
14	Other entertainment	3.93
N	305	

Being tagged on photos

The second Facebook behavior is "tagging": it is to identify who is present in the Facebook photo, or to post an updated status, saying who you are with. When you or someone is tagged in a photo, the post will be visible to the viewers and friends of yours or of the tagged person. Since the purpose of the tagging feature is to share with friends not only the content of photos, but also with other people, and such behavior is of concern about the subjective willingness of being tagged when one posts a photo and tags someone they might know. Therefore, respondents were asked: "Did you ask friends not to tag you on Facebook?" and, "When someone tags you on Facebook, what is your reaction?" to measure how many respondents were concerned about the tagging feature on their photos. Table 3 presents the frequency of responses from these two questions. One of the main findings shows that 70.86% of the respondents asked not to be tagged, and about 41% showed (while they have asked not to be tagged but still being tagged) their dislike or asked friends to un-tag them after being tagged. It implies that most of the respondents tagged on Facebook photos are not really acceptable.

Table 3

Frequency of Responses toward Facebook Tagging Feature

Q: Reaction if being tagged	Q: Ask not to tag		
	No(%)	Yes(%)	Total(%)
Don’t like	4(4.54)	27(12.62)	31(10.26)
Ask to un-tag	15(17.05)	60(28.03)	75(24.83)
Just fun	20(22.73)	56(26.16)	76(25.16)
Doesn’t matter	47(53.41)	58(27.10)	105(34.76)
Others	2(2.27)	13(6.07)	15(4.96)
Total	88(100)	214(100)	302*(100)

*Three out of 305 samples were missing

Check in

Another function provided by Facebook is “check-in,” a feature like a footprint to trace where you are as described on the website. “Let people know where you've been, where you're headed for, and where you are now.” We used two questions to capture respondents’ behavior and attitude towards the “check-in” function: “Have you ever used the Facebook ‘check-in’ function?” and “Do you agree or disagree that the ‘check-in’ function causes Facebook privacy leakage?” As shown in Table 4, it was found that 52.46% of the respondents agreed that the “check-in” function causes privacy leakage, but nearly 80% still use this function. Also, for those who do not agree with the relationship between the “check-in” function and privacy leakage, up to 97% have used the “check-in” function to let people know where they are. Overall, nearly 88% of the respondents have used the “check-in” function, which shows this function is quite popular among the college student samples, even though over half of them believe it will cause privacy leakage.

Table 4

Frequency of Responses toward Facebook Check in Function

Q: Have you ever used facebook “check in” function	Q: Do you agree that “check in” function causes facebook privacy leakage		
	No	Yes	Total
NO	4	33	37
YES	141	127	268
Total	88	214	305

Privacy Risk Index (PRI)

Issues of social privacy are the focus of this study, and this topic is explored by looking at the association between Facebook users’ behavior and their privacy concerns with social networking services. As for the attitude side, three questions were asked regarding the privacy concern about the disclosure of personal information, joining fan pages, and check-in information in the survey in response to their actual behaviors on these Facebook services. The first question on respondents’ privacy concerns was, “Do you concern about personal information on Facebook being leaked?”[3], and secondly, “Do you concern about your information on fan pages being leaked?” The third question was, “Do you concern about your information on check-in being leaked?”[4] The information of respondents’ privacy concerns are crucial to understanding the extent to which users view the issues of privacy and security, and will be compared to their actual behavior on Facebook in the analysis. For the behavior side, an objective index was proposed to measure Facebook users’ risk to privacy leakage and was named the Privacy Risk Index (PRI) based upon five key variables discussed above. To calculate one’s PRI, first select key variables of Facebook behaviors and assume behavior variables have different risk ranks from high to low and are subject to change by privacy

[3] In the questionnaire, “personal information” includes “real name” and “personal profile”.

[4] In the questionnaire, the question “check-in” is composed of two subset questions “being tagged” and “check-in”.

concerns. Here, we take five users' behaviors on Facebook as experimental design and rank their level of importance to privacy according to our samples' responses. For instance, our participants mentioned that compared to other variables; real names could be most easily identifiable to the real identity. The parameters we selected are inclusive, but not an exhaustive list of privacy risk behaviors. Researchers could add and / or remove variables into the model of PRI for their customized needs. Therefore, in this study variable of a real name on Facebook is given the highest score of weighted value in this study since Internet anonymity is the first priority of privacy protection. Next, the variable "number of personal information disclosure on Facebook" is given the second-highest score of weighted value because the more personal information that is disclosed, the higher the risk of one's privacy being leaked. Then, the variable "number of fan pages are weighted in the third order," followed by variables of tagging and check-in. The order of the weight score is subject to researchers, who can pick up as many variables as they think important and necessary for calculating each participant's privacy hazard rate. In order to approximate the features of these variables, a series of fixed parameters had to be set according to a descending geometric sequence. Hence, PRI can be obtained and expressed from the equation below:

$$W_i = \exp\left(\sum_{k=1}^{K} \Gamma_k X_k\right)$$

where W_i denotes PRI of respondent *i*. X denotes the variable of Facebook behavior with numbers of k. $\Gamma \in \{\gamma_1,\gamma_2,\cdots,\gamma_k\}$, and denotes the parameters needed to estimate. The purpose of taking exponential value from the original equation is for linearization for a better model fit. The γs are estimated based upon numbers of variables selected following the law of a descending geometric sequence, written as:

$\gamma_k=(K-(k-1))/K^2$, K=1,2,⋯,k

Therefore, in this study we select five key variables of Facebook behavior to estimate

PRI and get K=5, variables include:

x_1: Sign up Facebook account with real name

x_2: Disclose user profile on Facebook

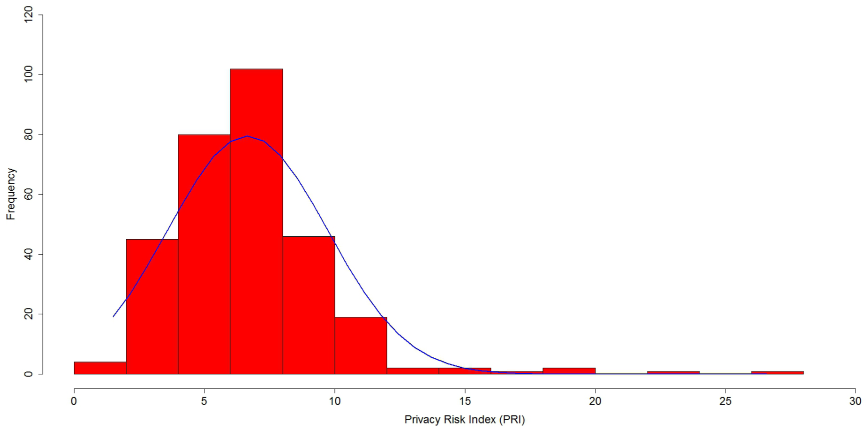
x_3: Join Facebook fan pages

x_4: allow friends to tag you on Facebook photos

x_5: Use “check in” function on Facebook

As a result, each respondent’s PRI can be estimated, and a higher value of PRI means one’s Facebook behaviors make one more vulnerable to respond to online social media privacy leakage. Obviously, a normal distribution of PRI with few outliers among respondents in this study is present (Figure 1). The descriptive statistics are as follows: the median rate is 6.554, the mean rate is 6.657 with 3.063 (s.d.), and the range is between 1.492 and 26.580. In the next section, PRI is taken as an aggregated index of one’s Facebook behaviors to compare one’s attitudes toward issues of social privacy for alternatives of redefining online social media privacy right.

Figure 1
Histogram with Normal Curve for PRI



Results

In this section, we present the preliminary statistics of the privacy risk index among our college student samples and its relations to their sense of Facebook privacy. In response to the relationship between Facebook users' vulnerability of privacy protection and their attitudes toward privacy concerns, we transform the PRI value into a categorical variable with three groups (low, middle, and high privacy risk). This is for risk evaluations purpose, as when Facebook users are classified into low, middle, and high-risk groups for privacy-concern allocation.[5] Hence, below we examine these relations by Chi-square test based upon the characteristics of our data to depict the better picture of the relationship between Facebook users' privacy concerns and their real behaviors.

PRI

As discussed above, the authors are interested in the association between Facebook users' behavior and attitude toward privacy. In the following analyses, the PRI index denotes respondent's Facebook behavior and is recoded into three categories to compare with their three privacy attitudes: low privacy risk (the 25th percentile of the PRI value and below), middle privacy risk (between the 25th percentile and the 75th percentile of the PRI value), and high privacy risk (the 75th percentile of the PRI value and above). We categorized the respondents into three groups by PRI scores to investigate whether the significant difference exists among the three PRI groups.

The measurement of privacy attitudes denotes how respondents perceive the risk of disclosing their personal information and online activities on Facebook. Our core research inquiry is how wide the gap between social media users' privacy concern and their practical risk behaviors. The privacy concerns are related to concerns about real name, personal

[5] We realize that the risk of re-categorizing the interval variable, the PRI, would probably remove the nuance we might otherwise get by leaving them as they are; however, it makes our purpose in this article clearer that privacy risk is understood at different levels not just at the subtle decimal difference and how it is related to privacy concern.

profile, fan pages, tagging, and check-in. Table 5 presents the average scores of respondents' privacy concerns about these behaviors on social media. Tables 6-8 show these results.

Table 5
Average of Privacy Concerns about Selected Facebook Behaviors

Facebook Behaviors	Average Scores of Privacy Concern[1]	n.
Real Name	.213 (.410)	305
Personal Profile	.184 (.388)	305
Fan Pages	.063 (.243)	128
Tagging	.295 (.457)	305
Check-in	.525 (.500)	305

1.Dummy variable

*standard deviation in parentheses

*regarding the original questions, please refer to Table 1.

Static Privacy (Real name and Personal information) vs. PRI

Table 6 shows about 81.63% of respondents did not concern that real name and personal information on Facebook will be leaked no matter which level of PRI they were at. One of the possible explanations for this result would be the overlap of Facebook friends and real friends, who have known the subject's real name and personal information from other sources as well as the Facebook disclosure. From the open-ended question in the questionnaire, participants mention one main reason they use Facebook is to keep in touch with their high school classmates. It indicates that users in this research can recognize the real identities with their "Friends" on Facebook since real friends should know one's personal and background information, Facebook users might or might not provide such information necessarily on their social networking media. Also, the x^2 test shows no significant difference between different levels of PRI in terms of whether concerning their real names and personal information have been leaked. That mean, even those respondents at a low PRI level did not express concern about it.

Table 6

Chi-square test of PRI and attitude toward personal information security

	Concern about personal information on Facebook will be leaked		
PRI	No	Yes	Total
Low	61(65.3)	19(14.7)	80
Middle	77(79.2)	20(17.8)	97
High	11(104.5)	17(23.5)	128
Total	249	56	305
		x^2=4.083, p=.130	

Note: Numbers in cells are frequency and numbers in parentheses are expected count.

Dynamic Privacy (Joining fan pages) vs. PRI

According to results from Table 6, the authors might argue that disclosed personal information is not the main issue of online privacy concerns towards the respondents. Now, to focus on analyzing if other Facebook activities would be the issue of privacy concern. Table 7 shows respondents' attitudes towards whether concerning that information on fan pages will be leaked across three levels of PRI. It shows nearly 90% of respondents did not concern about whether their information on fan pages will be leaked. It was found that 40% of them thought their information on fan pages is not important or that it did not matter, and around 29% of respondents said fan pages are trustworthy so that they did not concern. Also, significant difference was not found between levels of PRI in terms of fan pages privacy attitude, which means the respondents did not concern that their activities on fan pages will reveal their private information, due to the fact that fan pages are considered trustworthy, and/or their information is not that important.

Table 7

Chi-square test of PRI and attitude toward fan page privacy security

	Concern about your information on fan pages will be leaked		
PRI	No	Yes	Total
Low	69(71.9)	11(8.1)	80
Middle	85(87.1)	12(9.9)	97
High	120(115.0)	8(13.0)	128
Total	274	31	305
		x^2=3.792, *p*=.150	

Note: Numbers in cells are frequency and numbers in parentheses are expected count.

Dynamic Privacy (Check-in) vs. PRI

In the last table, the relationship between respondents' attitudes towards the privacy risk of the "check-in" function on Facebook was examined. The primary result shows those at a low level of PRI had a higher percentage concerning personal information on check-in will be leaked; on the contrary, those at a high level of PRI concern about it less (x^2=8.271, *p*=.016). It seems that respondents are more concerned about the privacy of their Facebook dynamic activities than static personal information. This finding, and those discussed above, provides significant evidence for reconsidering privacy among Facebook users.

Table 8

Chi-square test of PRI and attitude toward check in privacy security

	Concern about your information on check in will be leaked		
PRI	No	Yes	Total
Low	28(38.0)	52(42.0)	80
Middle	46(46.0)	51(50.9)	97
High	71(60.9)	57(67.1)	128
Total	145	160	305
		x^2=8.271, *p*=.016	

Note: Numbers in cells are frequency and numbers in parentheses are expected count.

Discussion and Conclusion

This research was inspired by the observations that social media users concern about privacy but still disclose information on the platform, i.e., privacy paradox on FB. Researchers are also interested in the definitions of privacy with the development of social media. Beginning with these enquires, this research delineated the nuanced definition of "privacy"—static and dynamic, to investigate participants' concerns with online privacy. Following these two categories of privacy, we selected three dimensions and five variables to develop a privacy risk index, say PRI, to understand participants' attitudes and behaviors while encountering with online privacy invasion. The findings show that participants care less about static privacy than dynamic ones. It also shows that people with low PRI are more intentional than those with high PRI to take action to prevent their privacy from invasion.

From our PRI test, we found that nearly 42 percent of our respondents (high-risk group) exposed much information on Facebook, resulting in their static and dynamic privacy were easy to be tracked and collected by a third party. It implies that college students in this study had lower sensitivity to privacy risk. Compared to their counterparts, the low PRI group (26% of student samples) showed that they tended to protect themselves from the potential damage of privacy leakage. From the self-evaluation of exposing online privacy risk, we demonstrated that the PRI is a simple and straightforward tool to assess online users' sensitivity to their privacy risk.

As to examining the contradiction of the "privacy paradox," we found that no significant association between participants' privacy concerns and behaviors in terms of providing real name and personal information and joining fan pages (static privacy in this paper). It indicates that most respondents did not express concern about their personal information to be disclosed on Facebook regardless of their PRI levels. This may imply that personal information is not considered as one of the privacy issues among the student samples. It may also indicate that personal information is part of basic information to leave on social media as a means of making new friends and keeping in touch with old friends. Some of the participants did mention in the semi-structured questionnaire that personal information does not account for privacy for them. Furthermore, this may also correspond to what the existing literature argues that joining SNS is a kind of tradeoffs (Dourish & Anderson, 2006; Chen, 2018). Although users judge that they can obtain more than their privacy being invaded, they would make the deal to disclose their privacy on FB. Our participants did mention that leaving personal information on social media is beneficial to their job-hunting since employers would search for applicants' personal information on FB. These abovementioned reasons may explain that the privacy paradox does not appear in our findings.

Then, what type of privacy issues is college students in this exploratory study concern and pay more attention to avoid themselves exposing on privacy risk? We found check-in (dynamic privacy in the paper) with the PRI test reflect the consistency between attitude toward privacy risk and their risk behaviors. That is, from this study, we found that people who concern about the information on check-in will be leaked tended to act at a low risk of privacy leakage. This tendency rejects the hypothesis of the privacy paradox. A possible reason provided in the questionnaire infers that dynamic privacy would be a tool to track users' destinations and activities at that time, which is not good for those taking excuses to reject other invitations. This finding also tells another story that the definition of privacy is subject to change and depends on what users in this research decide to disclose or not. If the users want to disclose, it may not be considered as privacy, and vice versa.

Apart from what is aforementioned, we synthesize some suggested explanations for the findings. Firstly, Facebook adopts a real-name registration policy that is one possible explanation for this high percentage of signing up using real names. Secondly, most Facebook users build their online friends' list based on their real/offline friends, so that issues of anonymity on the Internet are less of a concern among friends, or to friends of friends. Thirdly, our participants reported that they don't care whether their personal information will be invaded since they trust the fan pages management, and there is not really very much if any, private information they disclose. Fourthly, the participants reported that they did not intend to reveal their mobility information (check-in, dynamic privacy); for them, this seems to be stalked by their Facebook friends. These findings provide nuanced differences in privacy perceptions of Facebook users.

However, the findings and creation of the PRI index cannot be implied without limitations. The aim of this research is to explore the relationship between attitude and behavior on the privacy of FB users and experimentally create a preliminary index for investigation. Since there is currently not such an index in the literature, as pioneers, we tried to design a semi-structured questionnaire to collect data from the participants. As preliminary research, we tended to collect a convenience sample from college students, who were recruited from a private college in northern Taiwan. We suggested that more diverse backgrounds of participants being considered in future research (e.g., participants from national or public universities, universities from non-northern part of Taiwan, or technology/professional colleges students, etc.).

As an exploratory study, we also tended to simplify the content of the index. Thus, we only grasped three main dimensions and five variables to develop the PRI index, though we found participants mentioned what literature indicates as limiting profile visibility and cost-benefit trade-offs. Now with the advent of PRI index, the authors encourage researchers to add more new and mediated variables (e.g., such privacy management strategy as limiting profile visibility) in the PRI to make this index more suitable for different spatial (cultural) and temporal (time period) settings with new privacy management tools developed by FB. For future research, we also suggest considering more deliberately about each variable. Taking “tag” for example, researchers can delineate different situations of tagging with a friend’s name or photos, tagged by friends or friends’ friends, etc. These are the limitations an exploratory research encounters and could be advanced by future research.

Furthermore, the existing literature on Facebook privacy concerns comes mainly from the younger generation and from the English-speaking regions. This study also has the limitation of collecting data from the young generation, which is more convenient for creating an unprecedented index. However, regarding the region, we chose an Asian country Taiwan to be our case study. Some researchers are also starting to conduct comparative studies between Asian and Western countries (e.g., Chen, 2018). More data collecting from inter/intracultural settings are needed to implement social media privacy literature.

Despite the limitations, this research extends the privacy paradox by delineating online privacy activities to deliberate the situations the privacy paradox appears. This further provides a relatively comprehensive understanding of online privacy. This research also took an Asian country Taiwan as the case study to create an index to test the attitudes and behaviors of FB users on privacy. Researchers actively encouraged and very welcomed to adopt the PRI to conduct intercultural and intergenerational research in the future. Finally, the PRI variables are related to the subjective attitudes and behaviors of the users on the one hand. On the other hand, they are also limited by the open function settings of social platforms such as FB. Therefore, as the function settings of the FB platform become more complicated, the related variables of the PRI are also more diverse. Apart from FB, different social platforms, such as Instagram, are springing up. The privacy settings of these new social platforms can also be taken into consideration in the future. It is expected that follow-up research will develop a more comprehensive and general privacy risk index for all online social platforms.

References

Aysem, D. V., & Mehemt Bilal, Ü. (2017). The right to data portability in the GDPR and EU competition law: odd couple or dynamic dou? *European Journal of Law and Technology, 8*(1). Available at https://arro.anglia.ac.uk/701565/1/Diker%20 Vanberg_2017.pdf. Access on 2019/05/24.

Acquisti A., Gross R. (2006) Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In: Danezis G., Golle P. (eds) Privacy Enhancing Technologies. PET 2006. Lecture Notes in Computer Science, vol 4258. Springer, Berlin, Heidelberg.

Acquisti, Q., Brandimarte, L., & Loewenstein, G. (2015). Privacy and Human Behavior in the Age of Information. *Science, 347*(6221): 509-514. doi: 10.1126/science.aaa1465

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, ; Territory, and Crowding*. Monterey, California: Brooks/Cole.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). Available at http://firstmonday.org/article/view/1394/1312. Access on 2019/05/24. doi: 10.5210/fm.v11i9.1394

Birnholtz, J., Burke, M., & Steele, A. (2017). Untagging on social media: Who untags, what do they untag, and why? *Computers in Human Behavior, 69*: 166-173. doi: 10.1016/ j.chb.2016.12.008

boyd, d., & Hargittai E. (2010). Facebook privacy settings: Who cares? *First Monday, 15*(8). Available at http://firstmonday.org/article/view/3086/2589. Access on 2019/05/24. doi: 10.5210/fm.v15i8.3086

Campbell, J., Sherman, R.C., Kraan, E., & Birchmeier, Z (2001). Internet Privacy Awareness and Concerns among College Students. Paper presented to APS, Toronto. June 2001. Available at http://www.users.miamioh.edu/shermarc/aps01.htm. Access on 2019/05/24.

Chen, H.-T., Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking, 18*(1): 13-19. doi: 10.1089/cyber.2014.0456

Chen, H.-T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist, 62*(10), 1392-1412. doi: 10.1177/0002764218792691

Child, J. T., & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: the challenges of blogging and relational communication on the internet. In Kevin, B. Wright, & Lynne, M. Webb. (eds.), *Computer-Mediated Communication in Personal Relationships*, chapter 2. Peter Lang: International Academic Publishers.

Child, J. T., & Haridakis, P. M., & Petronoi, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: the variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior, 28*(5): 1859-1872. doi: 10.1016/j.chb.2012.05.004

Christofides, E., Muise, A., & Desmarais, S. (2010). *Privacy and Disclosure on Facebook: Youth and adults' information disclosure and perceptions of privacy risks*. University of Guelph. Available at https://www.ontariosciencecentre.ca/Uploads/researchlive/documents/OPC-FinalReport-FacebookPrivacy.pdf. Access on 2019/05/24.

Culnan, M. J., & Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*, 104-115. doi: 10.1287/orsc.10.1.104

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*, 61-80. doi: 10.1287/isre.1060.0080

Dourish, P. & Anderson, K. (2006). Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction, 21*(3): 319-342. doi: 10.1207/s15327051hci2103_2

Dwyer, C., Hiltz, S.R. and Passerini, K. (2007) Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace. Proceedings of AMCIS

2007, Keystone. http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf

Govani, T. & Pashley, H. (2005). Student awareness of the privacy implications when using Facebook. Available at http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf. Access on 2019/05/24.

Gross, R. & Acquisti, A. (2005). Information revelation and privacy in online social networks. Paper presented at ACM Workshop on Privacy in the Electronic Society (WPES). https://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf

Hartmann, M. (2013). From domestication to mediated mobilism. *Mobile Media and Communication, 1*(1): 42-49. doi: 10.1177/2050157912464487

Heravi, A., Mubarak, S., & Choo, K-K. (2018). Information privacy in online social networks: Use and gratification perspective. *Computers in Human Behavior*, 84: 441-459. doi: 10.1016/j.chb.2018.03.016

Lewis, K., Kaufman, J., Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication, 14*(1): 79-100. doi: 10.1111/j.1083-6101.2008.01432.x

Marsoof, A. (2011). Online social networking and the right to privacy: the conflicting rights of privacy and expression. *International Journal of Law and Information Technology, 19*(2): 110-132. doi: 10.1093/ijlit/eaq018

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs, 41*(1): 100-126. doi: 10.1111/j.1745-6606.2006.00070.x

Oliver, P. (2006) Purposive sampling. In V. Jupp (Ed.), The SAGE Dictionary of Social Research Methods. Sage, pp. 244-245.

Ortiz, J., Chih, W-H., Tsai, F-S. (2018). Information privacy, consumer alienation, and lurking behavior in social networking sites. *Computers in Human Behavior, 80*: 143-157. doi: 10.1016/j.chb.2017.11.005

Osatuyi, B., Passerini, K., Ravarini, A., & Grandhi, S. A. (2018). “Fool me once, shame on you…then, I learn.” An examination of information disclosure n social networking sites. *Computers in Human Behavior, 83*: 73-86. doi: 10.1016/j.chb.2018.01.018

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1). Available at https://firstmonday.org/article/viewArticle/2775/2432. Access on 2019/05/24. doi: 10.5210/fm.v15i1.2775

Raynes-Goldie, K. (2011). *Annotated bibliography: Digitally mediated surveillance, privacy and social network sites*. Proceedings from Cybersurveillance and Everyday Life: An International Workshop, Toronto.

Romanou, A. (2018). The necessity of the implementation of privacy by design in sectors where data protection concerns arise. *Computer Law and Security Review*, 34(1): 99-110. doi: 10.1016/j.clsr.2017.05.021

Spiekermann, Sarah and Korunovska, Jana and Bauer, Christine (2012) Psychology of Ownership and Asset Defense: Why People Value their Personal Information Beyond Privacy. *In: International Conference on Information Systems (ICIS 2012)*, 16-19 December 2012, Orlando Florida, USA.

Stutaman, F., Vitak, J., Elission, N. B., Gray, R., & Lampe, C. (2012). Privacy in interaction: Exploring disclosure and social capital in Facebook. Available at http://fredstutzman.com/papers/ICWSM2012_Stutzman.pdf. Access on 2019/05/24.

Toch, E., Wang, Y., & Cranor, L. F. (2012). Personalization and privacy: A survey of privacy risk and remedies in personalization-based systems. *User Modeling and User-Adapted Interaction*, 22: 203-220. doi: 10.1007/119574543

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Techonlogy, & Society, 28*(1): 20-36. doi: 10.1177/0270467607311484

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society, 16*: 479-500. doi: 10.1080/1369118X.2013.777757