Do Birds of a Feather Watch Each Other? Homophily and Social Surveillance in Location Based Social Networks

Shion Guha
Dept. of Information Science
Cornell University
Ithaca, NY 14853
sg648@cornell.edu

Stephen B Wicker
School of Electrical & Computer Engineering
Cornell University
Ithaca, NY 14853
sbw11@cornell.edu

ABSTRACT
Location sharing applications (LSA) have proliferated in recent years. Current research principally focuses on egocentric privacy issues and design but has historically not explored the impact of surveillance on location sharing behavior. In this paper, we examine homophily in friendship and surveillance networks for 65 foursquare users. Our results indicate that location surveillance networks are strongly homophilous along the lines of race and gender while friendship networks are weakly homophilous on income. Qualitatively, an analysis of comments and interviews provides support for a discourse around location surveillance, which is mainly social, collaborative, positive and participatory. We relate these findings with prior literature on surveillance, self-presentation and homophily and situate this study in existing HCI/CSCW scholarship.

Author Keywords
homophily;privacy;visibility;surveillance;vision;foursquare

ACM Classification Keywords
H.5.m.Information interfaces and Presentation (e.g., HCI): Miscellaneous.

INTRODUCTION AND MOTIVATION

Though LSAs are far from novel, in the past 10 years, the growing ubiquity of mobile phones, the proliferation of "smart" phones and the increasingly cheaper access to Wi-Fi and GPS signals have resulted in the sharp rise [47] in their development and use, particularly in mobile devices.

We define LSA's with standard social networking features such as adding friends, commenting, liking and tagging as location based social networks (LBSNs) e.g. foursquare or Jiepang. We also distinguish between these and other popular social networking sites (SNS) with geocoding features (e.g. Facebook, Twitter) by postulating that actions on LBSNs always revolve around a location or venue whereas on other SNS, locations are not the focal point. In this paper, we will concentrate on LBSNs with check-in type location sharing features because we believe that the ability to (not) disclose location is paramount when examining privacy, impressions or surveillance concerns.

There is a small, but growing body of HCI research that has looked at the patterns and practices of modern LBSN users. Lindqvist et al. [25] reports that people have multiple reasons for using foursquare. Some of these are social location sharing, personal location tracking, social gaming and location discovery. Cramer et al. [11] find emergent performative aspects around locations, linked to audience management arising from sharing location on foursquare. Guha and Birnholtz [17] discovered that users have different location sharing strategies involving deception, obfuscation etc. which, they argue is often used to manage offline social goals and enhance social signals. Patil et al. [35] found that privacy concerns have some influence on the adoption and continued usage of LBSNs. These privacy considerations may have undesired social consequences; may cause feelings of regret and grief but are also carefully balanced against economic and personal attractions i.e. a check-in might result in a discounted meal but could also have an unanticipated social cost.

However, impression management and privacy are only two of many potential perspectives to understand location disclosures. They take the point of view of the person *disclosing* the location but do not adequately inform us about the person *viewing* the location disclosures, which Trottier [44] recently theorized, can also be construed as social surveillance by network ties.

A traditional understanding of surveillance is that of a vertical, rigid structure [27] rooted in asymmetry and power politics. A contrarian position [2] maintains that in social networks, lateral surveillance – a flat, horizontal and amorphous system with opportunities for all social network ties to surveil each other is perhaps more suited for empirical explanation. In addition, two recent theoretical articles advocate for the participatory and empowering [1] and/or social and positive [28] nature of lateral surveillance.

CSCW '15, March 14 - 18 2015, Vancouver, BC, Canada

ACM 978-1-4503-2922-4/15/03…$15.00
http://dx.doi.org/10.1145/2675133.2675179

Homophily, or the propensity of similar users to connect together, [38] has been proposed as a theoretical framework to explain how people interact with their social network ties. Recently, homophily has also been hypothesized to contribute to self-presentation [13] on location as a natural product of [28] SNS surveillance. We asked ourselves: is this divergent from homophily friendship networks? Is there any sort of discourse around location surveillance? Towards this effort, we conceptualized a surveillance network as a weighted friendship network where edge weights represent net surveillance activity between any two pairs of connected nodes. In the paper that follows, we present a mixed methods study of 65 foursquare users, from which there are several novel findings.

First, we show that **Gender** and **Race** are significant predictors (with strong effect sizes) of homophily in surveillance networks while **Income** seems to be a significant predictor of homophily (with a weak effect size) in friendship networks. We argue that this may be driven by the engenderment and/or the racial construction of location and may be a way to carefully cultivate impressions by group affiliation. Second, we discuss participatory, social and collaborative interactions around location surveillance and debate the value of positive surveillance. Third, we pose feedback and social translucency as privacy-aware design features in supporting social surveillance in LBSNs but also advocate for recent calls against mandatory design implications in HCI based on participant design reflections.

LITERATURE REVIEW

The research reported in this paper lies at the intersection of three areas of prior work. First, we will describe existing human-centered research on LSAs focusing on behavioral patterns and practices. Second, we will illustrate current research on privacy-aware design in LSAs. Finally, we will explore relevant literature on social networks concentrating on homophily, privacy and surveillance theory.

Location Sharing: Behavioral Patterns and Practices

Systems that allow users to take advantage of location sharing or to be aware of others' location are not very new. Early systems include the Active Badge [46] in workplace settings and the Whereabouts clock [9] for family location awareness. Different groups of researchers have tried to understand the motivations and practices of LSA users. In an influential work, Consolvo et al. [10] found that users were mainly considerate of their specific audience when location was requested from them. They would acquiesce to sharing location if they felt it would be useful for that particular requester and adjust the granularity of their disclosed location accordingly. They did not find any evidence of location obfuscation strategies by their participants. Humphreys [19,20,21] conducted a study of Dodgeball and concluded that its primary use was spontaneous coordination and supporting serendipitous urban congregation. She also noted that most of her participants were not bothered by privacy concerns - perhaps because they were early adopters and heavy users.

Barkhuus et al. [4] conducted a field trial of Connecto and found that there was a gradual shift from location awareness to social interaction around collaboratively curated sets of "tagged" locations. Smith et al. [39] conducted a pilot study (n=8) of Reno and discovered that although people favored automatic location disclosure significantly more than manual location sharing there could be unexpected social costs. Location disclosure provides a context aware approach to negotiating social relations. Tang et al. [41] and found that participants (n=10) had a range of strategies for disclosing location – mainly driven by privacy and attention seeking. This latter finding gives us an intuition into location sharing - people *want to be seen* by their social networks. In a detailed questionnaire and diary study (n=10), Reilly et al. [37] studied location information need from the perspective of the viewer. They found that there is usually a negotiation of interests around location - the sharer balances her privacy concerns (and other social interests) against the receiver's need to know location and other associated information. Meanwhile, Page et al. [34] studied deception and lying in LSAs through interviews (n=20) and a large survey (n=1532) and found that deception is a relatively common tactic to negotiate online interpersonal and social boundaries but that, this may backfire and have unexpected offline social consequences.

Recently, Lindqvist et al. [25] conducted an exploratory study on foursquare and found that people use foursquare with multiple interleaving motives; foursquare could be used as a way for social location sharing and discovery, movement gamification, spontaneous coordination, as a personal diary or to take advantage of special offers and discounts. Cramer et al. [11] also studied foursquare and uncovered a shift from just location sharing to a more performative aspect around location disclosure. Guha and Birnholtz [17] reported on the results of a detailed interview study (n=30) of foursquare users. They found that users had evolved detailed strategies for managing and forming impressions to multiple audiences with multiple objectives based on the potential visibility of their check-ins. Summarizing this set of literature, it is clear that sharing location is not just a utilitarian objective but also serves as a nuanced way of managing impressions and furthering social goals. However, it is still an open question how people view and discuss the visibility of others' location disclosures.

Location Sharing: Privacy-Aware Design

Designing for privacy concerns has been a common topic in LSA research. Iachello and Hong [23] published a comprehensive survey of three decades of privacy research in HCI. In recommending future directions, they called for an expansion of research into understanding surveillance systems from a human-centered perspective. One specific example they used was the increasingly common usage of

locator badges on nurses in hospitals. Iachello et al. [22] implemented Boise and suggested, among others, denial, deception and evasion as LSA design features to support privacy management and "beat" location surveillance. One system actually built with these design principles is Locaccino, which was deployed by Toch et al. [43] (n_1=28, n_2=373); they found that people shared locations frequented by larger numbers of other users; those who visited diverse locations received more location requests and over time, develop sophisticated strategies for location disclosure.

Brush et al. [8] studied location obfuscation behavior of 12 households (n=32) using always-on GPS devices. Participants mainly wanted to obfuscate places that they frequented (home, work etc.) even from their friends. Benisch et al. [6] conducted a 3-week user study (n=27) and found that more complex privacy settings were the most useful and led to more sharing but also increased the user's burden of privacy management. In a similar vein, Tang et al. [42] studied the effect of offering more disclosure choices in LSAs (n=30). They found surprisingly, that users did not mind the additional burden of adding location granularity features even when presented with several different types of privacy filters. This may lead to more sharing and less complicated privacy management rules. Wilson et al. [49] explored the impact of existing privacy profiles on location sharing with Locaccino (n=37) and concluded that (a) "the complexity and diversity of people's privacy preferences creates a major tension between privacy and usability" and (b) privacy profiles can have a substantial impact on a user's behavior. Wiese et al. [48] presented results (n=42), which indicated that stronger ties, communication frequency and commonality in current locations influence the willingness of location disclosures.

Patil et al. [35] conducted a survey (n=362) to understand privacy attitudes in LBSNs. They realized that privacy concerns in LBSNs are directly tied to future "undesired social consequences." In another study, Patil et al. [36] (n=35) advocated feedback improvement for managing location disclosures. Tsai et al. [45] used Locyotion, (n=56) to understand the impact of location surveillance feedback on future location disclosures. Their main finding was that people want to know who viewed them (but not necessarily the reverse) and they were willing to sacrifice other system features to have this functionality. Boesen et al. [7] conducted an ethnographic study on the impact of location surveillance on strong ties, specifically within households (n=14). They observed that while surveillance can support maintenance of strong tie relationships, it might also have the detrimental effect of undermining existing trust networks. Summarizing this section, we can infer that various approaches (feedback, obfuscation, transparency etc.) exist to manage privacy and surveillance concerns. Location disclosures are affected by tie strength and the nature of relationship between users. What is unknown is if these and other underlying social network factors also influence location surveillance.

Social Networks: Surveillance, Homophily and Ties

Barkhuus [5] called for reconsidering privacy as *contextual integrity*" – a term coined by Nissenbaum [31] who hypothesized that there are norms of appropriateness and norms of information flow in social networks. Privacy is the optimization of negotiating these norms. Barkhuus specifically makes a case for LSAs and writes "*It is the dual pleasure of both being able to expose ones' self and being able to 'snoop' on others' private lives that is at play here.*" She advocates against mandatory design implications, as they may not "*provide more than coarse generalizations*" for phenomena already noted in theory.

The traditional construct [27] of surveillance is hierarchical, vertical and top down with distinct classes of surveillers and the surveilled. Asymmetry and power politics are two salient characteristics of this structure. However, for social media, Andrejevic [2] and Trottier [44] have defined "*lateral surveillance*" and "*interpersonal social media surveillance*"; these are horizontal, peer-to-peer surveillance systems where everyone is equally capable of surveillance. However, they still retain the traditional connotation of negativity associated with surveillance. Albrechtslund [1] framed SNS as "*participatory surveillance*" systems. He opines that surveillance needn't always be punitive or asymmetrical but rather, can act as an empowering catalyst for social sharing. This rests on the fundamental assumption that human beings want to be seen by others and also want to see what others are "up to". Recently, Marwick [28] has also suggested the notion of "*social surveillance*" which is a similar construct but also includes a sense of collaboration, sociability, positivity and interaction around visible personal information.

Homophily and peer influence are accepted [3,24,30,38] as the main reasons behind tie formation and management. De Souza e Silva & Frith [13] propose the "presentation of location"; encapsulating how people manage impressions through location disclosure. They postulate that this might encourage homophily, bonding and trust among people. We also note that people frequently use different SNS platforms with different audiences. Thus, tie management can suffer from context collapse. For instance, partially overlapped but differing audiences on Facebook and foursquare can complicate impression management strategies. Lingel et al. discuss [26] visibility of such conflicts along with code switching strategies of users among different networks.

Summarizing this discussion, we find that there has been a shift in recent frameworks of SNS surveillance. Homophily has been proposed as one contributor towards spatial impression management. What is not clear yet, is its role on location surveillance. Moreover, we do not know yet if

there are negotiations, norms and interactions around visible acts of location surveillance. We therefore ask:

RQ1: Do LBSN users view others similar to them? Is this different from homophily in their friendship networks?

RQ2: Do LBSN users interact with each other around public displays of location surveillance?

METHODS

Research Context and Terminology

We chose foursquare, a manual LBSN as our sandbox for interrogating these research questions. Our primary motivation for this choice is that foursquare is the largest and most popular LBSN [14] (as of May 2014) with over 50 million unique users and 6 billion check-ins. Moreover, the first author is a frequent user of foursquare and is deeply embedded within the foursquare user community. We deemed this an advantage for participant recruitment. A third reason for choosing foursquare is that, unlike Facebook or Twitter which also have location tracking features, foursquare is chiefly based around specific venues without much else interactivity. Finally, there are no standard privacy management features, which are usually available on other platforms such as access control lists or location granularity settings. This is ideal for studying surveillance because the primary user interaction on foursquare is to simply make the decision to (not) check-in. A detailed description [15] of foursquare features mentioned in Table 1 can be found freely online.

Our intended analytic approach was to test for homophily and compare between friendship and surveillance networks. To do this, we needed a fully connected network. In the context of our research study, this is defined as a social network where nodes represent people and ties represent their connections (via foursquare friendships). Fully connected refers to the fact that all the nodes in the network are connected to at least one other node and that, there exists at least one path from one node to every other node. Our choice of participant recruitment reflects this since we needed participants who were connected to each other to test for homophily and non-connected participants would not contribute to the homophily testing process. We followed the comparative approach described by Yuan and Gay [50] to test for homophily between two networks.

For the purpose of this work, we define two networks – a friendship network and a surveillance network. The friendship network is where the edges between the nodes are weighted by the mean of the self-reported tie strength rating. The surveillance network is where the edges between the nodes are weighted by the mean of the surveillance activity between them. The calculations of the weighting variables are defined in the "Variables and Measurements" section.

Data Collection

Data was collected along multiple dimensions. First, users were asked to complete an online consent form that included a series of basic demographic questions. Next, they had to explicitly grant the research team access to their foursquare data using a custom-built web application that communicated with the foursquare API. Unlike the APIs of many other platforms, developers need explicit permission from foursquare users to get access to their complete usage data. Users also had to download and install a simple custom-built mobile phone application (integrated with our custom foursquare data gathering application), which detected when users viewed their friends' check-ins through touch events and sent this information to our servers periodically. This was deployed because the foursquare API does not provide a summary of views for each check-in and was built for Android and iOS users. Finally, we also conducted follow-up semi-structured interviews and debriefing sessions with all our users both, in person as well as via Skype. Here, we also asked the users to rate the strength of their friendship with foursquare friends (those whose data we collected) on a scale of 1-10.

Participant Recruitment

We utilized convenience and snowball sampling using social media (such as Facebook and twitter) and personal contacts to collect data about 65 participants (34 male, 31 female). We collected their entire foursquare usage history as well as a summary of views on their friends' check-ins from May 2013 - January 2014. (9 months) Table 1 describes the overall characteristics of our participants. Our participants represent fifteen different countries including, but not limited to United States, Canada, India, Indonesia, Bangladesh, United Kingdom, Finland, Brazil and South Africa in decreasing frequency. Our participants included frequent as well as sparse users of foursquare indicated by the number of average daily check-ins.

Variables and Measurements

One of our primary challenges was to quantify surveillance activity. In the foursquare mobile application, users can visit their friends' check-ins by navigating to it within the application. This generates a touch event within the application. We use each such touch event as a proxy for a view on a check-in. For each pair of participants, μ_1 and μ_2 (when μ_1 is the focus) we calculate the total number of times μ_1 views any of μ_2's check-ins. We divide this by the total number of unique μ_2's check-ins. This gives us an overall sense of how often μ_1 looks at μ_2's location disclosures. Let us call this τ_{12}. Symmetrically, we can also derive τ_{21}. The arithmetic mean of τ_{12} and τ_{21} is the weight for the tie between μ_1 and μ_2 and gives us a sense of net surveillance activity between these two nodes.

For each pair of participants in the friendship network, μ_1 and μ_2, we calculated the arithmetic mean of their self-reported tie strengths for each other. This is the weight for

the edge between μ_1 and μ_2 and represents an overall sense of the average tie strength between any two nodes. The Pearson correlation metric of tie strength between two pairs of nodes is 0.87 indicating a high level of agreement and the mean was 7.83 hinting towards perceived strong ties.

Variables	Minimum	Maximum	Mean	Std. Dev.
Check-in views	153	1012	443.8	194.13
Total check-ins	137	19435	1556.4	2782.18
Friends	1	999	89.44	193.034
Mayorships	1	189	17.02	43.734
Badges	24	225	34.1	35.96
Tips	1	133	16.15	32.22
Photos	3	761	31.15	110.21
Age	20	61	33	3.3
Income	14400	156000	67000	19342.5

Table 1: Descriptive statistics summarizing participant foursquare usage history and demographics

We selected 5 variables to test for homophily. Our primary motivation for choosing these particular categories comes from prior literature [24,30,38] on network homophily. Age and Income categories were divided into approximately equal sized buckets. We adapted Race and Occupation categories from the US Census classification. Table 2 provides a description of the different levels and categories.

Variables	Category Labels and Descriptions				
Age	18-25	26-34	35-44	45-54	55-64
Gender	Male		Female		
Race	White	African or Black	Asian (incl. Indian subcont.)	Hispanic or Latino	Mixed
Income	0-29999	30000-59999	60000-99999	100000-129999	130000+
Occupation	Unemployed	Student	White Collar	Blue Collar	Self Employed

Table 2: Description of Homophily Variables

Analysis and Results

Homophily Analysis

First, we calculated homophily measures for our network for all variables using the weighted ANOVA density variable homophily model. This is a standard model used in empirical social network analysis and was defined by Hanneman and Riddle in 2005 [18]. This model evaluates the likelihood that the weighted density of ties within each group differs significantly from ties that are not within groups. We performed this analysis by writing a customized script in R and making judicious use of the tnet package [32]. Table 3 contains the results of our analysis.

	Friendship Network		Surveillance Network	
Variables	**Std.β**	**Effect Size (ω^2)**	**Std. β**	**Effect Size (ω^2)**
Gender	0.29	0.12	0.41**	0.53
Age	0.04	0.03	0.01	0.02
Race	0.24	0.2	0.44**	0.64
Income	0.41*	0.24	0.11	0.09
Occupation	0.02	0.01	0.03	0.01
Adjusted r^2	0.43		0.56	
* p < 0.05 ** p < 0.01				

Table 3: Results of Homophily Analysis

Our results suggest that Gender and Race are significant predictors of homophily in the surveillance network. In the case of gender ($\beta=0.41,\ p<0.01$) we also noted a large effect size (ω^2=0.53). This suggests that men and women look significantly more at check-ins by their own gender. Similarly, race ($\beta=0.44,\ p<0.01$) exhibits an even larger effect size (ω^2=0.64) suggesting that location surveillance is divided strongly along racial lines.

In these types of network based ANOVA models, there is no standard agreement on post-hoc tests as the covariance matrices are assumed to be correlated with each other and the variables non-independent. In spite of this, we conducted a post hoc Tukey HSD on Race because of its conservativeness and found significant differences between [White|AfricanorBlack](Tukey$_{HSD}$=*4.86,p<0.01*),[White|Asian](Tukey$_{HSD}$=*5.13,p<0.01*)and[Asian|Hispanic](Tukey$_{HSD}$ *=5.02, p<0.01)*. We urge the readers to take these particular findings with a pinch of salt because of the lack of statistical unanimity. However, this could imply a further degree of difference among these racial constructs.

In the friendship network, Income ($\beta=0.38,\ p<0.05$) is the only significant predictor of homophily. However, it only demonstrated a modest effect size (ω^2=0.23) implying that while it is significant, the strength of its importance is not very high as it pertains to homophily in this case. We hypothesize that this effect is possibly because friends of

the same income level initially started using foursquare together and as time progressed, they started adding other friends from other groups and "diluted" this affinity.

The main takeaway from this analysis is that, there is a significant difference between the friendship and surveillance network in terms of homophily. This highlights how latent networks reveal hidden trends about social interactions that could otherwise not be easily measurable.

Analysis of Comments and Interviews

There were a total of 4278 comments on 2856 unique check-ins. About 73.8% of these comments were made by users belonging to a similar category as that of the original user. We asked our participants questions focused on privacy concerns, surveillance, commenting patterns and location disclosure strategies. We also showed specific examples of their comments and asked them to reflect on the reasons behind their comment. The average interview length was 37 minutes and was transcribed manually by the first author. We utilized grounded theory [16] to analyze comments and interview transcripts. We iterated through the data seeking frequently occurring themes and concepts, gradually generalizing trends after discussions. We report three main themes here. All participant names are changed but reflect their ethnicity, gender and national origin.

Location Surveillance: Motivations and Strategies

Participants frequently mention that their foursquare network is different from other SNS network. This has a lot to do with perceived surveillance. For instance, Jack mentions his general "friending" strategy for foursquare:

"I don't accept random friend requests on foursquare like I do on Facebook. My foursquare friends … I know all of them in real life pretty well … I don't want random stalking from people I don't know but people, I know, that's fine."

However, this does not mean that there are no concerns at all about privacy and surveillance but rather, they might be substantially nuanced, contextual and spatio-culturally dependent. Hao is conscious about possible conflict with his family in China:

"I don't want my mother or father seeing me late night checkins to a bar. They know I drink but they don't see that I also study a lot. That's not visible to them but most places [he visits] *are fine. "*

Perceived visibility is one significant factor affecting location surveillance concerns. Frequently, participants would comment on their friends' check-ins to make this explicit. For instance, John commented:

"Yo ! I just saw you check-in to Teagle [a gym] *Wassup?"*

We followed up with John who remarked that he had never seen his friend at that venue before and therefore was both surprised and curious to know he was there.

We also specifically asked participants what would motivate them to look at and/or comment on their friends' check-ins. One frequent reason was that they were curious about check-ins by friends to unexpected locations or times. For example, Megan says:

"Normally, I glance at all my friend's check-ins when I go to check-in myself but if I see them at some cool new venue or somewhere I wouldn't expect them to be or go to then I'll go to that check-in and at many times I'll either like it or write a comment on it as well."

She comments on a friends' ongoing date to an expensive restaurant – something unexpected, which we learnt when we followed this comment up while interviewing her.

"Hows the boy? John Thomas [the venue] *!! Good call !"*

"Ping me if you want a rescue call - hope he's not on foursquare to see this ! hahaha"

Another reason is that most people were curious to see where friends with similar interests check-in. This might give them ideas for future activities other friends. For instance, George had the following to say about his friend:

"My friend [name removed] *and I lift weights together and do other outdoorsy things together. I am always curious to see, especially if she is visiting someplace else if she is checking in to a new trail or outdoors store or meeting up with other friends to do fitness things. It gives me a good idea what I can expect to do if I visit this place or if I can do something similar."*

We also found evidence that participants had evolved different strategies to deal with perceived location surveillance. These were, at many times, conflated with impression management. The ability to not check-in becomes very important in these cases. Tim remarks:

"Sometimes, if I don't want people to know I am somewhere, I just won't check-in. … I feel like even if it's my best friend, he doesn't need to know where I am and what I am doing at every point of time… I like my privacy sometime even though I am pretty active on foursquare and check-in a lot during the day. "

Some participants mentioned deceptive or obfuscating strategies in "gaming" location surveillance, especially to ward off spontaneous social coordination. Sarah says:

"I'll check-in to a place nearby or something completely different to where I am right now sometimes if I see that a friend is nearby. I like to be alone sometimes but still want to track my location generally. I have done with this with really good friends too."

Location Surveillance: Interaction and Collaboration

Another persistent theme from our data is how two or more foursquare friends will frequently comment, collaborate and coordinate about surveilling a *third* friend and even have conversations with the latter about their effort. For instance, Frank and Tim talk about observing the a friend.

Frank: "John went to more bars than you last night! :P"

Tim: *"Yep ! 6 bars?"*

Frank: *"Mans having fun in NYC !"*

Tim: *"I checked out the places … pretty expensive - I can't afford that without help. :D :D"*

Frank: *"Rich gf* [girlfriend]. *:P"*

This is a very interesting example because of two reasons. First, both Frank and Tim are friends with their common friend on foursquare. One peculiar design mechanic of foursquare is that all friends can see all check-ins at all times i.e. there are no access control lists or similar types of privacy-preserving features. Therefore, potentially, their common friend can see and react to this conversation. Second, this conversation is on Tim's check-in at a local bar and while initially being sparked by the type of venue that Tim checked in to has actually little to do with it.

Playful interaction could also be mixed with more explicit and implicit announcements of surveillance and this interaction could take place across a series of check-ins. Take for instance, a set of three comments on three different and successive check-ins of a friend by Jane. The first is at an ice cream parlor; the second in a park and the third at an outdoor entertainment venue, which includes a mini golf course.

"Ice cream ! I want some right now !"

"I hate that I am working now and seeing everyone having fun. [online on foursquare]"

"BTW, I am so totally stalking you right now. :P :P "

It is evident from these comments that Jane is engaging in a sustained communication about her surveillance (and associated offline social objectives) with her friend across distinct check-ins. This one-way interactivity is often extended to multi-party conversations. In one case, Tony and Jill had interacted on a check-in to a tattoo studio.

Tony: "*heh. when this popped up i couldn't believe it … looks like someone's getting inked !"*

Jill: "*And now you have witnesses to back this up !"*

Tony: "*Yeah ! give us monies or we will tell your boss !"*

It is clear that Tony and Jill have both observed their friends' check-in to a tattoo studio around the same time and signaled their inspection of this check-in to him. Furthermore, the tone of their banter is lighthearted and centers on making light hearted fun of their friend.

We also observed instances of similar behavior where the participants would tag the object of their conversation. There is a feature where multiple friends can be tagged in the comments section of a check-in. These friends would then get a notification regarding this tag and can then ostensibly visit that check-in. Sometimes, these friends would respond to comments and create an interactive atmosphere of lighthearted repartees. In one case, Stephanie tagged Olivia on Robert's check-in and bantered:

Stephanie: *"Running downtown are we?"*

Robert: *"grocery run + supplies!"*

Stephanie: *"you should have gone with Olivia [tagged] … think she spends 5 hours in Wegmans* [a local grocery store]"

Robert: *"I don't want to be late like her all the time"*

Olivia: *"Who said I am late? "*

Olivia: *"PS: Stop stalking me all the time you guys! :P"*

Stephanie: *"Can't help it. You are always late!"*

Robert: *"You said it sister!"*

Olivia: *"I am not always late! Don't trust foursquare. :P"*

Stephanie: *"Yeah right ! Don't you always checkin the moment you enter a place? :P"*

Clearly, two of the three friends have been watching her activities on foursquare as well as how and when she checks in when entering a new place. This provides fodder for a fascinating conversation on her activities and even provides an opportunity for the object of surveillance to chime in and interact with her observers.

Location Surveillance: Design Reflections

We also asked participants questions about their experience with the current foursquare platform and feedback for improving their own experience. There were two general trends from this discussion. First, some participants expressed interest in some privacy management features. Anna expresses some frustration and suggests:

"I feel like foursquare is sometimes too minimalistic. Its true that random people can't stalk you like they can on facebook but sometimes you want to hide stuff from your friends as well and I think that having the ability to hide certain check-ins from some people might be cool."

Meanwhile, some participants like Tina think that knowing who watched whom or an implementation of a feedback system could be very useful for foursquare users.

"*You know like Orkut had this thing where you could see which people were visiting your profile. I think that if something like that can be built here then we can have a better idea of who was visiting our profile or check-ins. This can be something very useful to foursquare users like me to know who is visiting your profile.* "

However, there were a substantial number of participants who thought that the current system worked well enough for their purposes. Specifically, Mary remarked:

"I think that I am fine with how foursquare is currently. I like being able to see what my friends are upto and also I filter who I add on foursquare … its always good friends … I have like 800 Facebook friends but 25-ish friends on foursquare … I don't mind them knowing where I am. If its that big a deal, I just won't checkin somewhere … there is no point in adding too many things. I don't like Facebook for this reason."

We see that some participants want some changes to design to improve their privacy management experience whereas others seemed quite content with the present systems.

DISCUSSION

We proposed two research questions in this paper. **RQ1** focused on whether LBSN users would look at the location disclosures of others similar to them and if this would be different than the similarities in their friendship ties. **RQ2** concentrated on whether there were user interactions around overt declarations of location surveillance. The results of our study provide answers supporting both **RQ1** and **RQ2** and we discuss these in the following sections.

Homophily and Location Surveillance

It is well accepted that homophily and social influence [3,24,30,38] guide formation and maintenance of social ties. Drawing a causal arrow between these factors is intractable for most empirical studies. This is further exacerbated when dealing with tacit networks. Shalizi & Thomas [38] recommends a strategy of holistic storytelling when reporting results. In this vein, our homophily analysis constitutes one piece of the overall narrative.

Consider **RQ1**. Do people view others similar to them? Or is it their similarity that drives their surveillance? Our quantitative analysis informs us that homophily differs between friendship (income) and surveillance networks (race, gender). The dimensions themselves are quite common and have been used in a wide range [30,38] of prior work. What is curious is that they differ along two different networks constituting the same people. Here, we can make two broad inferences. First, homophily type affects surveillance. There is scholarship on the gendered nature of locations [33] as well as differential surveillance [29] on genders. We argue that perhaps it is the dissimilar participation of gender in different locations that also drives homophilic tendencies. Similarly, prior literature also points towards racially constructed spatial participation [27] as well as the unequal nature of surveillance [47] among and on races. Second, recent work [11,13,17] has alluded to the construction of self-presentation using specific acts of location disclosures. The discloser may use this to cultivate favorable impressions assuming homophilic surveillance and unintentionally resulting in a self-fulfilling prophecy.

Public Displays of Location Surveillance

Andrejevic [2] argued that asymmetry and differential power is the one of the key characteristics of surveillance. In this light, those who are being watched may not know if, when and how they are being watched. However, Albrechtshlund [1] maintains that SNS, which facilitate and enhance interactions between different people, cannot be framed from such a vertical perspective. Rather, surveillance, in this case, can be a "*mutual, empowering and subjectivity building practice*." This, supported by our qualitative results is yet another piece of the narrative.

Let us appraise **RQ2**. Consider Tony and Jill, who commented on Mike's check-in. It is evident that they noticed Mike's check in to a tattoo studio. Their playful banter reveals their tacit surveillance of Mike's activities and even playfully "threatens" to report this to his boss who may or may not be supportive of an employee getting tattoos as it is considered a social taboo in some societies. Mike, on the other hand, had no problem in revealing his location to his foursquare friends and in fact, this free revelation (that may potentially reveal an action against workplace policies) is in itself quite empowering.

Guha and Birnholtz [13] found that foursquare users are careful about accepting foursquare friends as opposed to accepting friends on other SNS such as Facebook; foursquare friends tend to be relatively stronger ties. Thus, disclosing a particular location that may imply a certain set of behaviors (in Mike's case, getting a tattoo) to stronger ties is evidence of trust, empowerment and legitimization of offline actions.

However, there may be another interpretation from these results. During interviews, participants reported that if concerned about privacy or self-presentation, they would usually make the decision to not check-in to their current location. We did not find overtly negative reactions to surveillance within comments. This may imply that self-censorship and prudent non-use is used to manage and hide potentially negative or undesired consequences from presentation of location.

Collaborative social surveillance also resonated strongly within our results. Marwick [28] defines social surveillance as *"the ongoing eavesdropping, investigation, gossip and inquiry that constitutes information gathering by people about their peers, made salient by the social digitization normalized by social media."* Our results reinforce this definition. Take for instance, the interaction between Stephanie, Olivia and Robert around disclosing location about a grocery store, which has all the aforementioned elements of social surveillance.

However, Marwick also concludes that while the structure of social surveillance may be different from traditional surveillance and may have a few positive effects, the end result is the same - there are constantly shifting elements of power, hierarchy and reciprocity in both frameworks. We believe that her examination of twitter and Facebook - while applicable to them may not be perfectly amenable to LBSNs like foursquare. Both twitter and Facebook have audience management features embedded in their design while foursquare is minimalistic; everything is visible and there are no access control features. Guha and Birnholtz [17] found that the primary option for foursquare users to manage impressions and/or audiences is to *not* disclose their location or, for a minority, to opt for deceptive location disclosures. Thus, if foursquare activity must mean making everything visible to everyone, then

everything has the potential to be seen and interacted with. As our results indicate, this makes social surveillance a symmetric, collaborative and positive process, especially for strong ties and along the homophilic tendencies of gender and race that historically have a natural tendency to cluster around specific locations.

Humphreys [19,20] found that Dodgeball users (considered the precursor of foursquare) to be generally unconcerned about privacy. She found two reasons - (a) they felt that they had no control over their personal information and to whom it was sent and (b) they believed that they were experienced Internet users with a keen sense for online friendships. Let us examine our results keeping these in mind. First, social surveillance theory [28] predicts that people want to see, be seen, interact and be interacted with online. Thus, while these location disclosures are voluntary, they are also somewhat influenced by the positivity and the participatory aspect of surveillance that we have seen in our analysis. Second, homophily theory [30] predicts that a common attribute, group membership or affiliation influences people to form ties with one another. Thus, people not only want to see and be seen online, they want to see and be seen by those with whom they closely identify and align with. This, in essence, is one of our main takeaways from this work.

Implications for Design (Or Not?)

Our results also raised two issues about privacy-aware design in LBSNs. On one hand, some of our participants wished for more support on foursquare to manage their privacy and social surveillance goals. Anna is an exemplar of a vocal minority who wishes that foursquare changes its minimalistic ways and begins to listen to the concerns of those who would want to selectively disclose locations and manage privacy concerns. Tina specifically evokes the feedback and transparency features in Orkut and hopes that similar mechanisms are also implemented on foursquare.

Prior work has shown that feedback and translucence are important design considerations in LSA's. Stuart et al. [40] distinguished between identity, content and interaction transparency. Interestingly, foursquare is unusually transparent in terms of content and interaction transparency but not for identity transparency. Incorporating user customizable functions of translucency might support the overall empowerment and positivity that social surveillance brings to LBSNs. Tsai et al. [45] and Patil et al. [36] found that feedback is extremely important in privacy management in LSAs. Currently, foursquare offers no feedback mechanisms (other than standard social networking features such as a like button and a comment space). Feedback can take many forms - understanding who or what groups are interacting with a user might go a long way towards supporting behavior that is already prevalent on foursquare while preserving privacy concerns. For instance, summarized feedback about location disclosure and surveillance might buttress existing online interaction, facilitate offline serendipitous coordination or if necessary, allow users to surveil and avoid friends from different groups at different times - thus preserving privacy. Such features can support increased or decreased sociability depending upon the user's needs while being unobtrusive and out of the way of regular usage.

Another group of our participants, illustrated by Mary's comment, wants to preserve the current status quo on foursquare. According to this faction, they are generally happy with their foursquare experience. They cite their "friending" strategies as well as the choice to not check-in to be adequate. Their main concern is that they don't want foursquare to become complicated like other oft used SNS.

Barkhuus [5] and Dourish [12] called for understanding the limits of design interventions on human-centered systems. While Dourish advocated for the removal or elimination of mandatory design implications in the reports of every HCI research study, Barkhuus discouraged the necessity of designing technological solutions, specifically mentioning LSAs. Perhaps, in our study, this makes a case for specific design interventions superfluous? Shall we fix something that is not yet broken? Or shall we preemptively design for a particular future that may not come to pass? This could be a useful theoretical consideration for future designers of privacy-aware features in LBSNs.

LIMITATIONS AND FUTURE WORK

We used a mixture of convenience and snowball sampling for participant recruitment. This was a hard constraint since people had to be willing to install our custom mobile application and grant us full access to their usage data. A sample size of 65 satisfies our statistical assumptions and is historically comparable to similar studies. We plan to scale up in a future project and tease out finer patterns and practices. In particular, we would like to delve into location deception and obfuscation strategies as well as peer influence. Another limitation was that our custom application was developed for Android and iOS platforms. We could not build for Windows platforms for a lack of resources and expertise. However, we also note that during data collection, Windows phone participants made up less than 2% of our initial survey respondents. Windows phone installations for foursquare lag behind the other platforms.

CONCLUSION

In this paper, we have explored how people view their friends' location disclosures in a LBSN through the lens of homophily through an empirical study of 65 foursquare users. We discovered that implicit surveillance in location sharing is strongly homophilous along race and gender while the friendship network displays homophily for income. Qualitatively, we find that location surveillance can be a social, collaborative and positive process rather than current theoretical frameworks that mainly focus on power and information asymmetry. We discuss both sides of the design intervention argument leaving the readers with the partially rhetorical question of whether it is appropriate

to design for more privacy or more transparency if there is no compelling need for the users to change the status quo.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their constructive and detailed reviews. This project was supported by National Science Foundation Grant No.1016203.

REFERENCES

1. Albrechtslund, A. Online social networking as participatory surveillance. *First Monday*,13, 3 (2008).
2. Andrejevic, M. The discipline of watching: Detection, risk, and lateral surveillance. *Critical Studies in Media Communication*, 23,5 (2006), 391-407.
3. Backstrom, L., Huttenlocher, D., Kleinberg, J., & Lan, X. Group formation in large social networks: membership, growth, and evolution. In *Proc. SIGKDD* (2006). 44-54.
4. Barkhuus, L., Brown, B., Bell, M., Sherwood, S., Hall, M., & Chalmers, M. From awareness to repartee: sharing location within social groups. In *Proc. CHI* (2008), 497-506.
5. Barkhuus, L.The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. In *Proc. CHI* (2012), 367-376.
6. Benisch, M., Kelley, P. G., Sadeh, N., & Cranor, L. F. Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs. *PUC*, 15,7 (2011), 679-694.
7. Boesen, J., Rode, J. A., & Mancini, C. The domestic panopticon: location tracking in families. In *Proc. Ubicomp* (2010), 65-74.
8. Brush, A. J., Krumm, J., & Scott, J. Exploring end user preferences for location obfuscation, location-based services, and the value of location. In *Proc. Ubicomp* (2010), 95-104.
9. Brown, B., Taylor, A. S., Izadi, S., Sellen, A., Jofish'Kaye, J., & Eardley, R. Locating family values: A field trial of the Whereabouts Clock. In *Ubicomp* (2007), 354-371.
10. Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. Location disclosure to social relations: why, when, & what people want to share. In *Proc. CHI* (2005), 81-90.
11. Cramer, H., Rost, M., & Holmquist, L. E. Performing a check-in: emerging practices, norms and 'conflicts' in location-sharing using foursquare. In *Proc. Mobile HCI* (2011), 57-66.
12. Dourish, P.Implications for design. In *Proc. CHI* (2006), 541-550.
13. e Silva, A. D. S., & Frith, J. *Mobile interfaces in public spaces: Locational privacy, control, and urban sociability*. Taylor & Francis, 2012.
14. foursquare. URL: https://foursquare.com/about/
15. foursquare platform feature descriptions. URL: https://support.foursquare.com/hc/en-us
16. Glaser, B., & Strauss, A. *The discovery of grounded theory*. Weidenfield & Nicolson, London, 1967.
17. Guha, S., & Birnholtz, J. Can you see me now?: location, visibility and the management of impressions on foursquare. *In Proc. Mobile HCI* (2013), 183-192.
18. Hanneman, R. A., and Riddle, M.*Introduction to social network methods*. University of California, Riverside, 2005.
19. Humphreys, L. Mobile social networks and social practice: A case study of Dodgeball. *JCMC,* 13, 1 (2007), 341-360.
20. Humphreys, L. Mobile social networks and urban public space. *New Media & Society*, 12, 5 (2010), 763-778.
21. Humphreys, L. Who's watching whom? A study of interactive technology and surveillance. *Journal of Communication*, 61, 4 (2011), 575-595.
22. Iachello, G., Smith, I., Consolvo, S., Chen, M., & Abowd, G. D.Developing privacy guidelines for social location disclosure applications and services. In *Proc. SOUPS* (2005), 65-76.
23. Iachello, G., & Hong, J. End-user privacy in human-computer interaction. *Foundations and Trends in Human-Computer Interaction*, 1, 1 (2007), 1-137.
24. Lewis, K., Gonzalez, M., & Kaufman, J. Social selection and peer influence in an online social network. *Proceedings of the National Academy of Sciences*, 109, 1 (2012), 68-72.
25. Lindqvist, J., Cranshaw, J., Wiese, J., Hong, J., & Zimmerman, J. I'm the mayor of my house: examining why people use foursquare-a social-driven location sharing application. *In Proc. CHI* (2011). 2409-2418.
26. Lingel, J., & Naaman, M. 2014. City, self, network: transnational migrants and online identity work. In *Proc. CSCW* (2014), 1502-1510.
27. Lyon, D. *Surveillance Studies: An Overview*. Polity Press, Cambridge, 2007.

28. Marwick, A. E. The Public Domain: Social Surveillance in Everyday Life. *Surveillance & Society*, 9, 4 (2012).

29. McCorkel, J. A. Embodied surveillance and the gendering of punishment. *Journal of Contemporary Ethnography*, 32, 1 (2003), 41-76.

30. McPherson, M., Smith-Lovin, L., & Cook, J. M. Birds of a feather: Homophily in social networks. *Annual Review of Sociology*, 27 (2001), 415–444.

31. Nissenbaum, H. Privacy as contextual integrity. *Wash. L. Rev.*, 79, (2004) 119.

32. Opsahl, T. Structure and Evolution of Weighted Networks. University of London (Queen Mary College), London, UK, (2009), 104-122. URL: http://toreopsahl.com/tnet/

33. Pavlovskaya, M., & Martin, K. S. Feminism and geographic information systems: From a missing object to a mapping subject. *Geography Compass*, 1, 3 (2007), 583-606.

34. Page, X., Knijnenburg, B. P., & Kobsa, A.What a tangled web we weave: lying backfires in location-sharing social media. In *Proc. CSCW* (2013), 273-284.

35. Patil, S., Norcie, G., Kapadia, A., & Lee, A. J. Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice. In *Proc. SOUPS* (2012), 5.

36. Patil, S., Schlegel, R., Kapadia, A., & Lee, A. J.Reflection or action?:how feedback and control affect location sharing decisions. In *Proc. CHI* (2014), 101-110.

37. Reilly, D., Dearman, D., Ha, V., Smith, I., & Inkpen, K. "Need to know": examining information need in location discourse. *Pervasive Computing*, (2006), 33-49.

38. Shalizi, C. R., & Thomas, A. C. Homophily and contagion are generically confounded in observational social network studies. *Soc. Methods & Research*, 40, 2 (2011), 211-239.

39. Smith, I.Consolvo, S., Lamarca, A., Hightower, J., Scott, J., Sohn, T.,Hughes,J,Iachello,G and Abowd, G. D. Social disclosure of place: From location technology to communication practices. *Pervasive Computing*, (2005), 134-151.

40. Stuart, H. C., Dabbish, L., Kiesler, S., Kinnaird, P., & Kang, R. Social transparency in networked information exchange: a theoretical framework. In *Proc. CSCW* (2012), 451-460.

41. Tang, K. P., Lin, J., Hong, J. I., Siewiorek, D. P., & Sadeh, N. Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing. *In Proc. Ubicomp* (2010), 85-94.

42. Tang, K., Hong, J., & Siewiorek, D. The implications of offering more disclosure choices for social location sharing. In *Proc. CHI* (2012), 391-394.

43. Toch, E., Cranshaw, J., Hankes-Drielsma, P., Springfield, J., Kelley, P. G., Cranor, L.,Hong,J. and Sadeh, N. Locaccino: a privacy-centric location sharing application. In *Proc. Ubicomp-Adjunct* (2010), 381-382.

44. Trottier, D. Interpersonal surveillance on social media. *Canadian Journal of Communication*, 37, 2 (2012).

45. Tsai, J. Y., Kelley, P., Drielsma, P., Cranor, L. F., Hong, J., & Sadeh, N.Who's viewed you?:the impact of feedback in a mobile location-sharing application.In *Proc. CHI* (2009),2003-2012.

46. Want, R., Hopper, A., Falcao, V., & Gibbons, J. The active badge location system. *ACM Transactions on Information Systems*, 10, 1 (1992), 91-102.

47. Wicker, S. B. *Cellular Convergence and the Death of Privacy*. Oxford University Press, 2013.

48. Wiese, J., Kelley, P. G., Cranor, L. F., Dabbish, L., Hong, J. I., & Zimmerman, J. Are you close with me? are you nearby?: investigating social groups, closeness, and willingness to share. In *Proc. Ubicomp* (2011), 197-206.

49. Wilson, S., Cranshaw, J., Sadeh, N., Acquisti, A., Cranor, L. F., Springfield, J.,Jeong, S.Y. and Balasubramanian, A. Privacy manipulation and acclimation in a location sharing application. In *Proc. Ubicomp* (2013). 549-558.

50. Yuan, Y. C. and Gay, G. Homophily of Network Ties and Bonding and Bridging Social Capital in Computer-Mediated Distributed Teams. *JCMC*, 11, 4 (2006), 1062–1084.