Privacy in Online Social Networking at Workplace

Yang Wang
Department of Informatics
University of California, Irvine
yangwang@uci.edu

Alfred Kobsa
Department of Informatics
University of California, Irvine
kobsa@uci.edu

***Abstract*—Employees using social network sites (SNS) at workplace is a fact. As companies are further embracing social media, how if at all does this practice affect the work dynamics? While privacy has been a hot topic in online social network research in general, there is little work investigating the privacy aspect of this practice at workplace. This paper aims at starting the groundwork towards filling the gap. Based on a review of existing literature in social networks and workplace studies, we hypothesize a number of potential privacy issues in this work practice and suggest future research directions in this area.**

Keywords: social network site, workplace, privacy.

I. INTRODUCTION

A recent report shows that there is a significant amount of usage of SNS at workplace - 51% of users visit these sites at least once per day; 79% and 82% of users use these services at work for business and personal reasons, respectively [1]. What does this mean? How if at all does this work practice may change the work dynamics? The remainder of this paper is organized as follows. We will first discuss the characteristics of workplace SNS use in Section II, then summarize privacy issues identified in general SNS use in Section III. Building upon the two previous sections, we will outline and hypothesize potential privacy issues in SNS use at workplace in Section IV and provide an outlook of future research in this area in Section V. Finally we will conclude in Section VI.

II. USE OF SOCIAL NETWORK SITES AT WORK

There are two types of online social networks that may be used at work and it is important to make a distinction between them. The first type is *general* SNS that are open to the public for registration, e.g., Facebook. The second type is *enterprise* SNS that is internal to the particular corporate and thus only open to its employees, e.g., IBM Beehive [2]. As SNS are gaining momentum in enterprises, scholarship around the usage of online social networks at workplace has just started to emerge such as [3] [4] [5] [6] [7].

Who Uses What?

According to an online survey study [1], in the workplace, LinkedIn is the predominate SNS used for work-related purposes, while YouTube and Facebook are the leading SNS used for personal purposes. The report also notes that for users who access Facebook at work, Facebook group is the most popular activity for work-related purposes, while photo sharing and tagging are the most commonly cited activities for personal purposes.

Skeels and Grudin [5] recently conducted a study of Microsoft employees' workplace use of Facebook and LinkedIn and found that while current or recent students frequent Facebook, young professionals tend to use LinkedIn, and older professionals especially those with "established career, families and social networks" have little interest in using online social networks.

Reasons to Use

For general SNS usage at work, Skeels and Grudin [5] found that Microsoft employees use Facebook extensively to "maintain awareness of colleagues and to build rapport and stronger working relationships".

For enterprise SNS usage at work, DiMicco et al. [3] found that IBM employees use their internal social network, Beehive, mainly as a social tool "to strengthen their weak ties and to reach out to employees they do not know". They suggested that the motivations for employees to do this include "connecting with coworkers at a personal level, advancing their careers, and campaigning for their projects".

Motivate Contributions

To explore ways to encourage employees' contributions on Beehive, Farzan et al. [6] prototyped and integrated a point-based incentive mechanism on Beehive. Basically, users will earn points if they contribute content on the site, and as they have more points, their status may be upgraded to the next level (e.g., from new-bee to busy-bee). In studying the effect of their incentive mechanism, they found that while employees were initially motivated to add more content to the site, the persuasive effect quickly decayed.

In a study of Hewlett-Packard employees' usage of internal social media at work, Brzozowski et al. [4] found that others' attention to submitted content plays an important role in motivating employees to contribute to company-internal social media. They suggested that managers should "lead by example" in promoting use of internal social media, and that making attention visible would encourage employees' participation.

Identity and Impression Management

Employees who use general SNS may have friends on the sites both from their personal social circles as well as their professional contacts. How then if at all do they manage different identities for their different kinds of contacts? In a study of IBM employees who frequently use Facebook, DiMicco and Millen [7] identified three distinct groups of users

mainly based on the content of their profiles: (1) "College Days" are users who belong to a large number of school networks and have few connections in their professional networks; (2) "Dressed to Impress" are users who have a higher number of corporate members than personal friends on the site; and (3) "Living in the Business World" are users who are newest to Facebook, share very little information on the site, and present themselves on the site as professionals. Some of the study informants said to use different profiles to cater to different audiences, while others claimed to carefully clean up their Facebook footprints from the "college days". Despite Facebook's support in having multiple profiles and having control over who gets to see what, their study uncovered difficulties of users in attempting to maintain multiple identities and profiles for both personal and professional use on the site.

The Beehive point-based incentive study [6] mentioned earlier also found evidences of people carefully crafting their status such as "I have to be above other people that I work with" and "I didn't want to be a new-bee…I wanted to be a busy-bee." Once a user reaches her ideal status in the system, her points and status will stay the same even if she stops contributing. This reduces the motivation to moving forward as a user noted "I stopped contributing right after getting to busy-bee level". This gives a reason why their point-based incentive only has such a short-lived effect.

Benefits of Using SNS at Work

From these studies we can see that SNS usage at workplace is mostly for social purposes. In other words, employees generally do not use SNS at work to seek information or get answers to the questions that they may have.

We see several benefits of using SNS at workplace from these studies such as better connecting with co-workers and getting to know other employees. According to a recent study[1] conducted by Brent Coker [8], short and unobtrusive periods of using Twitter or Facebook at work or in general ""workplace Internet leisure browsing" as the researcher put it, may help employees get refreshed and keep focused and thus increase their productivities.

Tensions of Using SNS at Work

Contrary to the possible productivity benefit aforementioned, companies may deem SNS use at work as illegitimate or inappropriate. Skeels and Grudin [5] noted that a Microsoft Directive in 2004 considered the use of Plaxo or LinkedIn "a violation of company policy" on the basis of security risks but now more than one third of the company employees use LinkedIn.

Besides the issue of having identities on SNS for both personal and professional purposes, Skeels and Grudin [5] also pointed out two other related tensions. One is the tension from "crossing hierarchy, status, and power boundaries" within their personal sphere and within their professional sphere. For instance, imagine the situation in which one's parents, children, and personal friends on the Friend list at the same SNS. Another tension is the possibility of divulging company confidential information on general SNS.

III. PRIVACY IN ONLINE SOCIAL NETWORKS

In this section, we briefly review identified issues related to privacy in general SNS in existing literature.

Privacy Risks

Rosenblum [9] argued that Internet users "lack any realistic sense of how public or how permanent the record of" their posts online is. We have already seen incidents that contents on SNS have been used by employers and law enforcement to assess users. Once contents have been put up on SNS, even if they got deleted by the users, the SNS operators or even external web archive can still save copies of the contents which may be taken out of context and can have negative impact on the users in the future.

The fact that users can use pseudonymous user names on SNS further magnify the illusion that they will not be accountable for what they say or act on SNS. However, Liu and Maes [10] showed that pseudonymous users may be identified through face *re-identification*, in which the same user uses the same or very similar picture on different social network sites. Narayanan and Shmatikov [11] demonstrated an algorithm purely based on network topology that can de-anonymize users on social networks with very low error rate (in one study of Twitter users, the error rate was 12%). Gross and Acquisti [12] pointed out that other risks range "from identity theft to online and physical stalking, from embarrassment to price discrimination to blackmailing". Chew et al. [13] raised three privacy-sensitive areas in social networks: lack of control over activity streams, unwelcome linkage, and deanonymization through merging of social graphs.

Users' Behavior towards Information Sharing and Privacy

Gross and Acquisti [12] found that for the majority of CMU Facebook users, their personal data is generously provided and only a very small percentage of them change the default privacy settings on the site.

Certainly, there are notable differences across social networks, genders, and socio-economic groups of users. Dwyer et al. [14] found that Facebook users have a greater sense of trust in Facebook and in other members on Facebook and thus reveal more information, however despite their lower trust MySpace users are more likely to extend online relationships beyond the confines of MySpace. Fogel and Nehmad [15] observed that in general men have less privacy concerns than their female counterparts and thus tend to disclose more personal information such as telephone number and physical address on SNS. In a study of MySpace users, Gilbert et al. [16] found that rural users have less friends and fewer comments than urban users. Besides, rural users, particularly women, have a higher level of privacy concern and use privacy setting more than urban users.

Legal Implications

[1] We did not find a published paper of this study.

Identify applicable sponsor/s here. *(sponsors)*

From a legislative point of view, privacy in social networks poses unique challenges than online privacy in general. This is because users largely provide their information on social networks at their own initiatives (thus can be treated as their consent). Traditional privacy laws based "informed consent" protect users against unfair or disproportional data collection and usage by the websites would be ineffective in this new arena. Therefore, it is not clear how these privacy legislations would apply in SNS.

IV. POTENTIAL PRIVACY ISSUES IN SNS AT WORK

Most existing literature in SNS use at workplace either did not explicitly discuss privacy issues or commented that privacy is less of an issue. For example, DiMicco et al. [3] noted that they did not find privacy concerns from their study of Beehive. However, they only studied Beehive users and thus it is possible that the fact that some employees did not adopt Beehive was partly due to their privacy concerns. Therefore, it is also important to study employees who choose not to use SNS at work.

We believe the privacy landscape in the enterprise context is convoluted. From the employee's perspective, there are three types of privacy threats. First, there is privacy among individual users. In the corporate context, they can be your superiors, subordinates and peers. Secondly, there is privacy between users (employees) and their employers. What if the company keeps track of employees' computer usage at work? How would an employee's interactions with contacts from her personal circle on SNS affect the impressions that their employers have on them and even the assessment of their work performance. Thirdly, there is privacy between users and SNS operators[2]. From the privacy policies of popular general SNS, it is not clear if the operators can/will transfer or sell the contents on SNS to third parties, but our impression is that the operators still keep this option open.

Based on the discussion of the two previous sections, we identify the following privacy-related issues that need to be further investigated.

Impression Management

From existing literature we know that impression management plays an important role in employees' everyday work and also in SNS use at work. How do they manage their self-representations simultaneously at a SNS with regard to their personal contacts including family members, professional contacts including their peers, superiors and subordinates, and SNS operators is an open research question.

Pressure to Reveal Personal/Working Information

Brzozowski et al. [4] suggested that in order to encourage adoption of internal social media in an enterprise context, managers should "lead by example". We suspect this may put managerial and/or peer pressure on employees to contribute contents on enterprise SNS.

[2] For enterprise SNS, the operators are the employers.

Unintentional Social Undermining in Workplace

Baron [17] argued that interpersonal relationship and interaction are a critical factor affecting the workplace performance. Duffy et al. [18] showed that social undermining in workplace can be quite dramatic. They defined social undermining as "behavior *intended* to hinder, over time, the ability to establish and maintain positive interpersonal relationships, work-related success, and favorable reputation". We define *unintentional social undermining* as behavior that is not intended but practically cause social undermining effect. While (intentional) social undermining may be rare on SNS use at work since adding people to one's friend list are controlled by the users (they probably would not add people who they have negative relationships with), we suspect that unintentional social undermining on SNS can be more frequent. For example, tagging colleagues on photos may cause embarrassment. Besmer and Lipford [19] found that a common reason why people untagged photos is that they did not look good on these photos. Unintentional social undermining can seriously affect employees' carefully crafted self-representations. SNS at work can be a double-edge sword: it can encourage social support among co-workers but it can also lead to unintentional social undermining in workplace.

V. FUTURE DIRECTIONS

In this section, we outline some future research directions in this area.

Holistic and Longitudinal Studies

Dourish and Anderson [20] suggested a more holistic view of privacy and security, not simply as technical phenomena but rather as manifestations of collective information practices that are embedded in social and cultural contexts. We believe that studies that take on broad inquiries of everyday work practices in the era of SNS are needed. We also suspect that the impacts of SNS use at workplace in general and the privacy-related issues discussed above in particular may take some time to emerge, therefore we need longitudinal studies to better understand them.

Trust and Privacy Model

Gilbert et al. [16] advocated an incremental trust model for online social networks that mimics interpersonal relationship development in the real world. The mixing of different types of contacts and the crossing of power boundaries in SNS at work need more delicate trust and privacy models to capture the nuisances.

Tools Support

Dwyer and Hiltz [21] found that despite the regular occurrences of privacy incidents, built-in privacy management tools were not extensively used to protect users' privacy and thus suggested evidences of their poor design. Innovative tools are needed to better support the complex impression management on SNS at work. Gilbert and Karahalios [14] proposed a privacy control mechanism based on automatic and dynamic prediction of tie strengths among friends on SNS. These predictions can be used as smart defaults for privacy

control, e.g., share a piece of sensitive information only with strong ties. We believe that this is a promising direction since users are not likely to bother with often overly complicated privacy settings.

VI. Conclusion

As SNS use are becoming more popular at workplace (just like email and instant messaging). Its impacts still need to be closely studied. Current literature seems to suggest that privacy is not really an issue in SNS at work, but we argue that this may not be the case. Privacy issues may be at the background and only manifest through other issues such as impression management. To add to the literature, we hypothesize a number of potential privacy-related issues including complex impression management, pressure to disclose more information on SNS, and unintentional social undermining. These issues may be closely related with other workplace issues such as work performance and they may develop over time. Therefore, we need more holistic and longitudinal studies to better understand them and more delicate and usable designs and tools to support users' collective information practices at work.

References

[1] FaceTime, *The Collaborative Internet: Usage Trends, End User Attitudes and IT Impact*, 2008.

[2] J. DiMicco, W. Geyer, D. Millen, C. Dugan, and B. Brownholtz, "People Sensemaking and Relationship Building on an Enterprise Social Network Site," *HICSS '09, 42nd Hawaii International Conference on System Sciences*, 2009, pp. 1-10.

[3] J. DiMicco, D.R. Millen, W. Geyer, C. Dugan, B. Brownholtz, and M. Muller, "Motivations for social networking at work," *Proceedings of the ACM 2008 conference on Computer supported cooperative work*, San Diego, CA, USA: ACM, 2008, pp. 711-720.

[4] Michael J. Brzozowski, Thomas Sandholm, and Tad Hogg, "Effects of Feedback and Peer Pressure on Contributions to Enterprise Social Media," *Proceedings of the 2009 International conference on Supporting Group Work*, Sanibel Island, FL, USA: ACM Press, 2009, pp. 61-70.

[5] Meredith M. Skeels and Jonathan Grudin, "When Social Networks Cross Boundaries: A Case Study of Workplace Use of Facebook and LinkedIn," *Proceedings of the 2009 International conference on Supporting Group Work*, Sanibel Island, FL, USA: ACM Press, 2009, pp. 95-104.

[6] R. Farzan, J.M. DiMicco, D.R. Millen, C. Dugan, W. Geyer, and E.A. Brownholtz, "Results from deploying a participation incentive mechanism within the enterprise," *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, Florence, Italy: ACM, 2008, pp. 563-572.

[7] J.M. DiMicco and D.R. Millen, "Identity management: multiple presentations of self in facebook," *Proceedings of the 2007 international ACM conference on Supporting group work*, Sanibel Island, Florida, USA: ACM, 2007, pp. 383-386.

[8] Reuters, "Facebook, YouTube at work make better employees: study," *Reuters*.

[9] D. Rosenblum, "What Anyone Can Know: The Privacy Risks of Social Networking Sites," *IEEE Security and Privacy*, vol. 5, 2007, pp. 49-40.

[10] H. Liu and P. Maes, "Interestmap: Harvesting social network profiles for recommendations," *In Proceedings of the Beyond Personalization 2005 Workshop*, 2005.

[11] A. Narayanan and V. Shmatikov, "De-anonymizing Social Networks," 2009, www.cs.utexas.edu/~shmat/shmat_oak09.pdf.

[12] R. Gross, A. Acquisti, and I.I.I. H. John Heinz, "Information revelation and privacy in online social networks," *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, Alexandria, VA, USA: ACM, 2005, pp. 71-80.

[13] Monica Chew, Dirk Balfanz, and Ben Laurie, "(Under)mining Privacy in Social Networks," 2008, http://w2spconf.com/2008/papers/s3p2.pdf.

[14] C. Dwyer, S. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," *Proceedings of the Thirteenth Americas Conference on Information Systems*, Keystone, CO, USA: 2007.

[15] J. Fogel and E. Nehmad, "Internet social network communities: Risk taking, trust, and privacy concerns," *Computers in Human Behavior*, vol. 25, Jan. 2009, pp. 153-160.

[16] E. Gilbert, K. Karahalios, and C. Sandvig, "The network in the garden: an empirical analysis of social media in rural life," *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, Florence, Italy: ACM, 2008, pp. 1603-1612.

[17] Baron R. A., "Interpersonal relations in organizations," *Individual differences*, San Francisco: Jossey-Bass, 1996, pp. 334-370.

[18] M.K. Duffy, D.C. Ganster, and M. Pagon, "Social Undermining in the Workplace," *The Academy of Management Journal*, vol. 45, Apr. 2002, pp. 331-351.

[19] A. Besmer and H. Lipford, "Tagged photos: concerns, perceptions, and protections," *Proceedings of the 27th international conference extended abstracts on Human factors in computing systems*, Boston, MA, USA: ACM, 2009, pp. 4585-4590.

[20] P. Dourish and K. Anderson, "Collective information practice: emploring privacy and security as social and cultural phenomena," *Hum.-Comput. Interact.*, vol. 21, 2006, pp. 319-342.

[21] C.A. Dwyer and S.R. Hiltz, "Designing Privacy into Online Communities," *SSRN eLibrary*, Oct. 2008, http://ssrn.com/abstract=1305278.