Location-Based Social Networking and its Impact on Trust in Relationships

Sarah Jean Fusco, Roba Abbas, Katina Michael, Anas Aloudat
School of Information Systems and Technology, Faculty of Informatics
University of Wollongong
Wollongong, Australia
{sjf462, ra75, katina, anas}@uow.edu.au

Location based social networking (LBSN) applications are part of a new suite of social networking tools. LBSN is the convergence between location based services (LBS) and online social networking (OSN). LBSN applications offer users the ability to look up the location of another "friend" remotely using a smart phone, desktop or other device, anytime and anywhere. Users invite their friends to participate in LBSN and there is a process of consent that follows. This paper explores the potential impact of LBSN upon trust in society. It looks at the willingness of individuals to share their location data with family, friends, co-workers, the government, commercial entities and even strangers..

I. LOCATION-BASED SOCIAL NETWORKING

LBSN is a location based service that utilizes location information to facilitate social networking. LBSN applications allow users to view the location of their "friends" and/or allow users to view information about other users of LBSN applications that are located in proximity. Users invite their friends to participate in LBSN and there is a process of consent that follows, in which users provide permission for their location information to be viewed to varying levels of detail depending on their chosen settings. The manner in which LBSN applications work is illustrated simplistically in Figure 1, although variations to this model exist. LBSN applications such as Loopt, Fire Eagle, Navizon, iPoki, Locago, ZinTin, iFob, WhosHere and Google Latitude enhance our ability to perform overt or covert social surveillance. These applications enable users to view and share real time location information with their family and friends. With the emergence of this technology it is crucial to consider, as suggested by Kling, that "technology alone, even good technology alone is not sufficient to create social or economic value" [1]. Further to not contributing "sufficient" economic or social value, Kling and other scholars, such as Kraut et al., have identified that technologies can have negative impacts on society [2].

As location based social networking technologies are used between people they have the potential to impact relationships, which are integral not only to the operation of society but also to the individual's well being [3]. By enabling real-time location tracking, LBSN puts location-based technologies in the hands of "friends" while also enhancing the experience of online social networking (OSN). In essence it meshes together the positives and negatives of online social networking and location-based services, creating a unique domain of enquiry, forcing researchers to ask new questions. The purpose of this paper is to explore the possible implications of location based social networking upon relationships, with a particular emphasis on trust.

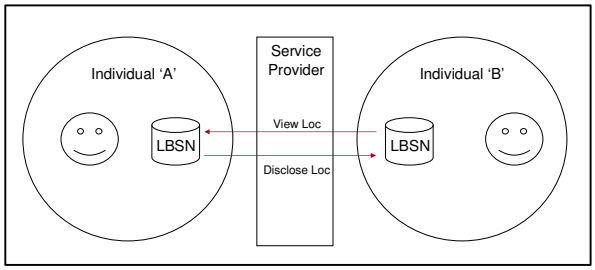

Figure 1. How location-based social networking applications work

II. STUDIES IN TRUST AND TECHNOLOGY

The domain of trust has been studied from a variety of disciplines. Some of the landmark works in the field of computer science and related areas of study have been contributed by Marsh [4] in general computer science, Jøsang [5] in computer security, Braynov and Sandholm [6] in electronic commerce, Resnick [7] in reputation systems, Castelfranchi and Falcone [8], [9] in multi-agent systems, Snijders and Keren [10] in game theory, and Slovic [11] in risk management. Outside areas of computing, economists such as Dasgupta [12], psychologists such as Erikson [13], and sociologists such as Coleman [14] and McKnight [15] have studied trust. The majority of studies to do with trust and social networks examine trust using formal methods which are mathematically-based techniques for the specification, development and verification of online systems. The studies are mainly focused on algorithms [16] or frameworks [17] that provide users of online social networks with trust ratings.

This study does not seek to replicate any of the previous research approaches on online social networks but rather hopes to break new ground in the exploration of the potential social implications of location-based social networking. This study gathered primary qualitative data in response to a research question- what is the impact of LBSN usage upon

trust. In this research project definitions of "trust" have been sourced from sociologists and management/organizational theorists, and presented in an unashamedly informal manner in contrast to the understandably rigid approach that has been taken in typical studies using formal methods.

Until 2009, there were very few qualitative studies that explored the concept of trust in online social networking. Despite being written prior to the birth of Web 2.0, Helen Nissenbaum's [18] seminal work on online trust is still relevant. She summates that trust is "key to the promise the online world holds for great and diverse benefits to humanity" and that generally "[p]eople shy away from territories they distrust" (p. 102). If location-based social networking applications are to stand the test of time, trust will be a key issue in their success and beneficial flow-on effects to society. Other works have considered how to build trust in an organizational context, and these studies have specifically looked at trust with respect to relationships and life which are also relevant aspects of this research [19].

With respect to trust in online social networks, Gross and Acquisti [20] have said that: "trust in and within online social networks may be assigned differently and have a different meaning than in their offline counterparts… [and that] trust may decrease within an online social network". There are three studies which have investigated the impact of OSN upon trust. The first by Dwyer, Hiltz and Passerini [21], compares perceptions of trust and privacy between different OSN applications. The second study, conducted at Ryerson University identifies the potential for OSN to impact upon trust, and the third study by Gambi and Reader [22] aimed to determine whether trust was important in online friendships. For a comprehensive literature review on the topic of location based social networking see Fusco, Michael and Michael [23,24].

A basic definition of trust, according to Rousseau and Sitkin, is the "[w]illingness to be vulnerable under conditions of risk and interdependence" [25]. Furthermore, Mayer et al. [26] describe that trust exists between persons "irrespective of the ability to monitor or control that other party." This is particularly pertinent when one considers the function of looking up the location of a friend or family member to check whether they are doing the right thing. The literature generally describes three forms of trust- cognitive, emotional and behavioral. Cognitive trust is considered to be based on "good reason" or "evidence of trustworthiness". According to Lewis and Weigert [27], "trust on the cognitive level of experience is reached when social actors no longer need or want any further evidence or rational reasons for their confidence in the objects of trust". Emotional trust is when two people trust one another because of the bond they share. The emotional component is present in all types of trust but it is normally most intense in close interpersonal trust, e.g. husband and wife. Behavioral trust has to do with behavioral enactment. It is important to highlight that trust is not static but dynamic in relationships. It also evolves as parties interact over time. The main stages of trust include (i) creation, (ii) development, and (iii) maintenance. In general "[w]hen a trustor takes a risk in a trustee that leads to a positive outcome, the trustor's perceptions of the trustee are enhanced. Likewise, perceptions of the trustee will decline when trust leads to unfavorable conclusions" [12]. Location-based social networking has the potential to strengthen trust between two or more persons (e.g. in business), but it also has the potential to erode trust and to lead to unfavorable conclusions (e.g. between husband and wife).

III. Research on Location Sharing

Several studies have been conducted that are centered on location-sharing applications and users' willingness to share location information. One of the earliest studies to be conducted, by Barkhuus, involved a two phased study comparing perceived privacy concerns with actual privacy concerns within a closed LBS environment [28].The research found that although users were concerned about their privacy in the actual situation of the closed environment the concern for privacy became less over time. A closed LBSN ecosystem differs from public LBSN in that it does not broadcast one's real-time location continuously as a public transaction, such as in the case of Facebook's Places. Another user study by Patil and Lai observed the configuration of privacy settings on a workplace-based LBS [29]. The study found that grouping permissions provided a convenient balance between privacy and control.

Tsai et al. [30] alternatively conducted an online survey of 587 participants in order to determine the perceived risks and benefits of users regarding location-sharing applications and therefore determine their privacy concerns. The authors also examined the privacy controls of commercial applications to determine whether they address the identified risks, and found that participants generally felt the risks associated with location-sharing applications overshadow the benefits, particularly in situations such as revealing their home location or being stalked. Furthermore, it was suggested that current privacy controls insufficiently address the user's privacy concerns, and therefore the authors offer guidelines for developers to address the shortcomings.

Anthony et al. [31] provided an alternative approach to measuring whether users were willing to disclose location information, conducting a study with 25 undergraduate students in order to examine the role, place and the requester with respect to willingness to share. The results of the study revealed that participants' privacy concerns are dependent on place and with whom they are sharing their location data. For instance, participants are generally willing to share location information with individuals on a predefined list as opposed to email, and when at home as opposed to in public places. These results differ from existing LBSN studies that suggest users will promote or share information in public places or when with friends.

Other studies are also centered on providing design recommendations based on user preferences. In a study describing how the prevalence of micro-blogging has affected location sharing applications and practices, Tang et al. [32] state that users are engaging in the social-driven form of location dissemination, rather than purpose-driven

forms of location-sharing; that is one-to-many versus one-to-one respectively. The authors performed a two-week study engaging nine participants to compare both forms of location sharing. Research results indicate that social-driven location sharing is concerned with impression management and the desire to attract attention by disclosing a particular location that may be considered favorable by those within one's social network. However, privacy concerns were also cited as important in determining the type of location information to be provided. These findings have several implications with respect to privacy and design, in that they enable informed design decisions to be made regarding the most suitable data types and visualizations that should be integrated into the application.

Moving away from a focus on privacy and location-sharing, Consolvo et al [33] conducted a three phased study exploring whether social networking users would use location enhanced computing in the first phase, the response of users to in situ hypothetical requests for information in the second, and a reflection upon the prior two phases in the final stage.

More relevant to location disclosure and trust, Boesen et al. [34] examined the use of LBS in the family context, focusing on four households familiar with LBS technology. The results of the study indicated that usage patterns vary amongst family members, and that the use of LBS in families results in benefits and concerns. The study found that while LBS was chiefly used for safety purposes, issues relevant to trust inevitably emerged in that common social interactions that aid in maintaining trust are being replaced with electronic interactions. The authors further suggest that in order to avoid the domestic and digital panopticon, mechanisms to preserve trust must be introduced.

Numerous studies also employed the use of actual or tailored LBSN, as opposed to focusing on closed or controlled environments. These include Brown et al's implementation of the 'Whereabouts Clock' [35], Humphrey's year-long qualitative field study on the LBSN 'Dodgeball' [36], Barkhuus et al's trial of 'Connecto' [37], and Vihavaninen et al's field trials of 'Jaiku' [38].

The cited studies vary in their approach to measuring users' willingness to share location within specific contexts and with specific individuals, applying varying methodologies in doing so. Some of the studies were conducted in controlled environments, while others involved the actual use of location-aware technologies. Many of the studies concentrated on understanding the use and usability of the devices, and users' perceptions of privacy. What has been unexplored in the area of LBSN is the concept of trust, and the effect of LBSN applications upon social relationships. This research aims at addressing this gap, by investigating the effect of LBSN, with a particular focus on its implications upon trust between "friends".

IV. Who Do You Trust with Your Real-time Physical Location?

The problem addressed by this research is: who would you willingly share your real-time physical location with, using an online social networking application? The purpose of this paper is to understand the bidirectional relationship between members of society (who are or might become online social networking users) and the LBSN technology itself (device, application, platform), in order to discover the potential circumstances within which trust will be negatively affected. The nature of social informatics warns against a simplistic cause and effect approach to technology [39]. As such this research topic does not contain simple propositions that A causes B, rather it is developed upon a set of questions that reflect the interrelated social and technical aspects of the research.

- What relationships will LBSN be utilized within?
- How is trust understood in these relationships?
- What are the limits of LBSN usage between people?
- What are the likely impacts of LBSN?

V. Focus Group Research Design

The purpose of this research was to explore the use, application and issues in using LBSN applications between friends, with a particular focus on the concept of trust. This was achieved through the use of focus groups to explore and discuss the use and implications of LBSN. Focus groups enable data collection through group interaction [40], thereby allowing attitudes, beliefs and feelings to emerge [41].

Five focus groups were conducted for this study. The focus groups were conducted with students enrolled in a third year core subject covering professional practice and ethics, in the information technology and computer science curriculum at the University of Wollongong in the first week of May 2009. Given the background of the students who participated in the study, all were technology literate and able to grasp and understand (if not already using) Web 2.0-based applications.

Morgan states that large focus groups can consist of between 15 to 20 participants and are appropriate for topics that are not emotionally charged. Larger groups are renowned for containing "a wide range of potential responses on topics where each participant has a low level of involvement" [40]. It should be noted that each focus group in this study consisted of 18 to 25 participants. The majority of participants were aged between 18 to 22 years old with several mature age students aged between 30 to 45 years old in each group. There was an approximate 60/40 mix of domestic and international students in each of the focus groups. The majority of international students came from China and Singapore. The authors acknowledge from the outset that the way in which trust is understood is affected by demographics related to age, race, and gender [42]. The focus groups however, are the first exploratory stage in a number of stages in the larger research project on location-based services. By no means is this project meant to

generalize findings across ages, race and gender, or other demographic units of analysis.

Two moderators were used to conduct the focus groups. In order to maintain consistency between moderators and encourage a balanced approach to the focus group discussion a *Question and Stimulus Pack* was created. The questions and stimulus material enabled the focus group to be structured into three sections of enquiry as shown in figure 2. It should be noted that outcomes from sections 1 have been published [24].

After describing the various features of a typical location-based social networking application using Google Latitude as an exemplar (Figure 3), participants were presented with five relationship contexts. For each context a number of trust-related scenarios were presented. Participants were asked to place themselves in the role of the trustee as they considered the impact of LBSN usage on trust in the following contexts:

- *family*: parent-child, partner-partner, sibling-sibling
- *friends*: close friend-close friend, acquaintance-acquaintance
- *work*: employer-employee, co-worker-co-worker
- *commercial*: business-consumer
- *government*: agency-citizen.

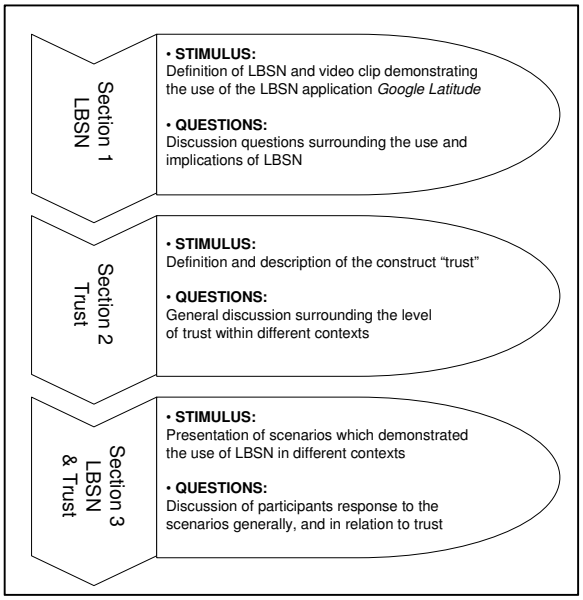

Figure 2. Focus group sections

A. *Limitations*

This research design had several limitations. First, a convenience sample of university students studying towards a degree in the Faculty of Informatics was used for the focus groups. In most cases the students were considering their own position in the contexts presented to them, primarily as a trustee in a given relationship, and not the trustor. Older, mature aged students in the focus group were able to switch between the roles of trustor and trustee quite easily and had the ability to intimately understand questions pertaining to the parent-child context or employer-employee context. Drawing students from a variety of disciplines, who had not previously had prior knowledge of LBSN applications, may have acted to amplify responses in the extreme positive or extreme negative.

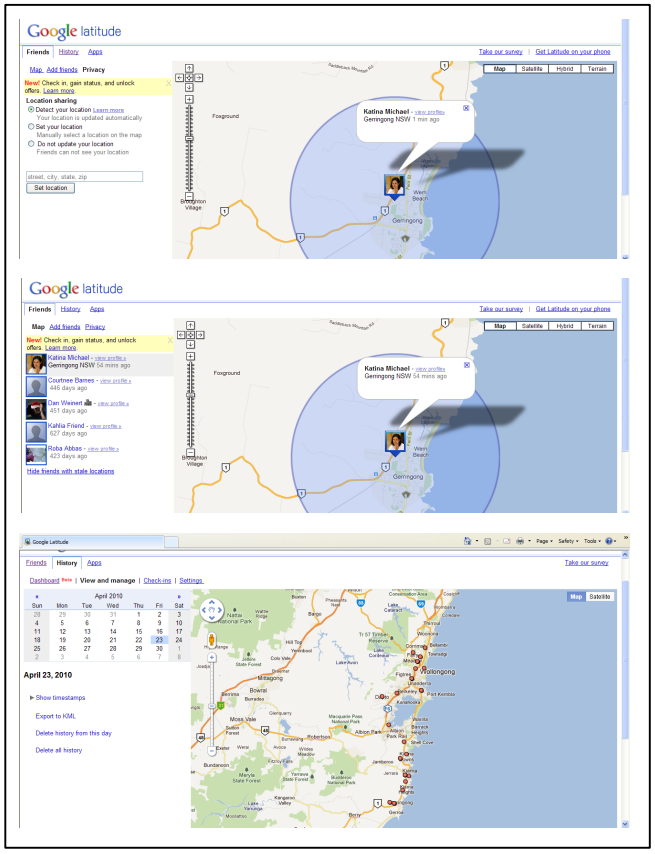

Figure 3. A Slide from the Question and Stimulus Pack: Privacy Setting Options in Reporting Location, Pinpointing a User and Sharing Location Data with Friends, and Location Histories in *Google Latitude*

Some of the respondents from various cultural backgrounds might also see different benefits and costs to the use of LBSN. What might act to increase trust in one culture, such as a repeat look-up of a "friend" on a given LBSN, might not be perceived as a caring gesture in another culture but rather one of spying or even stalking. Finally, running the same study again in 2011/2012 would render results more aligned to actual usage experiences rather than perception-based and predicted responses. It should be underscored however, that there were a small number of participants who had previously used LBSN applications, so some comments were being made from experience.

VI. CONTEXT AND ISSUES

Participants were asked to rate the level of trust they had in five different relational contexts: Family, Friends, Co-workers, Government and Commercial. This taxonomy was heavily influenced by the Ryerson University study into online social networks [43]. The "Stranger" category, in effect the ability to publicly share your location data with anyone from anywhere was omitted as a separate category but responses given by participants also informed beliefs and practices with respect to this context.

Figure 4 diagrammatically represents participant views, and was generated using focus group discussions, as opposed to statistically. As such, the diagram provides an indication of levels of trust in different relational contexts relative to one another. For example, participants generally trusted family and friends with their real-time physical location accessed via a LBSN application but were less inclined to share this kind of data with government or commercial entities. To some extent this had to do with the perception that location data could be somehow manipulated by government and commerce, and that sharing data with these entities meant sharing data with multiple "strangers" (i.e. government/company employees).

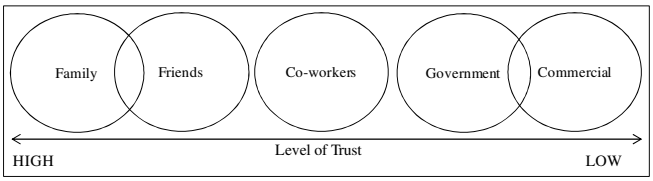

Figure 4. The level of trust users have of various social networks.

A. *Family*

In the context of "family", the parent-child and sibling relationships were explored using scenarios in the focus group. The participants identified four issues that emerged from the parent-child scenario. Firstly, that there is a balance to be found between the competing issues of trusting children and providing safety and care. Secondly, that LBSN may act as a barrier to building trust between parent and child. Thirdly, that the age of the child being tracked changes the appropriateness of tracking, and finally, that there may be legal issues related to tracking children (i.e., minors) using emerging technologies in a covert manner.

Participants identified that there is a need to trust children, while at the same time acknowledging that parents would also use LBSN for safety and care. When asked about the usefulness of LBSN to locate children in an emergency, participants almost unanimously agreed with the need. One participant said: "[y]ou would use it to monitor your children either for the reason that you want to keep them safe or you just do not trust them." Another participant reflected: "[i]t would be weird for parents not to care about their children's whereabouts so sometimes it is understandable for them to know the exact location. But it varies." Safety and trust however were separate matters in the eyes of some participants- the parental responsibility is to keep children safe from harm, whether a child accepts to use LBSN for this application or not, it should not have an impact on trust. But if "safety" was a surrogate for "us[ing] it for tracking as well" then trust could certainly be impacted.

Participants also saw that although motives of safety and care may drive the use of LBSN, the child can perceive this as a lack of trust. One participant noted that her parents were leaving the country and that if they had access to LBSN they would use it to "check [up on her] all the time… constantly, it would always be on." The participant described the resultant effect this kind of technology would have on her relationship with her parents saying that it would probably be at the centre of big arguments and definitely signal a loss of trust. She verbalized what she would say to her parents: 'do you not trust me to be myself on my own without you guys watching me all the time'. These sentiments were echoed by several other participants.

A contrary voice to this common opinion was that LBSN was actually useful between parent and child: "…sometimes I forget to tell my parents I am not going to be home, and then they call me and go 'Where are you we have got dinner for you?' | 'Oh I guess I forgot to tell you or you forgot that I was actually here.' To this another participant interjected and pointed: "[t]here would also be times where you would not want them to know where you are. Might not happen that often but there are always those occasions, and it would become annoying when they do." In this instance, the use of LBSN was not specifically for care, but for convenience. It however illustrates that some users have no problems revealing their location, but at the same time as noted by the participant above, at the outset you may not have any concerns showing your location but there are always exceptions to the rule.

The focus group participants also proposed that using LBSN over time would impact upon the ability of parents and children to develop trust.

> "See I do not think it is appropriate to be tagging your children. That is what you are basically doing- you are strapping them down and putting a GPS locator on their leg. Now having that from the time that they are little, they are going to associate that that is the normal thing and so they are going to grow up and do that to their kids, that is going to remove such a big element of trust for children… I do not think you could build up trust on a person like that. If I have constantly got their location, I am not going to need to trust them. Oh they are at home, or she is at home too or she is going out the door... This just removes all the trust. And basically there is no point in doing that at all. Because trust is everything in a family you have got to trust family members to look after themselves and the family by their actions. If you are not going to be able to trust your family then who can you trust?"

The importance of learning to trust without technology know-how was pointed out by another participant: "[a]nd how is the kid supposed to gain any trust when the family is

tracking them all the time?" Further to inhibiting the building of trust, one participant said that tracking children could be an exertion of force or control over the child and that the child "can never be herself/himself": "[i]f a child grows up knowing that he has been constantly tracked… [then] he has been forced to do what his parents want him to do, he can never be himself."

The participants commonly mentioned the age of the child as a factor which would influence whether the use of LBSN was appropriate or justified. It "[d]epends on the age and the scenario. At this age (34), I really do not care. At 16 when you are sneaking off to parties and stuff like that, and if they could see you then I guess that breaks the trust." The participant failed to recognize that young adults are breaking their parents' trust simply by "sneaking" or secretly engaging in activities that are not permitted, which could further justify parents' use of LBSN applications. When prompted by the moderator whether LBSN would be appropriate between parent and child when the child began secondary school the response was definitive by one participant who exclaimed: "[d]efinitely not". When asked by the moderator at what age it would be appropriate, another respondent considered that it would be on a case by case basis "…like once the child ha[d] proven they were responsible enough…" Other than a specific age or age group other participants specified a level of maturity: "I think it is not the number, because once parents acknowledge that you are able to make certain decisions, and they feel that your maturity levels are going up to take care of yourself, at that stage maybe you would be old enough to take care of yourself." Another participant likened it to recommended viewing ages on television- "they are only recommendations so it varies from person to person. You could have a really mature ten year old and you could have a very immature eighteen year old."

Other comments made during the focus groups about age being a factor in using LBSN within the family context demonstrated that age did not come into play for varying reasons. Some participants said that age was an irrelevant factor when considering when to use and not to use LBSN in a family context. Mostly participants claimed that it was what you were doing at a given moment, not your age that was important when using LBSN within a parent-child relationship. Others suggested that at "any age" you should respect your child: "I think you have to allow the child to have some sort of trust, if there is no trust at a younger age they will just play up more. You have got to respect children at any age."

A final issue that was mentioned was that if parents attempted to track their children without their consent, "[a]side from breaking trust, would not they be breaking some laws?" The legal side of covertly using LBSN applications to track family members or other people needs to be further explored both in the Australian context and in other jurisdictions. In response to being tracked by siblings participants were generally more at ease with siblings having access to their location. Some issues which were raised by the participants were that it could constitute a form of control by one sibling over another if a given piece of location information was provided without permission to a parent(s) by one sibling against another. Participants suggested that for siblings to use LBSN there would need to be "ground rules" so that it could be effective. And that you could even "play up with" your siblings using LBSN, especially for pranks. In terms of control, one participant concluded: "No I would not use it… the more you try and control things, the less you trust [someone]."

B. Friends

In the context of friends the participants brought out issues of acceptance of LBSN, lack of interest in using LBSN with friends, misconstruing stalkers as friends, and whether using LBSN promotes social or antisocial behavior. What is meant by acceptance of LBSN is the concern that people will simply allow (and not disable) the functionality of LBS on their online social networking application. As one participant stated: "[it] depends how it is used. Certain people are happy to add everyone [to their friends list]. If that becomes the norm then everyone will just accept it but I suppose I am older and you question things differently. It is all new to you, you have not had these experiences previously whereas everyone else is accustomed to it, it has always been there." The ease of which people accept LBSN and add everyone to their "friends list" may be risky. However one participant did not perceive this as a risk- "half the acquaintances that I have on Facebook would not give an iota about where I am. They might have a glance but they are not going to do the whole Facebook stalking thing and look in close detail." This comment sparked a debate in the focus group. In response, another participant brought up the dilemma that you do not know the intention of your acquaintances or friends, and could misconstrue a stalker as a friend. "You might think they are acquaintances but they might think, you know, maybe there is a stranger who might think you are their girlfriend."

The participants also discussed whether LBSN would cause social or anti social behavior.

> Participant A: It's a bit anti-social... People who want to know where you are should just ask you. It is a far more social thing to do. Saying: "Oh, I wonder where so-and-so is and he does not even talk to you." What is the point of having a friendship with a person if you do not really talk to them?
>
> Moderator: I guess just knowing a bit more information about them…
>
> Participant B: Yes but you can ask them and then you can spark up a conversation on things: "Where are you? | Oh I am here. | Oh what are you doing there?" As opposed to a shortened dialogue that might go something like: "Hey, where is so and so? | Oh, he is just there."
>
> Participant C: I would let people [use LBSN with me] for sure. They would be like, "what is the weather like down there?" You can say that it kind of kills conversation, but I think it may invoke a conversation if you go online and you

see: "Oh, they are some place unusual- I was not expecting to find them in Cairo– what are you doing there?"

This discussion highlights that depending on how LBSN may be used between friends and the personality and character of specific friends, in some cases LBSN might encourage social behavior but in other cases it may deepen anti-social behavior.

When participants were asked about how they might use LBSN with close friends, most participants felt very comfortable with disclosing location information with loved ones who were not official family. After all, as one participant pointed out, if close friends are really close, then "presumably… you are going to have a general gist of why they are there anyway and they are not going to mind you knowing and your are not going to mind them knowing exactly where you are." But participants also believed that the use of LBSN was unnecessary between close friends unless they were traveling together and there was an obvious need, "and you wanted to see where they were at that point in time" relative to your own location.

C. Work

When participants were presented with the scenario of employers monitoring employees they brought up two issues. Firstly, it would depend upon the job, and secondly, that there is a different type of trust relationship between employee and employer. In relation to the first issue participants saw that if the job was something where employees were mobile, like truck driving, real estate agents or pizza drivers, then the use of LBSN would be justified, however not for an office job where the use of LBSN would be a form of micro-monitoring within a closed office building space. As one participant noted: "[i]f you are sitting at a terminal, then I do not think Google Latitude is going to help." Furthermore, participants believed that the type of job one was engaged in could influence the justifiability of using LBSN in certain situations. For example, "[i]f you are working at Accenture then no, but if you are working on a secret military project then yes, they should track you because it is quite sensitive".

Participants also commented that there is a different type of trust between the employer-employee relationships than in parent-child or friend-friend relationships.

> Participant A: It has more to do with respect than trust.
>
> Participant B: I tend to disagree… I trust my employer to give me a safe environment to work in but that trust does not go this far…
>
> Participant C: But at the same time he is monitoring you, so that is not really trust.
>
> Participants suggested that if employers are paying for your time they have a "right to know that you are doing what [they] are paying you to do."

According to some participants during work hours, the employer was entitled to check where his/her staff was and what activity they were engaged in. It was only when the employer decided to continue the location look-ups, outside work hours, that they did not concur with this kind of application. One participant commented, "[s]o long as I am on the clock then it is okay, so long as I am being paid for it then they can track whatever I am doing but once I log off then it is turned off."

D. Commercial and Government

Participants were unlikely to trust commercial companies or Government with their location information, although some participants stipulated that they would certainly trust Government in emergency situations. In terms of commercial companies, participants identified that "as long as there [was] an opt in and an opt out [functionality] then [it was] okay." Another participant plainly stated that they did not trust commercial and/or government entities with their location information. "I would be paranoid [if I had to provide them with my location details]… The only real people it would affect [in terms of trust] is an emotional relationship, where I say I want to track you and they say no."

E. General

Emerging from participant responses was the general attitude that LBSN is or would be compulsory, and as such responses did not sufficiently cover the opt-in nature of many of the applications, further illustrating the lack of awareness of participants in regards to LBSN applications. With this in mind, participants commented that to some degree LBSN would by default encourage users to do the right thing. "I think it would be interesting though, if someone says they cannot get to a meeting you could see where they are and why they cannot get there." But to other participants, this only contributed to emotional distrust. One participant commented that it was only human to make mistakes and that like everyone else on occasion you too would be late by a few minutes to a meeting. Constantly checking to see if someone will be on time will just continue to diminish trust. More generally, participants reflected on the validity of the LBSN application they were presented with. The participants felt that while LBSN could provide pinpoint accuracy, that knowing where someone was did not provide the complete picture about the condition of a loved one: "[t]here could still be something wrong with them [i.e the child could still be in danger] even if you know where they are." One may increasingly develop a false sense of security just because they think they know where someone is on a digital map. The outcomes of this discussion which was based on trust and several scenarios using the LBSN taxonomy are summarized in Table I.

TABLE I. THE OUTCOMES OF THE DISCUSSION BASED ON TRUST AND SEVERAL SCENARIOS

Context	Issues
Parent and Child	• Balance between trust, safety and care • Barrier to building trust • Age of child • Legal issues

Siblings	• Control • Rules for effective use • Play games/ pranks
Friends	• Acceptance of LBSN • Lack of interest • 'Friends' as stalkers • Antisocial or social?
Close Friends	• Useful for traveling • Too busy to care • Unconcerned about sharing location
Work	• Type of job • Different type of trust
Commercial and Government	• No trust in either • Some trust in Government (emergency) • Ability to opt in or opt out
General	• General observations on use of LBSN

VII. The Impact of LBSN on Trust

The largest class of responses indicated that the impact of LBSN upon trust would be negative. Representative responses demonstrating this were plentiful. One participant noted: "[y]es, I can see how this technology can actually create mistrust amongst friends and family especially in cases where you might have an acquaintance which thinks they trust you a lot but you do not trust them as much… and when you reject their invite on Google Latitude it will create social problems." Another participant questioned: "[w]hy are you following me on Google Latitude?... Why do you not just believe where I am?"

With respect to trust, one participant was categorical in her claim that more or less LBSN discouraged trust by its mere functionality: "[a]s you no longer have to trust that the person is telling you where they are… because you can just go on [Latitude] and check, and you do not have to trust them." In the family context, trust could be eroded if family members relied upon LBSN for location data of a child, sibling or partner. One participant felt that LBSN allowed for almost constant monitoring of one's location. They said: "Well it is like… if you trust me, you should not need this location based service to prove where I am. You should perhaps trust that person." These responses identify that LBSN could cause "mistrust", exacerbate situations of disproportionate trust, "discourage" by removing the need or incentive to trust and that LBSN would ultimately erode trust.

Additionally while it was perceived by participants that LBSN could have a negative impact on trust, the participants did not identify that LBSN could have a positive impact upon trust. The logic given by most participants was that in order to strike an agreement whereby two people share their location data, they first have to have established trust in their relationship. "You do not get any bonuses for saying 'I'm going to do this' and then do it. That does not increase [trust]." And another participant warned: "[y]ou would have to establish trust with someone before you start using it [LBSN]. You do not know someone then give them your location at all times to build trust. You have got to have trust. So really this is only going to damage trust not build trust". This is an important point as it indicates that those who use LBSN should have a pre-existing element of trust in the individual(s) they share their location data with. This does not however preclude public LBSNs from broadcasting your location to everyone else in that social network.

Other participants indicated that the impact of LBSN upon trust would be dependant upon other factors including the stability of the relationship and the ethnicity of the users: "I think the more stable the relationship, the more understanding they would be if you go 'off the grid' for a while." It was also noted that ethnicity would be integral in how LBSN was used. "In ethnic families, gossip will just run. They would check it [*Latitude*], and if you are not there they will just talk behind your back, and ask why was she not there? Or why was he not there? Why were they somewhere else? It would just rule the world, it will rule everything." Both of these comments reflect the idea that the type of user (ethnicity) and the type of context or relationship (stability) LBSN is used within, will influence the way that the technology is applied, and this in turn will cause different resulting effects upon trust within relationships.

The participant who described "living off the grid" provided further commentary regarding a scenario depicted by another participant whereby a boyfriend would lie about his location to his girlfriend. This participant commented that "in that situation you could not tell a lie saying 'I am stuck in traffic' because in actual fact you are at the Pub." However, the participant fails to realize that in most LBSNs one is able to obfuscate their real time physical address location, or they can simply provide fuzzy details of their location to the nearest city. The underlying personal relationships within a LBSN context will impact upon what information is disclosed or not disclosed, whether the user uses white lies or reveals the truth. Furthermore, illustrative of the impact on ethnicity of the user can also impact the way that they use the device, with some individuals or families thriving on "gossip" and therefore using LBSN applications to feed their appetite. This increased vigilance and "talking behind your back" and perpetuating "gossip" will have a detrimental impact upon the trust in those relationships. However other families of different ethnicity may not have the desire to use LBSN for that purpose. There is also an inherent danger in continually altering your real time physical address location as it may raise undue suspicion as to your whereabouts. 'Friends' might be confused by the fact that their friends may mostly provide pinpoint visibility 24x7 but at times revert to other defaults such as "nearest city" or "manual" override mode where one provides a static physical address location, or even decides to "hide" their location altogether.

Something that was deemed vital by one of the participants was whether LBSNs like Google Latitude allowed you to know who was doing a location lookup on you. For the participant it was paramount that the service provider informed you when someone in your social network was "viewing your location". Similar feedback was also collected by Tsai, Kelley et al. as a feature which made users more comfortable using the LBSN Locyoution [44]. Despite having some control via privacy settings in the given LBSN and also the ability to manually set one's location and even

obfuscate one's location, some participants still found it unnerving that by default functionality tracking others was possible.

TABLE II. LBSN ISSUES

Entity	Description	Variables (•) and Issues (-)
Individual	The individual who is viewing the "friends" locations and disclosing their location.	• What they disclose? • Who they disclose to? • How they respond (e.g. drawing inferences, gossiping or uninterested)? - Privacy of the individual - Security of the individual
LBSN	The technology that provides location based social networking to the individual.	• Features of the technology (e.g. feedback and privacy controls) • Accuracy - Battery life - Security of the device - Resultant impact upon other layers in terms of trust, security and privacy.
Service Provider	The provider of the LBSN service including the servers, which store the information.	• Service provider policies • Government intervention • Commercial intervention - Privacy of information - Security of information
Relation-ship	The relationship that the device is used within.	• Type of relationship • Reciprocity of relationship • Level of trust in the relationship - Trust - Control - Anti-social/Social
Viewing Location	The receipt of location information.	• Accuracy • Constancy (real-time) • Errors in delivery - Resultant impact upon other layers in terms of trust, security and privacy
Disclosing Location	The transmission of location information.	• Accuracy • Constancy (real-time) • Errors in delivery - Resultant impact upon other layers in terms of trust, security and privacy

The following dialogue shows how LBSN can imbue feelings of power, control, and manipulation.

> Participant A: Knowing where they are is some kind of control, it is not definite.
>
> Participant B: The thing is you control people because if you guys knew where I was all the time I would act differently because I knew you guys would be watching me.
>
> Participant C: It would be an implicit sort of control.
>
> Participant B: Yes, you would be thinking I have got to act this out because I know people are watching.
>
> Participant D: Like guilt- emotional manipulation.

This is a fundamental problem that has its basis in trust but has far-reaching implications for how people might act differently if they thought someone they knew was watching them. For a list of issues which need to be addressed by LBSN entities, see Table II.

VIII. DISCUSSION

The outcome of this research was in identifying issues that need to be addressed by LBSN-related entities. The key variables and issues at play at each level, enable us to form an understanding of the circumstances in which LBSN will have an impact upon trust in relationships. Furthermore, the outcomes can be applied to various entities, notably:

- the research community to further their understanding of LBSN and trust-related issues;
- LBSN service providers to aid in the development of applications that provide adequate levels of privacy and security, and that do not conflict with user concerns; and
- users, individuals and society at large to ensure that they are informed about the privacy, security and other risks associated with the use of LBSN applications.

Therefore, the primary outcome of this research is not that LBSN reduces trust between "friends" or creates distrust in relationships. Rather, it is the knowledge that LBSN can negatively impact upon trust and that in particular circumstances this is likely to occur. These circumstances depend upon the context in which the technology is used, the pre-existing level of trust between users, the predisposition of the user, the accuracy and reliability of the location service and the features of the technology and how they are used.

IX. CONCLUSION

Location-based features are now widely available in popular online social networks. More recently Facebook also launched Nearby, although Google Latitude has been available since early 2009. Today there are well over one hundred location-based social networking applications available, some of these even tailored to specific contexts such as child safety, travel, dating, employment/user qualifications, sexual orientation etc. The results of the focus groups indicated that participants believe that LBSN will have major impacts on trust between people in a variety of relationships.

For some people LBSN will have unintended consequences that will be disruptive to their relationships. The negative impacts of LBSN on privacy, security, control and trust were also emphasized by participants as being

important concerns, especially for users who did not fully understand what they were revealing about themselves via the use of LBSN. Some participants believed that LBSN could act to strengthen relationships because providing one's real-time location to a friend would act to reaffirm aspects of trust. It remains to be seen however, how negative impacts of LBSN may be resolved by service providers and by individuals who agree to share their location data, only to realize how this data may be misused later.

One of the contributions of this research has been the need to reevaluate the default feature set that most LBSNs come endowed with, and ensure that there are new, more improved mechanisms which allow users to be actively aware of how often someone is doing a look-up on them. From this data there seems to be a subtle but strong link between "trust" and "monitoring" (i.e. in the context of surveillance)- *if you trust me then why the need to do look-ups on my real-time physical whereabouts? You should just believe me when I tell you where I am, where I have been and where I am about to go…*

ACKNOWLEDGMENT

The authors would like to thank Dr M.G. Michael for his contribution to this paper, and guidance throughout the whole study.

REFERENCES

[1] R. Kling, "What is social informatics and why does it matter?," The Information Society, vol. 23, pp. 205-220, 2007.

[2]R. Kraut, S. Kiesler, B. Boneva, J. Cummings, V. Helgeson and A. Crawford, "Internet paradox revisited," Journal of Social Issues, vol. 58, pp. 49-74, 2002.

[3] B. Misztal, Trust in Modern Societies - The Serach for the bases of Social Order. Cambridge: Blackwell Publishers, 1998.

[4] S.P. Marsh, Formalising trust as a computational concept. PhD thesis, Department of Mathematics and Computer Science, University of Stirling, 1994.

[5] A. Jøsang, "The right type of trust for distributed systems," Proceedings of the 1996 New Security Paradigms Workshop (NSPW), ACM, 1996.

[6] S. Brainov and T. Sandholm, "Contracting with uncertain level of trust," In Proceedings of the first ACM Conference on Electronic Commerce, Denver, pp.15-21, 1999.

[7] P. Resnick, R. Zeckhauser, E. Friedman and Ko. Kuwabara, "Reputation systems," Communications of the ACM, vol. 43, no. 12, pp. 45-48, 2000.

[8] C. Castelfranchi and Falcone, "Social trust: a cognitive approach," in C. Castelfranchi and Yao-Hua Tan (Eds), Trust and Deception in Virtual Societies, Kluwer Academic Publishers, pp. 55-90, 2001.

[9] C. Castelfranchi, R. Falcone, F. Marzo, "Being trusted in a social network: trust as relational capital," Lecture Notes in Computer Science, 3986, pp. 19-32, 2006.

[10] C. Snijders and G. Keren, "Do you trust? Whom do you trust? When do you trust?" In S.R. Thye, E.J. Lawler, M.W. Macy and H.A. Walker (Eds.), Advances in Group Processes, vol. 18, Amsterdam: JAI, Elsevier Science, pp. 129-160, 2001.

[11] P. Slovic, "Perceived risk, trust, and democracy", Risk Analysis, vol. 13, pp. 675-682, 1993.

[12] P. Dasgupta, "Trust as a commodity", in D. Gambetta, (Ed.) Trust: Making and Breaking Cooperative Relations, Department of Sociology, University of Oxford, pp. 49-72, 2000.

[13] E.H. Erikson, Identity: Youth and Crisis, W. W. Norton, 1968.

[14] J. Coleman, Foundations of Social Theory. The Belknap Press of Harvard University Press, 1990.

[15] D.H. McKnight, N.L. Chervany, "Trust and distrust definitions: One bite at a time". In R. Falcone, M. Singh, Y.H. Tan, (Eds), Trust in Cyber-Societies: Integrating the Human and Artificial Perspectives, Berlin: Springer, 2001.

[16] J. Golbeck and U. Kuter, "The ripple effect: change in trust and its impact over a social network," in Computing with Social Trust, pp. 169-181, 2009.

[17] C. James and L. Ling, "Social trust: tamper-resilient trust establishment in online communities," presented at Proceedings of the 8th ACM/IEEE-CS joint conference on Digital libraries, Pittsburgh PA, 2008.

[18] H. Nissenbaum, "Securing trust online: wisdom or oxymoron?" Virtual Publics: Policy and Community in an Electronic Age, ed. B. E. Kolko, Columbia University Press, New York, 2003.

[19] R. C. Solomon and F. Flores, Building Trust: In Business, Politics, Relationships, and Life, Oxford University Press, New York, 2001.

[20] R. Gross and A. Acquisti, "Information Revelation and Privacy in Online Social Networks " presented at Workshop on Privacy in Electronic Society, Virginia, USA, 2005.

[21] C. Dwyer, S. Hiltz, and Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," presented at Proceedings of the Thirteenth Americas Conference on Information Systems (AMCIS), 2007

[22] S. Gambi and W. Reader, "The development of trust in close friendships formed within social network sites," presented at Proceedings of the WebSci'09: Society On-Line, Athens, Greece, 2009.

[23] S.J. Fusco, K. Michael, and M.G. Michael, "Using a social informatics framework to study the effects of location-based social networking on relationships between people: A review of literature," IEEE Symposium on Technology and Society, 7-9 June, Wollongong, Australia, pp. 158-171, 2010.

[24] S.J. Fusco, K. Michael, M.G. Michael and R. Abbas, "Exploring the social implications of location based social networking: An inquiry into the perceived positive and negative impacts of using LBSN between friends," 9th IEEE International Conference on Mobile Business, June 13-15, Athens, Greece, IEEE, pp. 230-237, 2010.

[25] D. Rousseau and S. Sitkin, "Not so different after all: A cross-discipline view of trust," Academy of Management Review, vol. 22, pp. 393-404, 1998.

[26] R. C. Mayer and J. H. Davis and D. Schoorman, "An integrative model of organizational trust," Academy of Management Review, vol. 20, pp. 709-734, 1995.

[27] J. D. Lewis and A. Weigert, "Trust as a social reality," Social Forces, vol. 63, pp. 967-985, 1985.

[28] L. Barkhuus, "Privacy in Location-Based Services, Concern vs. Coolness," HCI 2004 workshop: Location System Privacy and Control. Glasgow, UK, 2004

[29] S. Patil and J. Lai, "Who gets to know what when: configuring privacy permissions in an awareness application," Proceedings of the SIGCHI conference on Human factors in computing systems. Portland, Oregon, USA, ACM, 2005.

[30] J. Tsai, P.G. Kelley, L.F. Cranor and N. Sadeh, "Location-sharing technologies: Privacy risks and controls," I/S: A Journal of Law and Policy for the Information Society 6(2):119-151, 2010.

[31] D. Anthony, D. Kotz, and T. Henderson, "Privacy in location-aware computing environments," IEEE Pervasive Computing, 6(4):64-72, 2007.

[32] K.P. Tang, J. Lin, J.I. Hong, D.P. Siewiorek and N. Sadeh, "Rethinking Location Sharing: Exploring the Implications of Social-Driven vs. Purpose-Driven Location Sharing," 12th ACM International Conference on Ubiquitous Computing (Ubicomp 2010), Copenhagen, Denmark, Sep 26-29, 85-94, 2010.

[33] S. Consolovo, I. Smith, T. Matthews, A. LaMarca, J. Tabert and P. Powledge, "Location disclosure to social relations: why, when & what people want to share," Proceedings of the SIGCHI conference on Human factors in computing systems. Portland, Oregon, USA, ACM, 2005.

[34] J. Boesen, J.A. Rode and C. Mancini, "The domestic panopticon: location tracking in families," In Proceedings of the 12th ACM international conference on Ubiquitous computing (Ubicomp '10). ACM, New York, NY, USA, 65-74, 2010.

[35]B. Brown, A.S. Taylor, S. Izadi, A. Sellen, J.J. Kaye and R. Eardley, "Locating Family Values: A Field Trial of the Whereabouts Clock," UbiComp 2007: Ubiquitous Computing, 2007.

[36] L. Humphreys, "Mobile Social Networks and Social Practice: A Case Study of Dodgeball," Journal of Computer-Mediated Communication13(1): 341-360, 2008.

[37] L. Barkhuus, B. Brown, M. Bell, S. Sherwood, M. Hall and M. Chalmers, "From awareness to repartee: sharing location within social groups," Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems. Florence, Italy, ACM, 2008.

[38] S. Vihavainen, A. Oulasvirta and R. Sarvas, "'I can't lie anymore!': The implications of location automation for mobile social applications," Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous, 2009. MobiQuitous '09. 6th Annual International, 2009.

[39] D. Mackenzie, "Introductory essay," The Social Shaping of Technology, Philadelphia: Open University Press, pp. 2-27, 1999.

[40] D. Morgan, Focus Groups as Qualitative Research, California: Sage Publications, 1996.

[41] Gibbs, "Focus group research," Social Research Update, vol. 19, pp. 1-4, 1997.

[42] P. Slovic, "Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield," Risk Analysis, vol. 19, pp. 689–701, 1999.

[43] A. Levin and M. Foster, "The next digital divide: Online social network privacy," Ryerson University, Ted Rogers School of Management, Privacy and Cyber Crime Institute, 2008.

[44] J. Y. Tsai and P. Kelley, "Who's viewed you?: the impact of feedback in a mobile location-sharing application," presented at Proceedings of the 27th international conference on Human factors in computing systems, Boston, MA, 2009.