The Privacy Calculus of “Friending” Across Multiple Social Media Platforms

Yu-Hao Lee¹ and Chien Wen Yuan²

Abstract
Relationship building through social network sites (SNSs) requires privacy disclosure that involves a calculus of potential benefits against privacy risks. Tie formation (e.g., friending, following, or connecting) on SNSs is one of the most significant forms of privacy disclosure that not only communicate one’s willingness to disclose but can also reveal past activity history and invite future interactions. Based on the communication privacy management theory, the current study examines how users consider the privacy calculus and tie-formation affordances of the SNSs to manage ties across multiple SNSs. Using an online survey of 630 Facebook and/or Instagram users, the study revealed that individuals with higher privacy concerns strategically manage their privacy by connecting with different relationship ties through different SNSs as a way to construct sociotechnical boundaries between networks. The findings have implications for understanding privacy management online and provide a potential explanation for the privacy paradox.

Keywords
social network sites, privacy calculus, privacy paradox, communication privacy management theory, tie formation

Introduction
Billions of people around the world regularly use social network sites (SNSs), such as Facebook, Twitter, or Instagram, to connect and interact with one another. SNSs provide a convenient way for people to develop and maintain relationships through exchanging private and public information in the form of posts, photos, or videos. SNS affordances, such as visibility, persistence, and associations, can facilitate relationship building by making interactions on SNSs, such as clicking the “like” button or commenting on a post are visible to other people within the network, providing an opportunity for further information exchanges (Treem & Leonardi, 2012). However, the same SNS affordances that facilitate relationship building can also create new privacy risks. For example, one’s shared information may be exposed to unintended audiences or shared with third parties without the user’s knowledge. Once information is shared, it becomes persistent in the companies’ servers and on the Internet, making it difficult for individuals to manage their privacy. As a result, when using SNSs for relationship building, SNS users must carefully negotiate their relational needs for disclosure against their personal needs for privacy.

Relationships on SNSs usually begin by initiating ties through SNS functions, such as “ friending,” “ following,” or “ connecting.” Ties can be initiated symmetrically when one person sends a request to another person, and that person needs to accept the request for mutual information disclosure (e.g., friending on Facebook). Tie formation can also be asymmetrical when one person “follows” another individual or a public account without requiring the other party’s approval (e.g., following on Instagram). Connecting on SNSs reveals one’s profile information, posts, or shares, including personal photos. Once people become connected, some systems will send notifications to alert people within the network whenever someone shares new content or makes a comment, which facilitates more potential interactions. In other words, tie formation (e.g., friending, following, connecting) through SNSs is a significant privacy disclosure that not only communicates one’s willingness for disclosing past, current, and future interaction records but also invites further informational exchanges with one’s network.

Many studies have argued that tie formation through SNSs is a significant form of privacy disclosure. For example, Ellison et al. (2011) argued that social media users

¹University of Florida, USA
²National Taiwan Normal University

Corresponding Author:
Yu-Hao Lee, University of Florida, PO Box 118400, Gainesville, FL 32611, USA.
Email: leeyuhao@jou.ufl.edu
manage their audience and privacy through three strategies: friending, site privacy settings, and information control. Based on this framework, Chen and Chen (2015) found that users managed their privacy concerns by limiting their friends and profile disclosure. But perhaps the most theoretical justification for examining tie-formation decisions comes from Petronio (2015)’s communication privacy management theory (CPM). CPM argues that people manage their privacy through managing “boundaries.” When people extend their boundaries to include other people, they extend personal ownership of their privacy to a co-ownership with the people within their boundaries. On SNSs, tie formation (i.e., friending, following, or connecting) is a significant boundary extension to include other people into one’s network. In doing so, the individuals disclose personal and network information by extending ownership of their information to the parties with which they are forming ties.

As a major form of privacy disclosure, tie formation involves potential benefits and risks. The benefits of forming ties through SNSs include access to information about other people, prompt notifications for monitoring one’s network, and frequent interactions that can lead to more social support, informational support, social capital, and entertainment gratifications (Choi & Bazarova, 2015; Ellison et al., 2007). However, tie formation on SNSs also carries the potential risk that one’s personal information may be misused or misinterpreted by other users or companies (Dienlin & Metzger, 2016; Krasnova et al., 2012). SNSs often bring together audience groups formerly separated by physical or social boundaries, making impression management much more difficult, resulting in context collapse where connections of different social circles coexist on a site (Marwick & boyd, 2011). An associated consequence is that information intended for one audience group being unintentionally exposed to another, revealing contradicting sides of oneself. Personal information also risks being shared with third parties without the user’s awareness and consent, creating unwanted problems, such as identity theft, aggressive advertisements, or government surveillance. Therefore, the decision to form a tie with someone through SNSs involves a privacy calculus in which people weigh the potential benefits against the potential risks of connecting through SNSs (Culnan & Armstrong, 1999; Dienlin & Metzger, 2016; Dien & Hart, 2006; Krasnova et al., 2012). When people juggle multiple SNSs, each with its different affordances and privacy calculus, it may create needs for the users to carefully deliberate with which ties to connect, and through which SNSs. People may strategically “friend” different ties through different SNSs as a way to negotiate their privacy boundary and control their context of privacy disclosure (Dienlin, 2014; Petronio, 2015).

The goal of this study is to examine how users’ privacy calculus affects their tie-formation decisions regarding four types of network ties (strong ties, existing weak ties, latent weak ties, and parasocial ties) between two SNSs (Facebook and Instagram) with different tie-formation affordances. We compared Facebook with Instagram because they are both popular SNSs but with different tie-formation affordances (Smith & Anderson, 2018; Ting et al., 2015). More specifically, by default, Facebook requires symmetrical agreements for tie formation, while Instagram supports asymmetrical tie formation. Given that many users use multiple SNSs to connect and interact with their networks, it is important to compare tie-formation practices between multiple sites to see how privacy calculus influences tie-formation decisions and how tie formation can function as a boundary-construction mechanism for managing privacy.

Literature Review

Social Media Tie Formation as Self-Disclosure

CPM is a theory about how people manage privacy through boundary negotiations (Petronio, 2002). CPM posits that relationships are developed through privacy disclosure and negotiation of privacy boundaries. When individuals disclose private information, the ownership of their private information is transferred to a collective co-ownership among people who have access to the information. Individuals manage their privacy by making rules about what information to disclose or withhold it on the individual level and the collective level. On the individual level, people’s privacy disclosure is determined by factors, such as cultural norms, the interaction context, and their privacy calculus (i.e., the risk-benefit analysis of privacy disclosure). On the collective level, privacy is maintained by considering relational ties and boundary permeability. CPM suggests that individuals manage their private information within the collective boundaries through negotiating with whom they connect (linkage rules), how much control they have over the co-owned information (ownership rules), and how much information to share (permeability rules).

In the context of SNSs, when individuals send or receive a tie-formation request, they extend their privacy from personal ownership to collective ownership by granting others access to their profiles, posts, photos, and other interactions (Child & Petronio, 2011). Each tie-formation request on SNS is a new opportunity to extend privacy ownership and build relationships, but at the same time, each new tie formation, both initiating and receiving, also requires one to assess and recalibrate their privacy management rules (Child & Westermann, 2013; Frampton & Child, 2013).

SNSs can help people initiate and maintain social relations with existing and otherwise unlikely offline networks (boyd & Ellison, 2007). Many SNSs also afford people to follow public figures (Ballantine & Martin, 2005) or activate potential social connections (Haythornthwaite, 2002). However, on SNSs, the offline physical or social boundaries that separate different networks tend to collapse, a phenomenon known as context collapse (Marwick & boyd, 2011).
Due to context collapse, the gradual relation-building process that takes place offline may be flattened and expedited on SNSs where information across different timeframes and social groups is laid out directly to strangers, acquaintances, friends, and potential connections alike. As a result, individuals face a privacy dilemma when revealing private information through SNSs to a mix of social ties. During these privacy dilemmas, users may try to manage their privacy boundaries by considering the privacy calculus of forming ties through different SNSs.

**Privacy Calculus and SNSs**

Managing privacy on SNSs involves a privacy calculus of the potential benefit of privacy disclosure against the potential risks (Culnan & Armstrong, 1999; Dinev & Hart, 2006; Krasnova et al., 2012). A certain degree of privacy disclosure is necessary for building and maintaining relationships. However, too much disclosure can lead to privacy risks, such as losing control over one’s self-presentation (Marwick & boyd, 2014), unwanted advertisements, or identity theft (Nosko et al., 2010). The concept of privacy calculus is included in CPM as a privacy management rule. Individuals will disclose more information if they determine the benefits of disclosing private information outweigh the costs and risks of disclosure. In contrast, individuals will withhold or withdraw information if they perceive the privacy risks to be higher than the potential benefits.

Many studies have identified motivations that drive SNS use, including relational development, information seeking, social support, identity expression, professional development, escapism, or entertainment (Choi & Bazarova, 2015; Papacharissi & Mendelson, 2010). Yet, none of these benefits can be obtained without first connecting with one’s network and maintaining a certain level of connectedness. Information disclosure is an essential part of relationship development, which relies on the social exchange of information at the appropriate level. The appropriate level depends on the relationship ties and the boundaries afforded by the context (Dienlin, 2014). Individuals who perceived more benefits from SNS use often disclosed more personal information (Baruh et al., 2017).

The cost of privacy disclosure on SNS is associated with privacy concerns and risks. SNS users are generally concerned about their privacy (Taddicken, 2014; Tufekci, 2008). However, a recent meta-analysis shows that privacy concerns do not seem to affect SNS use and only have a small effect on the amount of information shared and usage of privacy settings (Barnes, 2006; Baruh et al., 2017), a phenomenon known as the “privacy paradox.” A closer look at qualitative evidence suggests that the privacy paradox may be due to different ways that individuals manage their privacy boundaries. For example, several studies found that teenagers are not too concerned about the amount or the types of information they disclose on social media, as long as they have control over who has access to their information (Livingstone, 2008; Tufekci, 2008). Similarly, Young and Quan-Haase (2013) found that students used various strategies for managing their privacy, including limiting access and information to their profile through information exclusion and strategic friending decisions. In these interviews, participants described deliberate choices about the different modes of communication, the perceived affordances for each site, and how they managed access to their information through tie-formation decisions. In other words, instead of looking at how privacy concerns directly influence the amount of self-disclosure, researchers should take a step back and investigate the sociotechnical contexts where users negotiate boundaries for privacy management.

We argue that tie-formation decisions on SNSs are unique research opportunities to address the privacy paradox because the balance between privacy concerns and privacy disclosure can be contextualized in how users manage their networks through different SNSs (Child & Westermann, 2013; Frampton & Child, 2013). Recent studies on multiple site usage showed that some users try to construct boundaries between their social groups through compartmentalizing SNS use (Stutzman & Hartzog, 2012; Wilken, 2015). Compartmentalizing SNSs and ties allow users to control the context in which information is disclosed and to whom.

**Connecting With Strong, Weak, and Parasocial Ties Through SNSs**

SNSs can support connecting with large networks of social ties, including strong ties, weak existing ties, weak latent ties, and parasocial ties (Ellison et al., 2007; Haythornthwaite, 2002). Strong ties refer to close family and friends who share a high level of intimacy, self-disclosure, reciprocity, and interaction frequency (Haythornthwaite, 2005). Strong ties are closer connections and can provide social and emotional support. In comparison, weak existing ties consist of distant relatives, acquaintances, old friends, or coworkers with whom the individual does not interact regularly. Weak latent ties are people who are in the same geographical or professional area that have the potential to become collaboration partners in the future (Podolny & Baron, 1997). Weak ties often do not belong to people’s immediate, close networks; therefore, they function as a bridge to external and more diverse communities (Putnam, 2000). In some cases, connecting to weak ties of higher social or economic rank enables people to access otherwise scarce resources, such as financial support, career advantages, or information exchange (Granovetter, 1973). Weak ties provide information that expands an individual’s existing resources and increases coordination (Granovetter, 1973). SNSs allow users to sustain large networks of weak ties, which may help people to obtain small favors from whoever is available to offer a gesture of goodwill (Gilbert & Karahalios, 2009).

Some SNS tie-formation behaviors are motivated by parasocial relationships. Parasocial relationships are conceptualized as the perception of interpersonal relationships that
media users have with media personas, such as a character, actor, or celebrity (Horton & Wohl, 1956). Media users can develop strong parasocial relationships through following information about the characters and personalities (Ballantine & Martin, 2005). Most previous studies on parasocial relationships have focused on television, movie, or radio personas, but scholars suggest that the interactive and social nature of SNSs can intensify parasocial relationships (Thorson & Rodgers, 2006). Anyone can be a media persona on SNSs, such as online streamers and political commentators. Social media personas can interact directly with their audiences through live chatting, but most SNS users typically observe the personas disclosing information about themselves and interacting with other users. According to Horton and Wohl (1956), parasocial interaction is more likely to develop if the media personas address the audience using a conversational style that is akin to face-to-face interactions. In fact, social media personas often speak to their imagined audiences as if they are personal friends, stressing authenticity over scripted performance (Litt & Hargittai, 2016). These interactions and personal disclosures make online personas appear even more like friends than televised characters. People may form ties with media personas through SNSs to stay informed about these people (i.e., information surveillance) or to seek the possibility of interacting with the media personas (Kowalezyk & Pounders, 2016; Weeks & Holbert, 2013). Studies on self-presentation also suggest that people may connect through SNS for personal expressions (Gibbs et al., 2006). While these studies do not focus on how privacy concerns affect tie-formation decisions with parasocial ties, other studies suggest that SNS users often engage in mediated lurking to gather information about other parties without disclosing personal information and that users with higher perceived privacy risks were associated with more lurking behaviors (Ortiz et al., 2018).

As SNS users develop multi- and cross-platform SNS usage, it is essential to examine how factors like privacy calculus influence users’ tie-formation decisions across SNS platforms. According to Dienlin (2014), the context of privacy disclosure is an important multidimensional factor that affects people’s privacy disclosure. When deciding whether to disclose information, people will consider the amount of privacy collection occurring in the context (information privacy), who is the audience (social privacy), the level of intimacy (psychological privacy), and whether the self is observable and identifiable (physical privacy). Examining tie-formation decisions with different ties on different SNSs allow this study to take account of these different privacy contexts. One way to evaluate the adoption of social media tools for initiating, maintaining, and connecting different social ties is to ask people to compare tie-formation scenarios. This technique has been adopted in previous studies (Cummings et al., 2002; Duck et al., 1991). We apply this scenario approach to examining how privacy calculus affects tie formation with different social ties over Facebook and Instagram.

Facebook is currently the most popular SNS in the world with 2.23 billion monthly active users.1 The most prominent function of Facebook is to support connections with different online and offline networks, following public figures, and finding potential friends. Facebook also allows users to post or share multimedia contents and interpersonal information on the wall and their profile page. Supporting interactivity, Facebook affords public “Like” or comments on others’ posts or private messages. All these actions are recorded and visible to the users’ friends, depending on the privacy settings. Most importantly, tie formation with personal accounts on Facebook is symmetrical and requires mutual agreements.

As for Instagram, the tie-formation pattern is asymmetrical by default, meaning that users can “follow” other people’s public posts without their agreement. However, Instagram later introduced privacy settings that allow users to control who can view their posts and included a “Close Friends” function that limits a specific group of followers to access some posts. Nevertheless, tie formation on Instagram does not need to be symmetrical. Users can follow others or even be included in their “Close Friends” list without others reciprocally following back. Private (e.g., general users) and public (e.g., celebrities) accounts are both popular on Instagram, but users do not necessarily have to use their real name as account handles, thus raising the difficulty in searching for personal connections or activating potential ties. The major communication mode on Instagram is image-driven with video streaming options. People can comment or like others’ photos and give real-time feedback if they are viewing others’ live videos. Our first research question compares users’ privacy calculus regarding the two sites:

**RQ1. Will there be a difference between participants’ privacy calculus of Facebook and that of Instagram?**

Privacy calculus is a negotiation between the benefits and costs of privacy disclosures (Dinev & Hart, 2006; Petronio, 2015; Taddei et al., 2017). Previous studies have found that users consider both the affordances of the media and the social relationships they intend to connect when determining what information to disclose, through which communication media, and how to disclose it (Livingstone, 2008; Taddei, 2014). Given that initiating new social relationships, maintaining existing ones, and activating potential ones involve a complex privacy calculus, users are more likely to pick a site that they consider safe to engage in these social practices. However, despite potential privacy risks, users may form ties through SNSs out of personal interest to keep up with news and information about other people (Joinson, 2008; Weeks & Holbert, 2013). Users may manage their privacy by selectively forming ties with people whom they trust (Jiang et al., 2014). Other studies have found that personal interest in sharing information is another factor that drives privacy disclosure (Gibbs et al., 2006; Haythornthwaite, 2002). We hypothesize that:
**H1a.** Site trust will be positively associated with the likelihood of tie formation through SNSs.

**H1b.** Personal interest will be positively associated with the likelihood of tie formation through SNSs.

Under the privacy calculus framework, privacy risks and concerns are what drives people to strategically manage their privacy disclosure, such as tie-formation choices among SNSs and among relationship ties (Dienlin & Metzger, 2016; Dinev & Hart, 2006). When people are concerned about the privacy risks of a particular SNS, they may choose not to use the risky SNS or they may manage their privacy concerns by only using the SNS to friend close ties whom they trust with their private information. Therefore, we posit that higher privacy concerns will positively predict friending close ties through SNSs with higher privacy risks.

**H2.** Privacy concerns will positively predict connecting close ties on the SNS with higher privacy risks identified through RQ1.

As for weak and parasocial ties, the privacy paradox literature suggests that there may be no relationship between privacy concerns and self-disclosure to weaker ties. In most cases, people envision a general imagined audience when disclosing on SNSs (Marwick & boyd, 2011; Taddicken, 2014). Therefore, we pose a research question regarding the relationship between privacy concerns and friending weak ties and parasocial ties on SNSs. However, different SNSs have different affordances for tie formation. When comparing Facebook with Instagram, one of the most significant differences is that Instagram supports asymmetrical friending, while most Facebook connections require mutual agreements for friending. Thus, it is possible that individuals who have higher privacy concerns will strategically friend more distant ties (e.g., weak latent or parasocial ties) via Instagram instead of Facebook to limit their self-disclosure.

**RQ2.** To what extent will privacy concerns predict connecting (a) existing weak ties, (b) latent weak ties, and (c) parasocial ties on Facebook and Instagram?

**Method**

**Participants**

We recruited 630 participants from Amazon’s Mechanical Turk who live in the United States. Due to Institutional Review Board (IRB) regulations, no participants were rejected, but 29 participants were removed from the data because they did not use either Facebook or Instagram. Mechanical Turk samples are more diverse than traditional convenience samples in social science and are comparable to professional/commercial online panels in demographic representativeness (Buhrmester et al., 2011). In fact, Mechanical Turk samples outperform student samples and professional panels, such as Qualtrics in response quality and reliability (Kees et al., 2017). Several studies have used Mechanical Turk surveys to examine privacy behaviors, including Facebook privacy settings (Liu et al., 2011) and consumers’ privacy trust (Martin, 2016). The most recent demographic estimation of Mechanical Turk participants shows that they are fairly representative of the general population, balanced in terms of gender, diverse in ethnicity, but slightly younger and more educated than the general population (Difallah et al., 2018). Our participants reflect these demographics, with balanced gender (female, n = 312, 50%) and an average age of 35.58 (SD = 11.48) years, ranging from 19 to 73 years. Most of the participants identified their ethnicity as White (79%), followed by Black/African Americans (8%), Asian or Pacific Islander (8%), and Hispanic/Latino (5%). Most participants have a bachelor’s degree or higher (51%).

**Procedures**

An online survey was distributed. The survey structure was designed to match the participants’ Facebook and Instagram use, respectively. The site order was randomized to avoid response bias. Depending on the participants’ answers, the survey directed them to complete specific questions about the SNS(s) they used. In total, 576 respondents reported to be Facebook users and 346 to be Instagram users; 323 users actively used both sites. The survey included questions about site-specific privacy calculus and presented the participants with 12 scenarios that mapped onto strong ties, existing weak ties, weak latent ties, and parasocial ties, and the participants were asked how likely they were to use Facebook or Instagram to connect with the ties in each scenario. Finally, we asked demographic questions, including age, gender, race, education, employment, and relationship status. The survey took no longer than 20 min to complete. Each participant received US$1 as compensation for their voluntary participation.

**Measures and Scales**

**Social Ties and Tie-Formation Decisions.** We asked our participants to consider 12 different tie-formation scenarios that map onto four social ties, namely strong ties, weak existing ties, weak latent ties, and parasocial ties. The participants were asked to rate on a 7-point scale (1 = extremely unlikely to 7 = extremely likely) how likely they are to use Facebook or Instagram to connect with the ties in each scenario. The 12 tie-formation scenarios include as follows:

Strong ties—(1) a good friend of yours; (2) family members to whom I am close to.
Weak existing ties—(3) you were at a party and encountered a classmate from elementary school; (4) your classmates/coworkers who you do not socialize on a regular basis; (5) family members with whom I seldom interact; (6) someone whom you just met but works in the same area as you.

Weak latent ties—(7) your friend asks you a favor to help his or her friend whom you have never met before; (8) you are applying for a new job, your friend tells you that she has a friend working in that company and would like to introduce you; (9) a person recommended by the social media platform who shares many connections with you.

Parasocial ties—(10) a celebrity that you like very much; (11) a person who writes about topics of interest to you; (12) someone who you would like to show your posts to.

Privacy Calculus. The Privacy Calculus Scale (Dinev & Hart, 2006) includes 14 items that measure four dimensions on a 5-point scale with 1 = strongly disagree to 5 = strongly agree: perceived privacy risks (α = .92 for Facebook, α = .93 for Instagram), privacy concern (α = .95 for Facebook, α = .95 for Instagram), site trust (α = .82 for Facebook, α = .80 for Instagram), and personal interest (α = .90 for Facebook, α = .91 for Instagram). The participants answered the scale for Facebook and Instagram separately. Privacy concern and privacy risk were highly correlated (r = .53 for Facebook, r = .59 for Instagram). To avoid multicollinearity in our models, we only included privacy concerns in the regression analyses.

SNS Usage. We measured Facebook and Instagram use as control variables. The SNS usage was measured with a single-item question for each site that asked: how often do you spend time on [site]? The answers were ordinal from 1 = several times a day to 7 = less than once a month.

Results

Our first research question asked whether there are significant differences in the participants’ perceived privacy calculus between Facebook and Instagram. For the analysis regarding RQ1, we conducted a two-sample t-test to compare the four privacy calculus factors between Facebook and Instagram. The results showed that the participants reported higher privacy risk and privacy concerns for Facebook compared to Instagram. Site trust was higher for Instagram compared to Facebook. There was no significant difference with regard to personal interest. See Table 1 for t-test results, means, and standard deviations.

Our first hypothesis posited that site trust (H1a) and personal interest (H1b) would predict a higher likelihood of friending through SNS. H2 posits that privacy concerns will positively predict friending close ties through SNSs with higher privacy risks. RQ2 asked to what extent will privacy concerns affect the likelihood of friending weak (existing and latent) and parasocial ties. We conducted separate hierarchical regressions with the SNS usage as the control variable in the first block, and the three factors of privacy calculus (i.e., privacy concern, site trust, and personal interest) as the independent variables in the second block. The four types of social ties were entered as dependent variables (see Table 2).

For close ties, the model was significant for friending via Facebook, F(4, 565) = 14.76, p < .001, adjR² = .09. Privacy concern was a significant predictor of friending close ties via Facebook. Site trust was not a significant predictor. Personal interest was a significant predictor. For Instagram, the model was also significant for friending close ties, F(4, 340) = 5.07, p < .001, adjR² = .04. Privacy concern was not a significant predictor of friending close ties via Instagram. Site trust was a significant predictor. Personal interest was not significant. H1 was partially supported as site trust toward Instagram, and personal interest regarding Facebook was associated with higher likelihood of friending close ties, but there were some inconsistencies between the sites. H2 was supported.

For weak existing ties, the model was significant for friending via Facebook, F(4, 564) = 12.47, p < .001, adjR² = .05. Privacy concern was not a significant predictor. Site trust was a significant predictor. Personal interest was close to significance. For Instagram, the model was also significant, F(4, 342) = 6.01, p < .001, adjR² = .06. Privacy concern was not a significant predictor of friending weak existing ties via Instagram. Site trust was a significant predictor. Personal interest was not significant. H1 was supported for weak existing ties. Regarding RQ2, privacy concern was not significantly correlated with connecting with weak existing ties via either site.

For weak latent ties, the model was significant for friending via Facebook, F(4, 571) = 18.31, p < .001, adjR² = .10. Privacy concern was not a significant predictor. Site trust was a significant predictor. Personal interest was also
a significant predictor. For Instagram, the model was also significant for friending weak latent ties. Privacy concern was a significant predictor of friending latent ties via Instagram. Site trust was also a significant predictor. Personal interest was not significant. H1 was mostly significant; site trust and personal interest were associated with higher likelihood of connecting with weak latent ties via the sites. For RQ2, privacy concern was not significant for Facebook, but was significant for Instagram. This may be because Instagram supports asymmetrical tie formation; thus, users can use it to maintain a connection with weak latent ties with fewer concerns about disclosing privacy information.

For parasocial ties, the model was significant for Facebook, $F(4, 570) = 15.80, p < .001, adjR^2 = .08$. Privacy concern was not a significant predictor. Site trust was a significant predictor. Personal interest was also a significant predictor. For Instagram, the model was also significant for parasocial ties, $F(4, 344) = 16.14, p < .001, adjR^2 = .15$. All three factors of the privacy calculus were significant predictors for friending parasocial ties via Instagram. H1 was fully supported for parasocial ties; site trust and personal interest were significantly associated with connecting with parasocial ties. Privacy concern was not associated with connecting via Facebook but was significantly associated with connecting via Instagram. Similar to latent weak ties, people are mainly motivated to connect with parasocial ties for informational needs. The asymmetrical tie formation afforded by Instagram allows the users to stay connected with their parasocial ties, but without disclosing potentially risky privacy information themselves.

**Discussion**

Based on the CPM theory, this study examined to what extent the participants’ privacy calculus influences their tie-formation decisions with different social ties across two different SNSs: Facebook and Instagram, one site that affords symmetrical tie formation and the other asymmetrical tie formation.

This study has several limitations that should be taken into consideration when interpreting the results. The first limitation is that we only surveyed users who have adopted Facebook or Instagram. The data suggest that among the participants, site trust is generally high toward these platforms. We speculate that some non-users do not use these SNSs due to much lower site trust and higher perceived privacy risks and concerns. In other words, our results only reflect the relationship between privacy calculus and tie-formation behavior among SNS users. Second, while prior studies have shown that Mechanical Turk samples to be comparable to professional/commercial panels and are more representative than a convenience sample of undergraduate students (Buhrmester et al., 2011; Difallah et al., 2018; Kees et al., 2017), Mechanical Turk samples are self-selected and are not representative of the general population. Mechanical Turk samples have higher-than-average media literacy and proficiency in using the Internet, which was reflected in our sample. Finally, we used a scenario-based measure for measuring tie-formation decisions (Cummings et al., 2002; Duck et al., 1991). While scenario-based measures provide higher validity than abstract questions about theoretical constructs, they are, nevertheless, hypothetical scenarios and are subject to self-report problems, such as social desirability bias.

With the above limitations in mind, RQ1 examined the privacy calculus of the two SNSs. There were significant differences in the privacy calculus between Facebook and Instagram. Our participants perceived significantly higher privacy risks and privacy concerns toward Facebook and expressed higher site trust for Instagram. In other words, our participants did not trust Facebook as a site that can protect their personal information and have high perceived risks toward Facebook. There were no significant differences in

### Table 2. Regressions Results on the SNS Usage Based on the Three Factors of Privacy Calculus and the Four Types of Social Ties.

| Types of Social Ties | Strong Ties | Weak Existing Ties | Weak Latent Ties | Parasocial Ties |
|---------------------|-------------|-------------------|-----------------|----------------|
|                     | FB          | IG                | FB              | IG             |
| Privacy concern     | B = .10,    | B = .13           | B = .06,        | B = .13        |
|                     | $t_{FB} = 2.27$,  | $t_{IG} = 1.90$,  | $t_{FB} = 1.06$, | $t_{IG} = 1.64$, |
|                     | $p < .001$*** | $p = .058$        | $p = .292$,     | $p = .101$     |
| Site trust          | B = .04,    | B = .22           | B = .26,        | B = .38        |
|                     | $t_{FB} = .68$,  | $t_{IG} = 2.35$,  | $t_{FB} = 3.79$, | $t_{IG} = 3.42$, |
|                     | $p = .496$   | $p = .020^*$      | $p < .001$***  | $p < .001$***  |
| Personal interest   | B = .16,    | B = .11           | B = .12,        | B = .08        |
|                     | $t_{FB} = 3.29$,  | $t_{IG} = 1.26$,  | $t_{FB} = 1.96$, | $t_{IG} = .79$, |
|                     | $p = .001$*** | $p = 209$         | $p = .051$,     | $p = .429$     |

SNS: social network site; FB: Facebook; IG: Instagram.

* $p < .05$, ** $p < .01$, *** $p < .001$. 

$adjR^2 < .001$, $p = .987$. 

$adjR^2 < .001$, $p = .036$. 

$adjR^2 < .001$, $p = .001$. 

$adjR^2 < .001$, $p = .001$. 

$adjR^2 < .001$, $p = .001$.
personal interest between the two sites, suggesting that the users are equally interested in the potential benefits that the sites can provide.

Consistent with our H1a, site trust was significantly associated with friending all four types of social ties across the two SNSSs. However, the results were mixed regarding H1b: Personal interest was significantly associated with friending all four types of social ties via Facebook, but it was only significantly associated with friending parasocial ties via Instagram. As the most popular SNS, Facebook is a site that accommodates connecting with all four different social ties, which renders the phenomenon of context collapse. As a result, it is less surprising that people are motivated to use Facebook out of personal interest. The result with Instagram and parasocial ties may reveal an association between communication mode and self-disclosure. It is possible that the dominant communication modes on Instagram, photo sharing, and live video sharing allow users to engage in more intimate parasocial relationships with celebrities or other accounts in which they take interest. Photos and videos contain more social and contextual cues that may enrich parasocial relationships and enhance perceived connectedness by the audiences (Walther & Parks, 2002). After all, without real-life interaction opportunities, leveraging the rich cues afforded by Instagram is a good way for building parasocial ties.

H2 posited that privacy concern was positively associated with friending close ties on SNSs with higher privacy risks. The results showed that privacy concern was indeed significantly associated with friending close ties on Facebook, the SNS with higher perceived privacy risk. H2 was supported. Facebook, as the largest and most commonly used SNS, carries the highest risk due to context collapse (Marwick & boyd, 2011). Most people’s Facebook networks include close friends and family members as well as distant relatives and acquaintances from the past. For people with higher privacy concerns, they are more likely to connect close ties through Facebook as a way to manage their privacy risks. This is because close ties are usually of different background and more trustworthy (Granovetter, 1973), which makes them less likely to misuse or misinterpret one’s privacy information on Facebook. RQ2 examined how privacy concerns affected tie formation among weak and parasocial ties. Regarding weak and parasocial ties, privacy concern was significantly associated with tie formation via Instagram. Unlike Facebook, in which friending requires mutual acceptance, Instagram supports asymmetrical friending (i.e., following). The asymmetrical friending affordance of Instagram makes it an ideal platform for keeping up with information about others without giving off too much information about oneself.

In comparison to previous studies on the privacy paradox that found little to no relationship between privacy concern and the amount of self-disclosure (Barnes, 2006; Baruh et al., 2017; Taddicken, 2014; Utz & Krämer, 2009), our findings suggest that participants who have higher privacy concerns may use site selection as a means to manage their audience and their privacy. This finding is consistent with previous qualitative studies that some people did not manage their privacy concerns through regulating the amount of information they disclosed. Instead, they managed privacy concerns by limiting who had access to particular SNSs along with the information on the sites (e.g., Livingstone, 2008; Marwick & boyd, 2014; Taddicken, 2014). In other words, some people may manage their privacy through strategic tie formation across different communication platforms.

This current study provides a potential explanation for the privacy paradox. Most previous studies on the privacy paradox examined self-disclosure behavior on a single website and did not focus on tie formation as a way of managing privacy. According to the CPM theory, privacy management is a negotiation of individual and collective privacy rules through taking account of relational ties, context, and platform affordances, such as boundary permeability (Child & Westermann, 2013). People may use multiple sites to construct sociotechnical boundaries for the audience/social network management to manage their privacy. A potential reason why the previous studies found little to no relationship between privacy concern and the amount of information disclosure may be because the antecedent privacy management strategy is missing from the prior research: The decision of using which SNSs to form connections with different ties. Our findings suggest that users with higher privacy concerns may have considered the privacy calculus of different SNSs and managed their audiences in their tie-formation decisions across SNSs. Managing privacy through tie-formation decisions alleviates the need and effort of managing information disclosure, allowing individuals to treat the public channels as if they were private channels (Marwick & boyd, 2011; Young & Quan-Haase, 2013). This does not mean that individuals are no longer concerned about their privacy, but that a renegotiation of the privacy rules is only necessary when a privacy turbulence occurs, such as a breach of privacy when unintended information is shared to people outside the network or when unintended audience requests access to the private information (e.g., Child & Westermann, 2013; Frampton & Child, 2013). As more people use multiple SNS platforms to build relationships, it is imperative for researchers to examine the users’ perceived sociotechnical affordances for different sites and how they manage their relationships by utilizing multiple site affordances.

Declaration of Conflicting Interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) received no financial support for the research, authorship, and/or publication of this article.
ORCID iDs
Yu-Hao Lee https://orcid.org/0000-0002-0915-7616
Chien Wen Yuan https://orcid.org/0000-0003-0807-2714

Note
1. https://newsroom.fb.com/company-info/

References
Ballantine, P. W., & Martin, B. A. (2005). Forming parasocial relationships in online communities. Advances in Consumer Research, 32, 197–202.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9). https://firstmonday.org/ojs/index.php/fm/article/view/1394

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. Journal of Communication, 67(1), 26–53. https://doi.org/10.1111/jcom.12276

boyd, d., & Ellison, N. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon’s Mechanical Turk: A new source of inexpensive, yet high-quality, data? Perspectives on Psychological Science, 6(1), 3–5. https://doi.org/10.1177/1745691610393980

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. https://doi.org/10.1089/cyber.2014.0456

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 K. B. Wright & L. M. Webb (Eds.), Communication mediated in personal relationships (pp. 21–40). Peter Lang

Child, J. T., & Westermann, D. A. (2013). Let’s be Facebook friends: Exploring parental Facebook friend requests from a communication privacy management (CPM) perspective. Journal of Family Communication, 13(1), 46–59. https://doi.org/10.1080/15267431.2012.742089

Choi, Y. H., & Bazarova, N. N. (2015). Self-disclosure characteristics and motivations in social media: Extending the functional model to multiple social network sites. Human Communication Research, 41(4), 480–500. https://doi.org/10.1111/hcre.12053

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization Science, 10(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Cummings, J. N., Butler, B., & Kraut, R. (2002). The quality of online social relationships. Communications of the ACM, 45(7), 103–108. https://doi.org/10.1145/514236.514242

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J.-M. Mönig (Eds.), Medien und Privatheit (pp. 105–122). Stutz.

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. Journal of Computer-Mediated Communication, 21(5), 368–383. https://doi.org/10.1111/jcem.12163

Difallah, D., Filatova, E., & Ipeirotis, P. (2018, February). Demographics and dynamics of mechanical Turk workers. Paper presented at the Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining, Los Angeles, CA, United States.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Duck, S., Rutt, D. J., Hoy, M., & Strejc, H. H. (1991). Some evident truths about conversations in everyday relationships all communications are not created equal. Human Communication Research, 18(2), 228–267. https://doi.org/10.1111/j.1468-2958.1991.tb00545.x

Ellison, N., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook “friends”: Social capital and college students’ use of online social network sites. Journal of Computer-Mediated Communication, 12(4), 1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x

Ellison, N., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte & L. Reinecke (Eds.), Privacy online (pp. 19–32). Springer.

Frampton, B. D., & Child, J. T. (2013). Friend or not to friend: Coworker Facebook friend requests as an application of communication privacy management theory. Computers in Human Behavior, 29(6), 2257–2264. https://doi.org/10.1016/j.chb.2013.05.006

Gibbs, J. L., Ellison, N., & Heino, R. D. (2006). Self-presentation in online personals the role of anticipated future interaction, self-disclosure, and perceived success in Internet dating. Communication Research, 33(2), 152–177. https://doi.org/10.1177/0093650205285368

Gilbert, E., & Karahalios, K. (2009, April). Predicting tie strength with social media. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 211–220). ACM. https://doi.org/10.1145/1518701.1518736

Granovetter, M. S. (1973). The strength of weak ties. American Journal of Sociology, 78, 1360–1380. https://doi.org/10.1016/B978-0-12-442450-0.50025-0

Haythornwaite, C. (2002). Strong, weak, and latent ties and the impact of new media. The Information Society, 18(5), 385–401. https://doi.org/10.1080/01972240290108195

Haythornwaite, C. (2005). Social networks and internet connectivity effects. Information, Community & Society, 8(2), 125–147. https://doi.org/10.1080/1369180500146185

Horton, D., & Wohl, R. (1956). Mass communication and parasilicon socialization: Observations on intimacy at a distance. Psychiatry, 19(3), 215–229. https://doi.org/10.1080/00332747.1956.11023049

Jiang, Y., Hughes, J. L., & Pulice-Farrow, L. (2014). Coworker Facebook friend requests from a communication privacy management perspective. Human Communication Research, 40(1), 61–80. https://doi.org/10.1111/hcre.12053

Joinson, A. N. (2008, April). Looking at, looking up or keeping up with people? Motives and use of Facebook. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Florence, Italy.
Kees, J., Berry, C., Burton, S., & Sheehan, K. (2017). An analysis of data quality: Professional panels, student subject pools, and Amazon’s Mechanical Turk. Journal of Advertising, 46(1), 141–155. https://doi.org/10.1080/00913367.2016.1269304

Kowalczyk, C. M., & Pounders, K. R. (2016). Transforming celebrities through social media: The role of authenticity and emotional attachment. Journal of Product & Brand Management, 25(4), 345–356. https://doi.org/10.1108/JPBM-09-2015-0969

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. Business & Information Systems Engineering, 4(3), 127–135. https://doi.org/10.1007/s11576-012-0323-5

Litt, E., & Hargittai, E. (2016). The imagined audience on social network sites. Social Media+ Society, 2(1), 1–12. https://doi.org/10.1177/2056305116633482

Liu, Y., Gummadi, K. P., Krishnamurthi, B., & Mislove, A. (2011, November). Analyzing facebook privacy settings: User expectations vs. reality. Paper presented at the Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, Berlin, Germany.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers’ use of social networking sites for intimacy, privacy and self-expression. New Media & Society, 10(3), 393–411. https://doi.org/10.1177/1461444808089415

Martin, K. (2016). Do privacy notices matter? Comparing the impact of violating formal privacy notices and informal privacy norms on consumer trust online. The Journal of Legal Studies, 45(S2), S191–S215. https://doi.org/10.1086/688488

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passively: Twitter users, context collapse, and the imagined audience. New Media & Society, 13(1), 114–133. https://doi.org/10.1177/1461444810365313

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. New Media & Society, 16(7), 1051–1067. https://doi.org/10.1177/146144481453995

Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of Facebook. Computers in Human Behavior, 26(3), 406–418. https://doi.org/10.1016/j.chb.2009.11.012

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. https://doi.org/10.1016/j.chb.2017.11.005

Papacharissi, Z., & Mendelson, A. (2010). Toward a new (er) sociability: Uses, gratifications and social capital on Facebook. In S. Papatheoropoulos (Ed.), Media perspectives for the 21st century (Vol. 212, pp. 212–230). Routledge.

Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. Suny Press.

Petronio, S. (2015). Communication privacy management theory. In C. R. Berger, M. E. Roloff, S. R. Wilson, J. P. Dillard, J. Caughlin, & D. Solomon (Eds.), The international encyclopedia of interpersonal communication (pp. 1–9). Wiley-Blackwell.

Podolny, J. M., & Baron, J. N. (1997). Resources and relationships: Social networks and mobility in the workplace. American Sociological Review, 62(5), 673–693. https://doi.org/10.2307/2657354

Putnam, R. D. (2000). Bowling alone: The collapse and revival of American community. Simon & Schuster.

Smith, A., & Anderson, M. (2018). Social media use in 2018. http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/

Stutzman, F., & Hartzog, W. (2012, February). Boundary regulation in social media. Paper presented at the Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work, Seattle, WA, United States.

Taddicken, M. (2014). The ‘privacy paradox’ in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. Journal of Computer-Mediated Communication, 19(2), 248–273. https://doi.org/10.1111/jcc.12052

Thorson, K. S., & Rodgers, S. (2006). Relationships between blogs as eWOM and interactivity, perceived interactivity, and parasocial interaction. Journal of Interactive Advertising, 6(2), 5–44. https://doi.org/10.1080/15252019.2006.10722117

Ting, H., Wong, W., de Run, E. C., & Lau, S. (2015). Beliefs about the use of Instagram: An exploratory study. International Journal of Business and Innovation, 2(2), 15–31.

Treem, J. W., & Leonard, P. M. (2012). Social media use in organizations: Exploring the affordances of visibility, editability, persistence, and association. Annals of the International Communication Association, 36, 143–189. https://doi.org/10.1080/23808985.2013.11679130

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. Social Media+ Society, 3(1), 1–13. https://doi.org/10.1177/2056305116688035

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

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

Walther, J. B., & Parks, M. R. (2002). Cues filtered out, cues filtered in: Computer-mediated communication and relationships. In M. L. Knapp & J. A. Daly (Eds.), Handbook of interpersonal communication (3rd ed., pp. 529–563). SAGE.

Weeks, B. E., & Holbert, R. L. (2013). Predicting dissemination of news content in social media: A focus on reception, friendliness, and partisanship. Journalism & Mass Communication Quarterly, 90(2), 212–232. https://doi.org/10.1177/1077699013482906

Wilken, R. (2015). Mobile media and ecologies of location. Communication Research and Practice, 1(1), 42–57. https://doi.org/10.1080/22041451.2015.1042423

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. Information, Communication & Society, 16(4), 479–500. https://doi.org/10.1080/1369118X.2013.777757

**Author Biographies**

Yu-Hao Lee (PhD, Michigan State University) is an assistant professor in the Department of Telecommunication at the University of Florida, USA. His research interests include media psychology, immersive technology, and entertainment media.

Chien Wen Yuan (PhD, Cornell University) is an assistant professor of the Graduate Institute of Library and Information Studies at National Taiwan Normal University. Her research interests include mediated personal relationships, human–computer interaction, and computer-supported collaborative work.