When SNS Privacy Settings Become Granular: Investigating Users' Choices, Rationales, and Influences on Their Social Experience

YAO LI, University of California, Irvine, USA
XINNING GUI, University of California, Irvine, USA
YUNAN CHEN, University of California, Irvine, USA
HENG XU, American University, USA
ALFRED KOBSA, University of California, Irvine, USA

Privacy researchers have suggested various granular audience control techniques for users to manage the access to their disclosed information on social network sites. However, it is unclear how users adopt and utilize such techniques in daily use and how these techniques may impact social interactions with others over time. In this study, we examine users' experience during everyday use of granular audience control techniques in WeChat, one of the most popular social network applications in China. Through an interview study with 24 WeChat users, we find that users adjust their configurations and develop rationales for these configurations over time. They also perceive mixed impacts of WeChat's privacy settings on their information disclosure and social interactions, which brings new challenges to privacy design. We discuss the implications of these findings and make suggestions for the future design of privacy settings in SNSs.

CCS Concepts: • **Human-centered computing → Collaborative and social computing;** *Empirical studies in collaborative and social computing*

KEYWORDS

Privacy settings; social network sites (SNSs); audience control; information disclosure; social interaction

ACM Reference format:
Yao Li, Xinning Gui, Yunan Chen, Heng Xu and Alfred Kobsa. 2018. When SNS Privacy Settings Become Granular: Investigating Users' Choices, Rationales, and Influences on Their Social Experience. In *Proceedings of the ACM on Human-Computer Interaction,* Vol 2, No. CSCW, Article 108 (November 2018). ACM, New York, NY. 21 pages. https://doi.org/10.1145/3274377.

1 INTRODUCTION

Information privacy has long been a concern for users of social network sites (SNSs). SNSs allow users to share an enormous amount of information with other SNS users [12], which makes it more difficult to keep personal information private in online interpersonal interactions. This is because in SNSs, different types of audiences are at first pooled into a single group, "SNS friends", making it possible for users to disclose inappropriate information to unwanted audiences [13,18],

This work is in part supported by the National Science Foundation grant SES-1423629.
Author's addresses: Yao Li, University of California, Irvine, CA, USA; email: yao.li@uci.edu; Xinning Gui, University of California, Irvine, CA, USA; email: guix@uci.edu; Yunan Chen, University of California, Irvine, CA, USA; email: yunanc@ics.uci.edu; Heng Xu, American University, DC, Washington, USA; email: xu@american.edu; Alfred Kobsa, University of California, Irvine, CA, USA; email: kobsa@uci.edu.

 2573-0142/2018/November - ART108 $15.00 https://doi.org/10.1145/3274377

which is called "context collapse" [22]. Failure to control the information flow to the desired audience may lead to reputation damage, rumors, unwanted contact, harassment, stalking, and identity theft [6]. To mitigate such issues and their associated privacy concerns, several SNSs provide audience control techniques with fine-grained options for users to capture the granularities of online social contexts and to selectively disclose information to desired audiences. Prominent examples are Facebook's Friend List [15] and Google+'s Circles [32], which allow for the creation of (possibly overlapping) friend *subgroups*. Such techniques are considered more granular than coarse-grained options, such as "friends only", "everyone", and "friends of friends".

Researchers have studied the usage of these techniques and the mechanisms users apply to configure these techniques. For example, users can manage audiences based on closeness of relationship and topical interest in Facebook's Friend List [16] and Google+'s Circle [14]. However, these studies have not investigated whether and how users modify their mechanisms and configuration of privacy settings over time. Moreover, no study has examined how the usage of granular audience control techniques would impact users' information disclosure and online social interaction with others in naturalistic settings. Without such knowledge, it is hard for researchers and practitioners to evaluate the effectiveness of such techniques and to improve their future designs.

Our study aims to address this research gap. We are interested in users' behaviors in their everyday use of granular audience control techniques in SNSs. Particularly, we want to investigate how and why users configure privacy settings and how these behaviors impact their information disclosures and online social interactions with others over time.

To address these research questions, we conducted an interview study with WeChat users in China. WeChat is one of the most popular social network applications in China. In November 2017, WeChat users made 68 million daily posts and sent 38 billion daily messages [29]. Similar to Facebook, WeChat allows its users to share status updates, display their timelines, message others, manage social relationships, read news, and install applications. Compared to Facebook and Google+, WeChat offers more granular audience control techniques that allow users maximal customization to accommodate their fine-grained online social contexts. Users, whether inside or outside one's contact list, will have no access to one's posts in WeChat if their access is blocked. Hence, WeChat is an ideal environment to investigate users' evolving configurations of audience control and the associated impact of these configurations on information disclosure and social interaction in a naturalistic setting.

We interviewed 24 participants who had used WeChat for at least a year. We explored their usage of WeChat's audience control techniques and the perceived impact of this usage on their disclosure behavior and social interaction. We found that users' configurations and the rationale behind their configurations evolve over time due to changing social contexts. Additionally, users' configurations of audience control have various impacts on their online information disclosure and social interactions with others, which in turn prompts them to adjust their configurations and their rationales for these configurations. Our contributions are three-fold: 1) we examine users' evolving perceptions and behaviors in their interaction with privacy settings in a real system that they have used over a long period of time; 2) our rich empirical findings reveal new challenges produced by everyday use of granular privacy settings in users' social interaction with others; 3) we derive implications for future privacy design.

2 BACKGROUND

2.1 Audience Control Techniques

Users disclose an enormous amount of personal information on SNSs, such as basic demographic information (gender, birthday, hometown), contact information, personal information (interests, likes, personality), photos, friend list, status updates, and one's timeline [2]. Thus, many are concerned that their identifiable information can be accessed by unwanted audiences [27], causing unexpected consequences such as online stalking, bullying, identity theft, embarrassment, and so on [12,23]. To mitigate these issues and concerns, many SNSs provide privacy settings to empower users' control over who can see what they disclose, which is known as audience control [8,30].

Some early examples of audience control focused on providing control over the level of "visibility" of one's information disclosure. For example, Facebook allows users to change the visibility of the posts and profiles from every registered user to friend only. However, such privacy settings have been criticized for not being able to reflect the granularities in our social life [20,34]. In offline face-to-face communications, individuals adapt their information disclosure based on who is in their actual audience [11]. But in SNSs, different types of the audience are combined into a single group of "SNS friends", even though users have different disclosure preferences for those that they meet in distinct contexts [16]. Hence, users often underestimate the size of their audience [22,27].

To solve the gap between the granularity of offline social contexts and those on SNSs, researchers and practitioners have proposed privacy designs that grant users finer-grained control over the audience of their posts [5,17,20]. For example, when users post content on their Facebook pages, they have different granularities to control the audience: Only Me, Specific friends, Friends Except (do not show to some friends), Friends Only, and Public [20]. They can also customize a subset list of friends, name it, and use it to control the audience of their posts [35]. For past Facebook posts, users can choose to limit the audience to their friends only. Users can also add a friend to the restricted list to prevent this person from seeing Facebook posts. More recently, Facebook has allowed users to control the audience of their friend list, Newsfeed, others' comments on their timeline, and tagged posts, similar to how they control their own posts. Another example of such designs is "Circles" on Google+. Users group contacts into different circles. The default circles in Google+ are friends, family, acquaintances and followers [35]. By customizing their own circles, users can control with whom they share content and filter incoming content from contacts [14,35].

However, several flaws of such granular settings have been documented. First, the default categories of these settings are still coarse-grained, inadequately reflecting the granularities of social contexts. Second, cross-referencing features in SNSs, such as tagging, can leak information to people outside targeted online social networks. On Facebook, for example, anyone tagged in past posts and their friends can still access these posts even when a user restricts access to past posts. Facebook friends who have been added to the restricted list to prevent them from seeing a user's posts can still see things shared with the public or with mutual friends.

Compared with these SNSs, WeChat is a semi-closed sphere where information sharing happens mostly within users' contacts. It offers highly granular privacy settings for its users to control the audience of their information disclosures much more tightly than is possible in either Facebook or Google+. We will describe these points in the following section.

2.2 WeChat's Audience Control Settings

WeChat is a popular mobile social network application whose vast majority of users reside in China. WeChat started out as an instant messaging system but evolved to become China's biggest

social network application (it hit one billion monthly users in March 2018 [38]). WeChat users can share status updates, manage social relationships, read news, install applications, make payments, and so on. It has become integral to the daily lives of many people in China [29].

"WeChat contacts" refers to people who have been accepted to a WeChat user's contact list. Those can range from known ties to strangers. Status updates are called "Moments" in WeChat (Figure 1 shows its interface). In Moments, users can share posts of photos, text, videos, links, and so on, and view, like and comment on their contacts' posts. However, different from Facebook where friends of friends, or even the public can access one's posts, WeChat only allows one's WeChat contacts to "like" and comment on one's Moments. Users can only access likes and comments made by mutual contacts between themselves and the authors of Moments, rather than by people beyond their contact lists (e.g., friends of friends, the public). People outside of one's contact lists cannot leave likes and comments on one's Moments, though they can be allowed to view-only if users relax their privacy restrictions on strangers. Generally, WeChat is a semi-closed sphere where information sharing happens mostly among users' contacts.

Figure 1. WeChat Moments interface.

WeChat provides several privacy settings for users to control audience access to their Moments, even within their contacts. The first feature is "tags", which allows users to control the audience of a particular Moment. Tags is similar to Facebook's customized friend list and Google+'s customized circle. Users need to create a tag first, name it, and assign WeChat contacts to this tag. They can assign several contacts to one tag at once, or assign them contact by contact. Before posting a Moment, they can control the audience by selecting tag(s) that contain the desired contacts. Once the Moment is published, only the contacts in the selected tag(s) can view, like, and comment on the Moment. "Tagged out" contacts, who are not on the tag(s) because they have never been added to or have been removed from the tag(s), will not see that Moment. Figure 2 compares a viewer's interfaces of one's Moments page before and after the application of Tags. Once Moments have been published they will remain unchanged. Even if the selected tags are modified in future, the audience of published Moments will not be altered. Users can edit the existing tag(s) by changing a tag's name, adding or removing its members, or deleting the entire tag(s). Compared with Facebook's audience control, which offers five default options for users to

limit who can see a particular post, "tags" asks users to create their own lists without offering default options. The created lists can be as granular as users want, and thus can be tailored to users' specific needs.

Figure 2. Moments visible to someone who is tagged out (left figure) and who is not (right figure). The Moment highlighted in square is not shown in the left figure because that viewer is tagged out.

Figure 3. Interface for viewers not on the "Don't Share" list (left) vs. on the "Don't Share" list (right).

The second audience control feature is "Don't share my Moments" (referred to as "Don't share" in the rest of the paper), by which users can completely block contact(s) from accessing all of their past and future Moments, as opposed to "tags," which only affect particular Moment(s). Users can simply add contact(s) to or remove contact(s) from their "Don't share" list. Those who are on one's "Don't share" list can only see a blank page with a gray line in someone's Moment (see Figure 3). Compared to Facebook's blocking features where restricted users can still see posts one shares publicly or on a mutual friend's timeline, "Don't share" completely blocks its listed contacts.

Figure 4. Viewer's Interface on July 5, when not using any Time Limit (left) vs. using a 3-day Time Limit (right).

The third feature is "Time Limit", through which users can set a time limit for their past Moments. The current options are to limit posts to three days, to 6 months, or to assign no limit. Moments posted before the selected time limit will be hidden from all contacts. Once users set a time limit for their past Moments, their contacts will see the notice "Only x days of Moments are viewable" on their Moments page (see Figure 4 for an example). Compared with Facebook's audience control for past posts where all old posts are still visible on the timeline, though limited to friends only, "time limit" can hide all old posts from anyone.

The last feature is "Hide Moments", similar to Facebook's "unfollow." When a user adds a contact to their "Hide Moments" list, Moments updates by that contact will not be shown to this user. It is a way to keep someone on one's contact list but hide their Moments from one's view. This feature is different from the others as it does not control one's own audience but rather oneself as an audience.

Compared to Facebook's privacy settings, WeChat allows some granular audience control features to apply to future and past posts. With these privacy settings and the fact that information sharing takes place mostly within users' contacts, WeChat allows users to restrict unwanted audiences as much as possible from accessing their Moments.

3 RELATED WORK

Several studies have investigated users' rationale behind the use of granular audience control techniques. These studies found that most users configure these controls based on types of social relationships [15,16,25], closeness [14,25,36], interest [14,25], and co-location of contacts [35,36]. For example, they tend to create groups such as "work", "school", "family", "close friends", "church friends", etc., and selectively disclose information to these groups [16,25,35]. While these techniques were designed to better target users' information disclosure to the desired audience, users complained about the great amount of labor involved, such as the upfront time investment [3,37], recurring efforts [16,27], and insufficient self-efficacy in privacy management [31]. Some users would configure these settings at some point, but tended to use them only once or stop maintaining them [25]. They would rather adopt the default categories, such as "friends only", "friends of friends'", and "public" [25], or use alternative strategies, such as creating multiple accounts [28] and simply limiting disclosure [15].

However, these findings do not fully capture users' long-term perceptions and practices of using granular audience control techniques in naturalistic settings. First, two of these studies investigated the mechanisms by asking users to segregate their Facebook friends as an experimental task [16,36]. Another two studies were based on users' interactions with prototypes of these techniques [5,17]. Second, in other studies that asked participants about their past usage of these techniques for their posts, a few participants reported limited past experience with these techniques [3,16,19,25,35,37]. For example, one study showed that participants configure the settings, but never had a situation where they actually needed to control the audience [16]. Thus, they did not reflect users' long-term experience about SNS granular audience control. Third, several studies found that the low usage of the granular settings was due to the great amount of effort involved in first-time configuration [3,37]. These studies however did not investigate how users' perception of these burdens evolved over time, nor how users would trade off these burdens with the benefits of high granularity of audience control after long-term experience with these techniques. Hence, we have limited knowledge of how users' perceptions and attitudes towards these granular privacy settings evolve over time.

Additionally, little work has been done to investigate the impact of using granular audience control on users' information disclosure and social interaction with others in SNSs. Most prior studies focus on how users struggled in managing online social contexts and understanding existing granular audience control techniques [25–27]. It remains an open question whether adopting these granular settings would assist or rather impede users' online social interaction in SNSs. This makes it difficult for SNS providers to improve the design of audience control.

4 METHODOLOGY

We conducted 24 semi-structured interviews with WeChat users from December 2017 to February 2018. Two authors first developed the interview protocol, and conducted pilot studies with nine participants. Based on the pilot studies, they refined the interview protocol and conducted 24 interviews formally. We recruited interviewees through direct contact and snowball sampling. All interviewees were Chinese WeChat users who participated voluntarily without compensation. Their demographic data and their familiarity with WeChat audience control features can be found in Table 1.

The interviews were conducted through WeChat audio chat in Mandarin. The average length of the interviews was 40 minutes. We started with general questions, such as questions about demographics, length of WeChat use, frequency of usage, number of WeChat contacts, and

frequency of sharing Moments. We then asked the interviewees about the contents they posted in Moments and how they controlled the audience of their Moments through WeChat privacy settings. We particularly asked how long they had used the settings, what motivated them to use them, how they configured their settings when they posted Moments, whether they revisited the settings, what they perceived as the impact of privacy settings, and how they behaved after choosing a setting. There were a few users who had never heard of or used the privacy setting(s) to control their audience. We did not exclude these participants, but rather asked them why they choose not to use the privacy settings. We transcribed all the interviews in Mandarin.

Table 1. Demographics of interviewees (**: have used the feature; *: know the feature, but have not used; -: do not know the feature)

#	Gender	Age	Occupation	Length of Use (year)	# Contact[2]	Tags	Don't share	Hide Moments	Time limit
1	Female	32	Human Resource Manager	5	400	**	**	*	*
2	Male	20	Student	4	127	**	**	*	*
3	Female	20	Student	4	245	**	*	*	*
4	Female	20	Student	5	1000	**	*	*	*
5	Male	30	Engineer	5	200	**	**	*	*
6	Male	40	Engineer	3	200	**	*	*	**
7	Female	32	Human Resource Manager	5	100	**	*	*	*
8	Female	30	Teacher	4	150	*	**	*	*
9	Female	27	Analyst	5	300	*	**	*	-
10	Male	56	Public service worker	4	300	**	*	**	**
11	Female	37	Manager	4	1160	*	*	**	**
12	Female	29	Teacher	7	200	**	**	**	**
13	Male	32	Manager	5	302	*	*	**	*
14	Male	23	Pastry Chef	5	186	**	*	**	*
15	Male	29	Student	7	398	*	**	**	**
16	Female	30	Analyst	7	390	*	*	*	*
17	Female	28	Student	7	530	**	**	*	*
18	Female	28	Database Admin	8	308	**	*	*	*
19	Female	31	Researcher	8	425	**	**	*	**
20	Female	59	Retired	4	300	*	*	-	-
21	Female	49	Retired	4	47	*	**	-	**
22	Male	32	Researcher	4	98	**	*	*	*
23	Female	32	Editor-in-Chief	7	500	**	**	**	*
24	Female	55	Judge	4	200	**	**	**	**

[2] A few interviewees reported the exact number of contacts in their WeChat, while most reported the approximate number.

To identify themes that were strongly linked to our data, we applied thematic analysis [7] in an inductive approach [21]. Two researchers (including the first author) are familiar with WeChat and participated in the analysis. We first familiarized ourselves with the data and intensively read the data while marking ideas. The two researchers had several regular daily meetings to discuss the ideas. Each then individually assigned initial codes across the whole dataset. Next, we compared our initial code lists through discussion and combined them into a single list. As suggested by Braun and Clarke [7], we generated as many potential themes as possible, which led to over 95 codes. With this initial code list, we advanced our analysis to collect the overarching themes from our codes in several rounds of discussion. During this process, we also went back and forth between the generated themes and the dataset to refine the themes, with the goal of ensuring internal homogeneity and external heterogeneity [21]. Our final thematic map consists of two primary themes: rationale behind the usage of WeChat privacy settings, and impact on personal cognition and social interaction of using WeChat privacy settings. When reporting interview quotations, we use P1, P2, etc. to indicate the different interviewees. We translate all of the quotations into English when reporting them in the paper.

5 FINDINGS

Two thirds of our 24 participants had used Tags, and one third had heard of Tags but had not used it. Half of participants had used Don't Share, while the other half had only heard of it. One third had used Hide Moment, 58.3% had heard of it but chose not to use it, and 8.3% did not know this feature. One third had used Time Limit, 58.3% had heard of it but never used it, and 8.3% did not know about this feature.

Participants who had heard of but chose not to use one or more of these features were probed for their reasons. Most of them reported that they applied other strategies instead of the WeChat privacy settings to control the audience of their Moments, such as self-censoring content before posting and reducing the posting frequency, because they were concerned about the risk of incorrect configuration. For example, P15 mentioned that he would be embarrassed if his contacts found out he was using Tags against them. Some participants found that it cost too much effort to configure these features, especially the Tags. Another reason for not using audience control was that WeChat did not give enough instructions to users about these features, and users were not willing to learn from other sources either.

In the following sections, we report on participants' rationales for their chosen privacy settings, and the impact of their configurations on their information disclosure and interpersonal interactions.

5.1 Rationale Behind Privacy Setting Configurations

Our participants reported various rationales behind their decisions on which privacy setting to use or not to use and how to use them. Even though different settings have different features, we found common rationales across our participants' configuration of these settings:

5.1.1 Pairing Content with Social Relationship

Participants' social relationships with their WeChat contacts influenced how they configured their privacy settings to restrict the audience of contents in Moments. Their usage of Tags, Don't Share, and Time Limit were different between close and weak ties. Participants adjusted these settings as their relationships with contacts evolved. They also considered indirect relationships in addition to direct relationships.

Closeness of Social Relationships

The closeness of social relationships affected how participants selectively controlled the audience of their Moments through Tags, Time Limit, and Don't Share. "Close ties" in our data refers to family, peers, close friends, colleagues and classmates. Most participants preferred fewer restrictions for close ties. They deemed Moments with family, travel, and selfies as suitable for close ties rather than for weak ties like acquaintances and strangers.

Nevertheless, participants carefully curated certain topics even for their close ties using Tags. For example, they only disclosed Moments containing personal feelings, relationship status, personal interests, parties, dirty words, etc. to peers, especially close friends, because they had frequent or long-term interactions with close friends and understood each other. They would rather not disclose these Moments to parents since this might trigger concerns and interventions. As P2 described how he used Tags to prevent his parents from seeing some of his Moments: "*I tag my parents out if I post about my girlfriend because they'll ask a lot.*"

Moments with trivial but intimate details, such as meals, schedules and locations, were open to parents rather than peers, because participants felt that such details were useful for their parents to know so that they would be less worried, but that these details would not be meaningful to other contacts. In such cases, they would also use Tags to control the audience.

Participants used privacy settings to prevent weak ties from viewing Moments with personal details. Some participants accepted acquaintances and unknown people into WeChat for instrumental reasons like "leasing a room" or "merchant". They would thus put them on the "Don't share" list because they regarded Moments as private and unnecessary to share with people they hardly knew. However, some participants reported a small number of topics that could be shared with acquaintances and unknown people, such as landscape photos, news and jokes, and preferred Tags to control these audience groups. Despite the restrictions on acquaintances and unknown people, participants would not remove these people from their contact lists because they might need to contact them again for instrumental reasons in the future. P19 said:

I tagged the bakery salesman as "unknown people" who is completely out of my selection when I posted Moments. I also added him to "Don't share" list when I accepted him as my contact. This is like double check to make sure he can't see any of my Moments. But I would not delete this person because I might still need to purchase bakery items from him in the future.

Another example of weak ties were superiors, for whom the restrictions were more complicated. Superiors were participants' teachers and employers. Participants imposed more restrictions on superiors because they were concerned that their Moments might give their superiors bad impressions of them. However, our participants did not dare to use "Don't share" or "Tag" to prevent superiors from seeing their Moments, because their usage of these settings could be easily detected and might offend their superiors. Thus, participants used Time Limits to control this audience of past Moments. Although setting time limits would also prevent other contacts from viewing the past Moments, they felt that the benefit from restricting superiors would override such cost. For example, P7 mentioned:

I posted a variety of things in my Moments a long time ago. I added my employer in WeChat. I can't tag him or add him to "Don't share" list cuz he can find out. (How could he find out?) There is a line if he opens my Moments page, implying that he is on my "Don't share" list. Besides, if he sees no Moments from me, he will know it. But I don't want him to see my past posts. So I just make posts in the last half year available.

Evolving Relationships

Participants considered the dynamics of social relationships when using privacy settings. They reported the need to adjust Tags and Don't share after relationships had evolved. When strangers became friends, participants would modify Tags related to them or remove them from their Don't share list. Conversely, when close relationships became weak, topics previously considered suitable were no longer appropriate, and thus related Tags would change. For instance, P19 explained,

I tagged some people I knew during the internship as "friends", and they could see most of my posts. But now it's been two years since I was done with my internship. We haven't communicated that often any more. So I tag them out. They feel like I share less now, but the truth is I still post a lot. They just can't see them.

Indirect Relationships

In addition to considering their direct social relationships with WeChat contacts, participants also considered the relationships among their contacts when managing privacy settings. Most participants used Tags to control these contacts. For example, participants said that they also carefully tagged out relatives and friends of their parents when they wanted to exclude their parents from their Moments, because their parents might learn about those Moments from those contacts. For example, P3 said,

I have a tag for relatives, and one for relatives' friends. My parents got divorced, I have a tag for my father's friends and a tag for my mother's. If I post something and these relatives forward it to my parents or talk about my Moment with my parents, my parents will teach me a lesson.

Participants also considered the relationships between two contacts to avoid potential conflicts when adjusting Tags. For example, they would put contacts with similar relationships into the same tag so that these contacts could be treated equally to avoid one of them finding out he or she was blocked while the others were not. For instance, P23 explained,

I consider the relationships between two contacts. If they are in a good relationship with each other, I will put them in the same tag.

5.1.2 Based on Interests

Another important consideration when configuring WeChat's Tags and Hide Moments regards both personal and mutual interests. Participants hid Moments shared by their contacts that did not align with their own personal interests, such as ads and irrelevant topics, because this information wasted their time and annoyed them. P11 complained:

I hid some contacts' Moments (using Hide Moments) because they just posted so many ads that impact my life. I liked to get to know what my friends are doing by browsing their Moments. If someone posted like hundreds of ads, they are disturbing my life.

Participants also configured Tags based on their pre-existing knowledge of mutual interests with their contacts. They believed that only contacts with mutual interests would understand and likely create further interactions around the mutual interests. P3 said:

There are some friends who share the same interests and we chat a lot. When I post Moments, I will tag those friends because they will be interested in what I am saying. For others, they won't be interested nor create interactions. I don't want these people to see such Moments.

Participants' perceptions of mutual interests would change over time; thus, they adjusted their privacy settings to align with the change. They used Hide Moments to exclude contacts who no longer shared certain mutual interests, and gave up Tags for potential members of mutual interests. For example, P5 said,

There's one time I posted something about soccer. I am a fan of Real Madrid, and I hate Barcelona. In that match, Real Madrid kicked the ass of Barcelona. So I posted a Moment to celebrate. I shared it with all my contacts. I thought only friends that I knew were Real Madrid fans would be interested. But there were some other people who were also fans, but I had no idea of that. They replied to my post like 'oh, I am a fan, too'. ...Thus, sharing with all my contacts actually helped me make more friends who are also soccer fans.

5.1.3 Based on Perceived Personality.

The perceived personality of WeChat contacts is the third important factor that participants considered when they configured settings such as Don't Share and Tags. Past interactions with contacts shaped our participants' perceptions of their personalities. If the perceived personality of a specific contact was likable, users were highly likely to relax the control over Moments for this contact; if not, they would tighten their control, mostly by using Don't share and Tags. For example, P15 told us,

I added two friends to Don't Share because I don't want to talk with them. They always judge me. I don't want them to see any of my Moments because, you know, they will judge.

P23 shared a similar experience. She considered the personality of her contacts when posting certain types of Moments:

When I post Moments related to how happy I am and how much I love my job, I also tag out a contact whom I went to college with, because she gets jealous easily.

5.2 Impact of Privacy Setting Configuration

The use of WeChat's privacy settings impacts users' information disclosure and their social experience.

5.2.1 Impact on One's Information Disclosure

WeChat's privacy settings provided participants with considerable control to share information in the way they desired and to mitigate the risk of unexpected consequences. Using Tags, Time Limit, and Don't share encouraged participants to a certain degree to share more about themselves. For example, P22 mentioned:

I posted a Moment about my mechanic keyboard just among a small number of friends, cuz I like playing video games. If I made it public, there would be someone asking stupid questions that I didn't want to answer because they had no idea of what it means to me and it was like a waste of time. Since I can use Tags to filter the audience, I am more willing to share that kind of Moments.

This participant used tags to limit this Moment to those contacts who could understand the literal message of this Moment (what a mechanic keyboard is) as well as the contextual message (a mechanic keyboard means a lot to gamers), which was the kind of disclosure he desired. Using tags prevented him from being asked questions by contacts that he did not care about, which was a waste of time to him. Thus, the availability of tags actually encouraged this participant to post Moments. Without tags, he would have decided not to post them.

5.2.2 Cognitive Burden

Configuring privacy settings imposed a cognitive burden on participants. Most of this cognitive burden was caused by Tags. For example, the upfront time invested into the definition of tags intimidated several participants. Contacts need to be assigned to tags one by one, so this was very cumbersome for those with large online social networks. In addition, certain WeChat contacts might be in multiple relationships and would thus belong to multiple tags. Participants felt that

this was not only tedious but also complicated without sufficient feedback from the system. P9 said:

I have more than three hundred friends. Let's say I want to assign 50 people to one tag. I have to check if each one of the 300 friends should go into this tag. One by one for all the 300 friends. If I create another tag, I have to go through this again. And I don't have a clear picture of how it works. What if one contact goes into two tags? Can they see my posts if I made my posts available to one tag? There's no clarification about this.

Another significant cognitive burden relates to the reconfiguration of Tags when the original rationale changes. As mentioned above, participants often needed to adjust privacy settings when certain social relationships evolved. However, participants saw no way but to create new tags if they wanted to add or delete a person from their existing tags, because they thought the current design did not support that (which it actually does). For example, P2 said,

I can't edit the tags. If I want to add contacts to an existing tag, I have to create a new one. The worst thing is, if I previously didn't want some contacts to see my posts, but change my mind now, no matter what I do, they will never see those posts.

While WeChat allows users to edit tags, 6 participants in our study were not aware of this, because WeChat does not indicate it saliently.

Due to the complexity of Tags, participants were also at risk to configure them incorrectly. Incorrect configurations resulted in unexpected consequences. Participants reported that they had overlooked some contacts who should have been tagged out for certain Moments. When they found out, the Moments had already been viewed by these unintended contacts. In reaction, some would delete the Moment, re-configure their Tags and post it again, while others would have to explain the situation to the contacts involved, which further increased the cognitive burden for their future Tags use. Some participants would be more careful, hesitant and even stressed when using Tags again. For example, P17 shared his experience,

I posted something and I wanted to exclude my family. But I forgot about my sister. She saw that Moment, as I found her "like". I didn't know if she told my parents. I reposted that Moment anyway with her excluded. Will be more careful about that.

Two participants described their strategies to cope with the cognitive burdens of privacy settings. P19 said that she would add contacts to tags at the moment she accepted their friend requests. This would cost less effort than to configure Tags once the network size became huge and reduce the chance of unintentionally leaving someone out of audience control. P3 mentioned that she used to adjust her disclosure preferences and stop using privacy settings for non-sensitive information, such as links and news, to reduce the privacy configuration effort for these Moments. This indicates that participants needed the granular settings, but they developed their own strategies to lower the cognitive burden of using these settings.

5.2.3 Impact on Social Interactions

The use of WeChat privacy settings has various impacts on users' social interactions because one's settings of Tags, Time Limit, Don't Share and Hide Moments can be found out by impacted contacts. There were two ways that participants found out they were the targets of privacy settings: 1) they communicated with unimpacted contacts about someone's Moments. For example, P23 explained,

I had two WeChat friends who were my college roommates and they often hang out together because they work in two cities which are quite near. ...I put them into different tags. So one could see my post, but the other could not.... There's one time when I posted such a Moment, when they

were hanging out. One was like "see, [name] was doing this recently"; the other was like "what? I can't see it".

2) They inferred from the WeChat interface whether they were affected by someone's privacy settings. As shown in Figure 2, if B is on A's Don't Share list, there will be no post in A's Moments for B to view and a line shows up instead. If A sets a time limit for Moments, B cannot access the posts beyond that limit, but rather receives a message saying "only X days of Moments are viewable".

No matter how participants found out that they were being restricted by others or impacted by privacy settings, they usually thought of it negatively and their interpersonal interactions were affected.

Undermining Social Relationships

Many participants reported undermined social relationships after the impacted contacts found out that participants had used Tags, Time Limit, Don't Share or Hide Moments against them. For example, P19 explained,

I set up a three-day limit to my Moments. Then I ran into some stuff and was very busy in the next few days so that I didn't post anything for a long time. If someone came to my Moments, there was nothing but a blank page, like he was on my Don't Share list. My sister saw it and said to me, "why do you show me nothing? People like just an acquaintance would give me at least half-a-year." I felt it was indeed hurtful to my friends if there was just a blank page in my Moments.

In his case, the participant's sister found out that the participant was using a three-day time limit for her Moments and explicitly informed the participant of how hurtful this was to their relationship, which urged the participant to relax the audience control.

However, the impact was worse if the impacted person did not explicitly complain about it. For example, P3 told us,

I had a tag for four friends. Then I tagged the fifth person who was new but happened to know one of the four friends that I had already tagged. This fifth person could not see my past Moments posted before he was tagged. When he talked with one of the first four friends, he found that he could not see some of my Moments and felt like I blocked him. If he asked me, I could explain. But most of the time people don't say it. They may hate me.

While this was not the participant's fault but rather a design problem, the impacted contact would think of it as "I was blocked by someone". It was even impossible for the participant to explain the situation because the impacted contact kept silent about it, which made it difficult to fix the impaired social relationship. To avoid such an impact, P16 said that she would make an announcement to all her close friends to explain the situation.

Moreover, when finding themselves as the targets of Tags, Time Limit, Don't Share and Hide Moments, participants reported that they felt untrusted, unequally treated and distanced by their friends, which would influence their future interactions with them. For example, P11 explained,

Someone tags me out. When I hang out with our mutual friends, they mentioned something he posted, but I could not see it. I know that I am either tagged out or on the Don't Share list. I will keep my distance from him in future. It means that I am not that close to him, nor trusting to him. We probably have a lot of discrepancies. I would not ask him. It was his choice anyway. But I will keep my distance from him.

While this participant preferred to adjust her relationship silently, some participants would ask about it. As P12 said,

I had a friend who had a three-day limit to her Moments. Sometimes I wanted to get to know what she's been doing recently, there was nothing cuz she happened to post nothing in the past three days.

I was wondering if she put me on the Don't Share list or tagged me out. Why would she hide things if she chose to post? So I just asked her why and asked her to change it. We were good friends. So she changed it back. (what if you were not a good friend?) I would probably ask, too, if I were interested. Like 'hey I just want to have a look. You can change it back after.

This participant mentioned a negative impact of a time limit on her catching up with her friend's updates, and a straightforward strategy to cope with it.

Emotional Disturbance

In addition to the negative impact on the social relationship, some participants also felt emotionally disturbed when they knew that they were the targets of Tags, Time Limit, Don't Share and Hide Moments, especially when they did not expect it to happen or had no clue about the reasons. For example, P5 shared his feeling with us,

It was like a thunderbolt out of a clear sky to me. He was the first one that I know who tagged me out. I was keeping thinking and thinking if I did something wrong to him. I actually felt we were good friends. I texted him. He said he forgot to tag me correctly. But I think he still tagged me out after that. WTF. Never mind. (how did you find out?) He went back to his home country and posted the message in his Moments. Everyone knew it except me. They mentioned this in front of me. I was like "what? why don't I know that". They showed me that Moment. I opened his Moments on my phone. There was nothing. They told me he might tag me out.

For this participant, the setting of another user's Tags was completely unexpected since he thought they were good friends, which was the main reason for his emotional reaction.

On the other hand, some participants also felt embarrassed and guilty when someone found out that they had used privacy settings against him or her, because they did not expect the impacted contacts to find out. For example, P12 said,

I used Hide Moment on a guy because he posted a lot of ads. Then we attended a party together. Someone brought up his Moments. He asked me if I knew them. I was so embarrassed. But I put it directly like 'I don't like so many ads'. Later I intendedly looked at his posts to catch up with his recent updates. Now he's no longer posting ads. I don't hide his Moments anymore.

While the two participants above responded directly to the situation, some other participants who showed a negative emotion would choose to use the same audience control in a reciprocal manner, or delete this person from their contacts. For instance, when P15 found out he was on the Don't Share list of a contact, he was so unhappy that he deleted the contact immediately: *"I was shocked at first. What had I done to her? What for? I was unhappy. I didn't ask her. I DELETED her!"*

However, for some participants, the emotional disturbance from finding out they were the targets of the WeChat privacy settings of a contact depended on the closeness of this contact and the number of mutual contacts who were also impacted. If they were not close friends with this contact, or found that all mutual contacts were equally affected, i.e., through a time limit, then they would not have an issue with the restrictions. If instead they found out they were the only ones who were affected then this was indeed disturbing. For example, P13 explained,

It depends. If we are not good friends, it doesn't matter if I can't see his Moments. If I think we are good friends and he used privacy settings against me, I am not happy. If we are colleagues and he doesn't do that to others but to me, I am not happy. If he does it to every colleague, then I don't care.

5.2.4 Restricted Information Flow

Some participants were upset by the fact that information they expected a person to disclose was restricted by this person's privacy settings. Such situations were mostly about Time Limits. For example, P17 explained,

I found my boyfriend using a three-day limit. I asked him to change that, because people may not know he has a girlfriend.

For this participant, her boyfriend's chosen time limit restricted the information disclosure that she expected. Her boyfriend's contacts might not get the message about their relationship status. Hence, the information flow that she expected was restricted.

Participants also found it restrictive when they unsuccessfully sought certain information about their contacts, though they were not upset about it. Viewing a contact's Moments is an easy way to get information about this person's recent updates. However, if the person uses a Time Limit on the Moments, others will have trouble finding information about this person. This is worse in a new relationship, where people typically want to know more about each other. For instance, P20 wanted to know more about a new contact by viewing the contact's past Moments, but found it impossible:

I added someone. Everything was good. I want to know more about him from his Moments. There were only posts in the past three days. I had no idea what he was doing.

Many participants expressed their confusion about the restrictions, especially about the Time Limits, as they violated the nature of information flow. They believed that Moments were designed for information sharing. A three-day limit was too restrictive for them to receive the information flow they desired. For example, P7 explained,

I don't quite get it why people use it. What's the point? You post Moments for others to see. Half-a-year limit is fine cuz some people may not want others to go that far into their personal histories. But three-day limit? I don't get it, unless you completely hide it.

6 DISCUSSION

The present study aims to explore the usage and impact of WeChat privacy settings. We found that users adjust the granularity and restrictions based on the content they want to share, the social relationships between them and their contacts, and their contacts' interests and perceived personalities. They evolved their configuration and the rationale behind it along with changing social relations, the makeup of online social contexts, and users' own reflections on past experiences with privacy setting configurations. However, even though some users appreciated that the WeChat privacy settings allowed them to disclose personal information selectively to desired contacts in different social contexts, they reported several negative impacts on their information disclosure and social interactions. We will discuss these findings in this section.

6.1 Nuanced and Evolving Rationale Behind Privacy Setting Configuration

Our study shows that users' configurations of WeChat audience controls are not only highly nuanced but also evolving along with changing social relations, the makeup of online social contexts, and users' own reflections on past experiences with privacy setting configurations. Users continuously develop their privacy management practices during this progression.

First, we found that our participants' privacy setting configurations constantly evolved with the changing social relations and makeup of online social networks. Our participants' disclosure decisions were different in different online social contexts. To avoid "context collapse" [22], they adopted and heavily customized the audience control techniques of WeChat, based on shared content, social relationships with SNS contacts, personal interests, mutual interests and the

perceived personalities of contacts. Most previous studies examined users' configuration of audience control in a static manner without considering the changing nature of online social contexts. For example, they reported the general considerations that users applied in one-time groupings of their contacts [25,35]. One exception is Bauer et al.'s study, in which they conducted a longitudinal survey to explore whether users' privacy settings for Facebook post visibility changed over time [4]. However, they studied the changing privacy settings within only one month, and only revealed very general factors for the changes (e.g., "a specific event occurred" or "my relationship with the people changed"). Our findings involve a longer period of time and an in-depth analysis of how these factors changed to motivate users to adjust privacy settings over time. For example, participants mentioned they would adjust privacy settings when new contacts turned into close relationships, or when participants reached a new life stage. Another exception is Kelley et al.'s study [16]. While their participants only did a grouping task in a single session in their lab and had "little understanding how users would like to and should modify their groups over time", Kelley et al. acknowledge that social relations and online social networks may change over time [16]. Our study that has a longer-term focus confirms their argument by finding that our participants indeed reconfigured their privacy settings when their social relations and online social networks changed. Further, our study reveals the concrete ways in which users modify their privacy settings over time. For instance, when the tie strength changed, participants would alter their Tags and other related settings to adjust their desired audience. When they moved onto a new life stage or an event, they would also change the configuration. This indicates that we should treat privacy configuration as a dynamic process because it is sensitive to evolving social contexts.

Second, our participants' rationale and practices of privacy configuration also evolved as they interacted with the privacy settings and reflected on their past experiences. They developed new rationales for who could see which Moments when they realized the consequences of unintended disclosure. For example, participants' rationale changed from "restricting every contact" to "relaxing for close contacts" when they learned that the former might hurt their social relationships. Thus, privacy setting design and research cannot ignore the learning process in one's privacy management.

Design Implications: Users' privacy settings configurations should be considered as an evolving process along with changing social relations, the changing makeup of online social networks, and users' own learning process. In SNS use, many details may indicate changes in social relationships, such as frequency of online interaction, number of mutual friends, and SNS groups. The system can take advantage of these clues to visualize tie strength, inform users of changes in relationship status, or nudge users to revisit their privacy settings from time to time, so that they can adjust their privacy settings accordingly. Additionally, systems should increase users' awareness and reduce their effort of reconfiguration, so that users can easily and frequently revisit their privacy settings when their social relationships change.

6.2 Impact of Privacy Settings on Social Interactions and the Privacy of Privacy Settings

Granular privacy settings bring new challenges to users' social interactions with others. Our study shows that when participants configured the granular privacy settings to accommodate their online social contexts and satisfy their disclosure preferences, their configurations could be discovered by the impacted SNS contacts, because these impacted contacts could infer their status through the associated interface or through communications with unimpacted contacts. Most impacted contacts were not aware of users' justifications for the objectionable configuration, and regarded it as

offensive or confusing. This potentially undermines the social interactions between users and their contacts and creates emotional turbulence for both sides.

This finding is a unique contribution of our research, as such issues have been less studied in prior work and can only be revealed by looking at users' long-term usage of audience control settings in their interactions with real-world SNS contacts. Most prior studies call for fine-grained group-based privacy settings to ensure that users can target their information disclosure to their desired audience [13,18]. Our study, however, raises the caution that besides being cognitively burdensome to manage, such settings may cause an unpleasant impact on users' social interactions and emotions. People in the social world seek to maintain not just a personal life but also a social life with others [24]. It is unrealistic for users to ignore the unpleasant impact of privacy settings on their social interactions. This suggests that privacy researchers and designers should look at the broad and manifold facets of users' lives when examining information privacy practices.

These findings offer us another new perspective to consider in future privacy design: designing for the privacy of chosen privacy settings. Prior privacy research and design focused on how to enhance the privacy of personal information, such as safeguarding identifiable and other sensitive information [2]. Few studies have considered the privacy of privacy settings. Users' configurations of privacy settings are also a part of the sensitive personal information they want to protect, and our study shows that participants indeed wanted to keep this type of information private, as unintended disclosure of it may damage their social interactions.

Design Implications: SNSs should remind users about potential social problems with their configurations that they may not have considered. For example, when users make audience control settings for one contact very different from others, the system can inform them that this contact is likely to find it out when interacting with the others. Alternatively, the system can provide a list of mutual friends when users add a new contact in their SNSs, so that users can review and adjust prior privacy settings.

In addition, differences in the interface should be subtle for users who are impacted by someone's privacy settings. For example, the current design of WeChat Time Limit explicitly shows "only X days of Moments are viewable" for viewers (Figure 4). The interface for users who are on someone's Don't Share list also shows a blank page with a gray line in the middle indicating that they are blocked (Figure 3). These indicators make it easy for users to infer others' privacy settings. Future design should enable users to hide their privacy configuration from others and to provide justifications and explanations to their contacts when users make changes to their settings.

6.3 Cognitive Burdens on End Users and Users' Strategies

Granular privacy settings impose a heavy burden on end users. In our study, participants who actively adopted WeChat privacy settings reported the cognitive burdens of initial configuration and of reconfiguration. Participants who chose not to use the settings also reported they were scared away by the amount of work required to set up the privacy settings. This echoes previous findings that users gave up granular audience control techniques because of lack of awareness [3,15], upfront time investment [3,37], recurring efforts [16,27], and insufficient self-efficacy in privacy management [31]. Thus, there is an urgent need to reduce these cognitive costs for users configuring granular privacy settings.

Additionally, we found that users perform a cost-benefit analysis of perceived privacy control versus the cognitive burden of this control, which is also in line with previous research [1]. In our study, there were participants who concluded that the perceived privacy control outweighed the cognitive costs. For example, participants felt that the Tags and Time Limit made it easy for them

to avoid information disclosure to unwanted audiences, and thus they were willing to make the effort to configure the settings.

Our study also reveals that some participants even developed their own strategies to cope with the cognitive cost. For example, one strategy was to set up audience control when adding new contacts to their networks. This was especially efficient for those who had large online social networks, as it divided one big time-consuming task into small pieces. It also reduced the chance of unintentionally leaving someone out of audience control. Another strategy was for users to rethink their disclosure preferences and relax their restrictions for non-sensitive information. In this case, participants re-evaluated their previous rationales and changed their privacy sensitivity, which saved them efforts in privacy configuration. These strategies can shed light on how to design SNS audience controls to mitigate the cognitive cost of configuration.

Design Implications: We reinforce the call for privacy designs that entail less end-user effort. For example, systems can reduce the time investment for users' first-time configuration, intelligently auto-classify contacts based on contextual factors, offer clear built-in instructions, and lower the complexity of operation [15,16,25]. Moreover, many recent studies have proposed forms of privacy support that do not completely rely on end-user efforts and that make it easier for users to manage their privacy, such as context-aware privacy defaults [32], automatic privacy setting configuration [10], privacy nudges [33], and privacy recommendations [9]. These privacy designs should be integrated into granular audience control techniques.

In addition, the user strategies that we found can shed light on desired system design. First, systems can divide privacy configuration into smaller tasks, so that users perceive it as less burdensome. For example, systems can offer users the option to set up audience control when they accept a new SNS contact. This also encourages users to customize privacy settings for each contact. Second, they can remind users to revisit their privacy needs when they detect that users potentially face large privacy configuration efforts (e.g., when users have a sudden increase in the size of their online social networks).

7 LIMITATIONS AND FUTURE WORK

Our study has some limitations. We only interviewed 24 WeChat users, who may not be representative for the general population of WeChat users. Nor can our findings represent the population of other SNSs around the world. However, our study yielded novel and insightful results about the impact of privacy settings on users' personal and social life. Future research can consider larger-scale studies to capture broader demographics.

Our study proposes several directions for future research. First, there is a need to systematically investigate users' strategies in coping with cognitive burdens in the use of SNS privacy settings, as our study has shown that some users develop their own strategies to reduce cognitive efforts rather than stopping using privacy settings. Second, future research can delve into mechanisms and prototypes that will mitigate the negative impact of privacy settings on social relations. Special emphasis needs to be put on protecting the privacy of users' chosen privacy settings, and on providing explanations to contacts when users make changes to their settings. Such mechanisms and prototypes will benefit future privacy design in a broad socio-technical context. Third, as there were interviewees who knew privacy settings but never used them, it will be interesting for future work to find out the reasons. Fourth, future research could investigate users' privacy settings across different SNSs to compare users' perceptions and strategies, so that privacy design for specific SNSs could be tailored to users' needs.

8 CONCLUSION

The present study aims to explore the usage and impact of WeChat privacy settings for audience control. Through an interview study with 24 WeChat users, we found that users adjust their configuration and their rationale over time. Users also perceived both positive and negative impacts of WeChat's privacy settings on their information disclosure and social interactions, which brings new challenges to privacy design. We discuss the implications of these findings and make suggestions for the future design of privacy support in SNSs.

ACKNOWLEDGEMENTS

We are grateful to our study participants for their dedication. Many thanks to our anonymous reviewers for their insightful feedback. This work was in part supported by NSF grant SES-1423629.

REFERENCES

[1] Alessandro Acquisti. 2014. The Economics and Behavioral Economics of Privacy. In *Privacy, Big Data, and the Public Good*, Julia Lane, Victoria Stodden, Stefan Bende and Helen Nissenbaum (eds.). Cambridge Univ. Press, Cambridge, England.

[2] Alessandro Acquisti and Ralph Gross. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In *Privacy Enhancing Technologies*, George Danezis and Philippe Golle (eds.). Springer Berlin Heidelberg, 36–58.

[3] Louise Barkhuus. 2012. The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems* (CHI '12), 367–376.

[4] Lujo Bauer, Lorrie Faith Cranor, Saranga Komanduri, Michelle L. Mazurek, Michael K. Reiter, Manya Sleeper, and Blase Ur. 2013. The Post Anachronism: The Temporal Dimension of Facebook Privacy. In *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society* (WPES '13), 1–12.

[5] B. van den Berg and R. Leenes. 2010. Audience Segregation in Social Network Sites. In *2010 IEEE Second International Conference on Social Computing (SocialCom)*, 1111–1116.

[6] Danah Boyd. 2008. Facebook's Privacy Trainwreck Exposure, Invasion, and Social Convergence. *Converg. Int. J. Res. New Media Technol.* 14, 1 (February 2008), 13–20.

[7] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qual. Res. Psychol.* 3, 2 (January 2006), 77–101.

[8] Ralf De Wolf and Jo Pierson. Who's my audience again? Understanding audience management strategies for designing privacy management technologies. *Telemat. Inform.*

[9] Cailing Dong, Hongxia Jin, and Bart P. Knijnenburg. 2015. Predicting Privacy Behavior on Online Social Networks. In *Ninth International AAAI Conference on Web and Social Media*, 91–100.

[10] Lujun Fang and Kristen LeFevre. 2010. Privacy Wizards for Social Networking Sites. In *Proceedings of the 19th International Conference on World Wide Web* (WWW '10), 351–360.

[11] E. Goffman. 1959. *The Presentation of Self in Everyday Life*. Doubleday & Company, Inc., Garden City, NY.

[12] Ralph Gross and Alessandro Acquisti. 2005. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (WPES '05), 71–80.

[13] Gordon Hull, Heather Richter Lipford, and Celine Latulipe. 2011. Contextual gaps: privacy issues on Facebook. *Ethics Inf. Technol.* 13, 4 (December 2011), 289–302.

[14] Sanjay Kairam, Mike Brzozowski, David Huffaker, and Ed Chi. 2012. Talking in circles: Selective Sharing in Google+. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1065–1074.

[15] Pamela Karr-Wisniewski, David C. Wilson, and Heather Richter-Lipford. 2011. A New Social Order: Mechanisms for Social Network Site Boundary Regulation. In *AMCIS 2011 Proceedings*, Paper 101.

[16] Patrick Gage Kelley, Robin Brewer, Yael Mayer, Lorrie Faith Cranor, and Norman Sadeh. 2011. An Investigation into Facebook Friend Grouping. In *INTERACT*, Pedro Campos, Nicholas Graham, Joaquim Jorge, Nuno Nunes, Philippe Palanque and Marco Winckler (eds.). Springer Heidelberg, Lisbon, Portugal, 216–233.

[17] Heather Richter Lipford, Andrew Besmer, and Jason Watson. 2008. Understanding Privacy Settings in Facebook with an Audience View. In *Proc. of the 1st Conference on Usability, Psychology, and Security*. Retrieved April 25, 2014 from http://dl.acm.org/citation.cfm?id=1387649.1387651

[18] Heather Richter Lipford, Gordon Hull, Celine Latulipe, Andrew Besmer, and Jason Watson. 2009. Visible flows: Contextual integrity and the design of privacy mechanisms on social network sites. In *Computational Science and Engineering, 2009. CSE'09. International Conference on*, 985–989.

[19] Eden Litt and Eszter Hargittai. 2016. "Just Cast the Net, and Hopefully the Right Fish Swim into It": Audience Management on Social Network Sites. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (CSCW '16), 1488–1500.

[20] Yabing Liu, Krishna P. Gummadi, Balachander Krishnamurthy, and Alan Mislove. 2011. Analyzing Facebook Privacy Settings: User Expectations vs. Reality. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (IMC '11), 61–70.

[21] Courtney Rees Lyles, Lynne T. Harris, Tung Le, Jan Flowers, James Tufano, Diane Britt, James Hoath, Irl B. Hirsch, Harold I. Goldberg, and James D. Ralston. 2011. Qualitative Evaluation of a Mobile Phone and Web-Based Collaborative Care Intervention for Patients with Type 2 Diabetes. *Diabetes Technol. Ther.* 13, (May 2011), 563–569.

[22] Alice E. Marwick and Danah Boyd. 2011. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media Soc.* 13, 1 (February 2011), 114–133.

[23] Anne Oeldorf-Hirsch, Jeremy Birnholtz, and Jeffrey T. Hancock. 2017. Your post is embarrassing me: Face threats, identity, and the audience on Facebook. *Comput. Hum. Behav.* 73, (August 2017), 92–99.

[24] Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (CHI '03), 129–136.

[25] Manya Sleeper, Rebecca Balebako, Sauvik Das, Amber Lynn McConahy, Jason Wiese, and Lorrie Faith Cranor. 2013. The Post That Wasn'T: Exploring Self-censorship on Facebook. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work* (CSCW '13), 793–802.

[26] Manya Sleeper, Justin Cranshaw, Patrick Gage Kelley, Blase Ur, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2013. "i read my Twitter the next morning and was astonished": a conversational perspective on Twitter regrets. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '13), 3277–3286.

[27] Katherine Strater and Heather Richter Lipford. 2008. Strategies and Struggles with Privacy in an Online Social Networking Community. In *Proceedings of the 22Nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1* (BCS-HCI '08), 111–119.

[28] Frederic Stutzman and Woodrow Hartzog. 2010. *Boundary Regulation in Social Media.* In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work* (CSCW '12), 769-778.

[29] IBG Tencent. The 2017 WeChat Data Report. *WeChat Blog: Chatterbox.* Retrieved April 15, 2018 from http://blog.wechat.com/2017/11/09/the-2017-wechat-data-report/

[30] Zeynep Tufekci. 2008. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bull. Sci. Technol. Soc.* 28, 1 (February 2008), 20–36.

[31] Jessica Vitak and Jinyoung Kim. 2014. "You Can'T Block People Offline": Examining How Facebook's Affordances Shape the Disclosure Process. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '14), 461–474.

[32] Na Wang, Pamela Wisniewski, Heng Xu, and Jens Grossklags. 2014. Designing the Default Privacy Settings for Facebook Applications. In *Proceedings of the Companion Publication of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW Companion '14), 249–252.

[33] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. 2014. A Field Trial of Privacy Nudges for Facebook. In *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*, 2367–2376.

[34] Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. "I regretted the minute I pressed share": a qualitative study of regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 10:1–10:16.

[35] Jason Watson, Andrew Besmer, and Heather Richter Lipford. 2012. +Your Circles: Sharing Behavior on Google+. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (SOUPS '12), 12:1–12:9.

[36] Jason Wiese, Patrick Gage Kelley, Lorrie Faith Cranor, Laura Dabbish, Jason I. Hong, and John Zimmerman. 2011. Are you close with me? are you nearby?: investigating social groups, closeness, and willingness to share. In *Proc. UbiComp 2011* (UbiComp '11), 197–206.

[37] Pamela Wisniewski, Heather Lipford, and David Wilson. 2012. Fighting for My Space: Coping Mechanisms for Sns Boundary Regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '12), 609–618.

[38] WeChat hits one billion monthly users - are you one of them? - BBC News. Retrieved April 15, 2018 from http://www.bbc.com/news/business-43283690

Received April 2018; revised July 2018; accepted September 2018.