

---

# Maximizing the Quality of Social Support and Minimizing the Networked Privacy Risk

**Jennifer Jiyoung Suh**

Department of Communication  
University of California, Santa Barbara  
Santa Barbara, CA 93106-4020 USA  
suh@umail.ucsb.edu

## **Abstract**

This extended abstract introduces a way to conceptualize networked privacy risk in the context of seeking social support on SNSs. It presents four scenarios that illustrate the potential effects of SNS users' tie strength shared with their direct contacts and their network structures on the 2<sup>nd</sup> degree contacts' interest in others' information. For an SNS user who wants to receive quality social support while minimizing their networked privacy risk, a strong tie in a broker position may be the most ideal source of support.

## **Author Keywords**

Networked privacy; social support; social media

Copyright is held by the author.  
CSCW 2017, February 25 – March 1, Portland, OR.  
ACM XXX-X-XXXXX-XXX-X/XX/XX.

## **ACM Classification Keywords**

K.4.1 Computers and Society: Public Policy Issues; Privacy.

## **Introduction**

As more people use social network sites (SNSs), users' networks continue to grow. Almost four out of five online adults in the U.S. are now on Facebook, and more than half of online adults use more than one SNS [12]. SNS use is associated with various types of social capital (e.g., staying in touch with friends who are in distant locations, finding out about local or social events, etc.), and disclosing information is often necessary to take advantage of these benefits [10]. As seeking social support on SNSs involves sharing information that may be personal or sensitive, users' decision-making when seeking social support via SNSs should take into account not only the quality of support, but also the privacy risk associated with this disclosure which is complicated in a networked setting.

## **Social Support and Tie Strength**

Social support is an important element in human interaction because it makes people feel loved and valued, and it provides a sense of belonging to a network of communication [9]. Prior research shows

that social support has a stress-buffering effect that is positively associated with physical health, psychological well-being, and longevity [7, 25].

Users can receive social support from both strong and weak ties because SNSs allow weak ties to provide low-cost social support (e.g., clicking “like”) [21]. Although users’ sense of well-being is better predicted by social support from strong rather than weak ties [27], Rains and Keating found that blogging helped people receive support from weak ties when that from strong ties was unavailable [20]. That said, strong ties provide more empathic support, and SNS users seem to perceive the difference between effortful and low-cost social support [6, 7]. In this way, although both types of ties can provide social support, strong ties are more likely to provide higher quality support.

### **Privacy Risk of Seeking Social Support**

Privacy has been traditionally defined as people’s control over their information [1, 18]. Therefore, others’ access to information about a personal problem could make people feel vulnerable [5, 18]. When SNS users disclose information with their intended audience in mind, they often find that their actual audience is much larger than that [14, 15]. An analysis of 222,000 users’ audience logs on Facebook shows that users typically underestimate the size of their actual audience as only 27% of its true size [4]. This shows that seeking social support on SNSs might expose personal information to those outside the intended audience. While it is true that SNS users now apply stricter private settings than before [23], these settings give users only some control over their information.

### **Networked Privacy Risk on SNSs**

Marwick and boyd define networked privacy as an “ongoing negotiation of contexts in a networked ecosystem in which contexts regularly blur and collapse” (p. 1063) [17]. One of the most important implications of sharing information in networked settings is that others’ actions can reveal users’ information to a larger network of people, to whom these users may not be directly connected [26]. SNS users can monitor how their direct contacts share information with others (e.g., their mutual contacts and/or other non-direct contacts). For example, if a social support provider tags a support seeker on a public post on Facebook in order to help him or her, this provider’s “Friends” can see that the post has been shared with the support seeker and may be able to infer why that post was shared with him or her. Even with a good intention to help others, social support providers may accidentally share (or “leak”) support seekers’ private information to others in their networks on SNSs. As a result, an unexpectedly larger number of people may gain access to SNS users’ information.

The current definition of networked privacy does not explain how to prevent or manage information leakage to non-direct contacts of users who have already used available privacy settings to restrict their actual audience to match their intended audience, as in the example above. Discussion about how to manage such information leakage can begin in the context of identifying the most ideal source of social support on SNSs. This is an appropriate context for this discussion because seeking social support requires users to balance their need to disclose and their need to maintain boundaries of privacy. While tie strength between the social support seeker and provider may

predict the quality of social support, it cannot be used to predict the support seeker's privacy risk.

### **Effects of Tie Strength and Network Structure on Users' Interest in Others' Information**

Depending on the potential social support provider's network structure, the social support seeker's 2<sup>nd</sup> degree contacts (i.e., the social support provider's direct contacts) may have different levels of interest in the support seeker's information. On SNSs, these 2<sup>nd</sup> degree contacts may gain some unintended access to the social support seeker's information, but this access may have little impact on the social support seeker's risk of experiencing a privacy violation (e.g., others' misuse of personal information, stalking, etc). This is because having access to others' information does not necessarily mean they will notice and/or remember that information for future use. Understanding the effects of tie strength shared between the social support seeker and provider and the support provider's network density can help determine when the 2<sup>nd</sup> degree contacts would have enough interest in the seeker's information to potentially remember and use it later in a way that violates privacy. Assuming that the support seeker's goal is to not only maximize the quality of social support, but also minimize their networked privacy risk, there are four different scenarios for social support seekers to consider when choosing to disclose information on SNSs. These scenarios are described next and summarized in Table 1.

#### *Social Support Providers With Dense Networks*

A potential support provider with a dense network is more likely to share strong ties with his or her network contacts because strong ties and social cohesion often

co-occur [3]. People in cohesive networks promote the norm to cooperate and reciprocate, and strong ties they share may lead them to put in greater effort to transfer knowledge [19]. As they share multiple pathways of communication, information diffuses more quickly in cohesive networks [3, 11, 19]. Seeking social support from a direct contact with a dense network may lead to faster diffusion of potentially sensitive information to other, unintended users.

#### **STRONG TIE VS. WEAK TIE**

If the potential social support provider shares strong ties with both the support seeker and those in his or her network, there is a higher chance for these dense network contacts to be mutual contacts between the support seeker and provider. Sharing mutual contacts or the same social context may increase the relevance of the support seeker's information, thereby increasing others' interest in that information. On the other hand, if the social support seeker shares a weak tie with the potential support provider who is in a generally dense network, the support provider may value the relationship with others in his cohesive network more than the weak tie he or she shares with the support seeker. The lack of trust between two weak ties may provide less motivation to keep the support seeker's information from flowing into the support provider's cohesive network. Thus, seeking social support from a weak tie with a dense network would result in social support that is both lower in quality and increases the networked privacy risk for the support seeker.

#### *Social Support Providers with Sparse Networks*

If the potential social support provider is brokering multiple clusters of connections in a sparse network, more people from different social contexts may have

access to the information provided by the social support seeker. The theory of structural holes suggests that a broker that spans a structural hole has access to resources and information from multiple groups [8, 13]. However, this broker's large set of contacts tends to be disconnected from each other [22]. Brokers are often connected to a large number of people, but they cannot effectively diffuse ideas [11]. Because people in a sparse network communicate less frequently and are more likely to share weak ties, information flows at a slower rate [2]. In such a network structure, the support provider's contacts would have less interest in learning information about others in the network, including that about the social support seeker. As transfer of knowledge is not successful if it is not retained [24], there is less chance for the social support seeker's information to have negative consequences. Without remembering what they saw, these 2<sup>nd</sup> degree contacts are less likely to use that information to harm the social support seeker.

#### STRONG TIE VS. WEAK TIE

A potential social support provider who is a weak-tie contact with a sparse network would have less motivation in general to use his or her resources to help the support seeker. In contrast, if the social support seeker discloses information to a strong tie with a sparse network, this potential support provider may be more trustworthy to not misuse the support seeker's information because the support provider will value his or her strong tie with the support seeker more than weaker ties with other network contacts. Even if the strong-tie support provider's direct contacts in a sparse network (i.e., support seeker's 2<sup>nd</sup> degree contacts) do gain access to the support seeker's information, they may have less interest in paying

attention to information about someone who is not directly connected to them. If the social support seeker's goal is to get high quality social support while minimizing their networked privacy risk, this user would benefit most from reaching out to a strong-tie contact that spans a structural hole between multiple clusters of people (i.e., someone with a sparse network).

		Tie strength with the social support provider	
		Weak	Strong
Social support provider's network density	Sparse	Weak-tie contact with a sparse network	Strong-tie contact with a sparse network
	Dense	Weak-tie contact with a dense network	Strong-tie contact with a dense network

**Table 1:** Tie strengths between social support seekers and social support providers and their network structures.

#### Ideal Source of Social Support on SNSs

If privacy is defined as control over personal information [1, 18], reaching out to a strong-tie contact with a large, sparse network may seem paradoxical. However, as SNS users do not have complete control over the flow of their information due to the networked nature of the platform, the discussion about networked privacy should move beyond understanding dyadic relationships between users that are connected to each

other as direct contacts by choice (e.g., linked “Friends” on Facebook). Even when the support seeker and provider share a strong tie, the support seeker may post sensitive information on the provider’s wall without properly understanding who that information really reaches, or a supportive post by the provider may inadvertently harm the seeker’s desired self-presentation to others in the network (i.e., face threat) [16, 28]. To continue theorizing networked privacy, the discussion should focus not only on the number of people that have access to a particular user’s information, but also on 2<sup>nd</sup> degree contacts’ potential interest in this user’s personal information. Examining network structures of direct contacts—how users’ direct contacts are connected to others (e.g., their 2<sup>nd</sup> degree contacts)—could be an important next step to understanding networked privacy risk on SNSs.

## References

1. Altman, I. (1975). *The environment and social behavior: privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole Publishing Company.
2. Aral, S., & Van Alstyne, M. (2011). The diversity-bandwidth trade-off. *American Journal of Sociology*, *117*(1), 90–171.
3. Balkundi, P., Kilduff, M., Barsness, Z. I., & Michael, J. H. (2007). Demographic antecedents and performance consequences of structural holes in work teams. *Journal of Internet Banking and Commerce*, *28*, 241–260. <http://doi.org/10.1002/job>
4. Bernstein, M. S., Bakshy, E., Burke, M., & Karrer, B. (2013). Quantifying the Invisible Audience in Social Networks. In *CHI 2013*. Paris, France: ACM.
5. Brashers, D. E., Neidig, J. L., & Goldsmith, D. J. (2004). Perceptions of health care providers’ communication: Relationships between patient-centered communication and satisfaction. *Health Communication*, *16*(3), 305–331. <http://doi.org/10.1207/S15327027HC1603>
6. Burke, M., & Kraut, R. (2013). Using Facebook after losing a job: Differential benefits of strong and weak ties. *Proceedings of the 2013 Conference on Computer Supported Cooperative Work*, 1419–1430. <http://doi.org/10.1145/2441776.2441936>
7. Burke, M., & Kraut, R. E. (2016). The Relationship between Facebook Use and Well-Being depends on Communication Type and Tie Strength. *Journal of Computer-Mediated Communication*, *21*(4), 265–281. <http://doi.org/10.1111/jcc4.12162>
8. Burt, R. S. (1992). Structural holes: The social structure of competition. In *Harvard University Press, Cambridge Massachusetts* (pp. 57–91). <http://doi.org/10.1177/0265407512465997>
9. Cobb, S. (1976). Social support as a moderator of life stress. *Psychosomatic Medicine*, *38*(5), 300–314. <http://doi.org/10.1097/00006842-197609000-00003>
10. Ellison, N. B., 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). Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg. <http://doi.org/10.1007/978-3-642-21521-6>
11. Fleming, L., Mingo, S., & Chen, D. (2007). Collaborative brokerage, generative creativity, and creative success. *Administrative Science Quarterly*, *52*(3), 443–475. <http://doi.org/10.2189/asqu.52.3.443>
12. Greenwood, S., Perrin, A., & Duggan, M. (2016). *Social Media Update 2016*.
13. Hargadon, A., & Sutton, R. I. (1997). Technology Brokering and Innovation in a Product Development

- Firm. *Administrative Science Quarterly*, 42(4), 716.  
<http://doi.org/10.2307/2393655>
14. Litt, E. (2012). Knock, Knock . Who's There? The Imagined Audience. *Journal of Broadcasting & Electronic Media*, 56(3), 330-345.  
<http://doi.org/10.1080/08838151.2012.705195>
  15. Litt, E., & Hargittai, E. (2016). The Imagined Audience on Social Network Sites. *Social Media + Society*, 1-12.  
<http://doi.org/10.1177/2056305116633482>
  16. Litt, E., Spottswood, E., Birnholtz, J., Hancock, J., Smith, M. E., & Reynolds, L. (2014). Awkward encounters of an "other: kind: Collective self-presentation and face threat on facebook. In *CSCW*. Baltimore, MD: ACM.  
<http://doi.org/http://dx.doi.org/10.1145/2531602.2531646>
  17. Marwick, A., & boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, 16(7), 1051-1067.  
<http://doi.org/10.1177/1461444814543995>
  18. Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.
  19. Raegans, R., & Mcevely, B. (2003). Knowledge Transfer : Ray Reagans. *Administrative Science Quarterly*, 48(2), 240-267.  
<http://doi.org/10.2307/3556658>
  20. Rains, S. A., & Keating, D. M. (2011). The Social Dimension of Blogging about Health: Health Blogging, Social Support, and Well-being. *Communication Monographs*, 78(4), 511-534.  
<http://doi.org/10.1080/03637751.2011.618142>
  21. Rozzell, B., Piercy, C. W., Carr, C. T., King, S., Lane, B. L., Tornes, M., ... Wright, K. B. (2014). Notification pending: Online social support from close and nonclose relational ties via Facebook. *Computers in Human Behavior*, 38, 272-280.  
<http://doi.org/10.1016/j.chb.2014.06.006>
  22. Sosa, M. E. (2011). Where Do Creative Interactions Come From? The Role of Tie Content and Social Networks. *Organization Science*, 22(1), 1-21.  
<http://doi.org/10.1287/orsc.1090.0519>
  23. Stutzman, F., Gross, R., & Acquisti, A. (2012). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*, 4(2), 7-41.
  24. Szulanski, G. (1996). Exploring Internal Stickiness: Impediments to the transfer of Best Practice Within the Firm.pdf. *Strategic Management Journal*, 17, 27-43.
  25. Thoits, P. A. (2011). Mechanisms Linking Social Ties and Support to Physical and Mental Health. *Journal of Health and Social Behavior*, 52(2), 145-161. <http://doi.org/10.1177/0190272512467653>
  26. Vitak, J., Wisniewski, P., Page, X., Lampinen, A., Litt, E., De Wolf, R., ... Sleeper, M. (2015). The future of networked privacy: Challenges and opportunities. In *CSCW* (pp. 1-6). Vancouver, BC: ACM.
  27. Vitak, J., Ellison, N. B., & Steinfield, C. (2011). The ties that bond: Re-examining the relationship between Facebook use and bonding social capital. In *Hawaii International Conference on System Sciences* (pp. 1-10).
  28. Wohn, D. Y., & Spottswood, E. L. (2016). Reactions to other-generated face threats on Facebook and their relational consequences. *Computers in Human Behavior*, 57, 187-194.  
<http://doi.org/10.1016/j.chb.2015.12.021>