Sharing Location in Online Social Networks

Nan Li and Guanling Chen, University of Massachusetts Lowell

Abstract

Online social networks (OSNs) have become important media for information sharing among Internet users. In particular, several OSNs provide mechanisms to facilitate sharing of the users' location, which is gaining increased popularity due to the growth of GPS-equipped smartphones. These location-based OSNs (LSNs) bridge users' physical and social worlds, allowing users to know where their friends are and enabling location-based information access and user interactions. In this article we first introduce several LSNs and compare their location-sharing related features. A user's location, however, is sensitive and personal information that may raise significant privacy concerns. To understand real-world users' location-sharing behavior, we collected 21 months of data traces from a commercial LSN and analyzed its users' location-sharing updates. We found that the characteristics of the users' privacy protection behavior is correlated with their age, gender, mobility, and geographic region. In addition, friends tend to have similar privacy protection patterns. To the best of our knowledge, this article is the first large-scale empirical study of a modern LSN.

With the growth of the Internet and the continued advances of Web 2.0, communication behavior among Internet users has significantly changed. In addition to traditional information access, users have started socializing in cyberspace mediated through online social network (OSN) applications. Over the past several years, OSNs have become an important social phenomenon on the Internet. For example, Facebook has more than 400 million active users and more than 25 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month.[1]

Sharing and interacting around content is a primary OSN feature. Recently, several OSNs have provided explicit mechanisms to allow their users to share location information. These location-based OSNs (LSNs) enable users to see where their friends are, to generate or search location-tagged content within their social network, and to meet others nearby who may have the same interests. The increased availability of GPS-equipped smartphone platforms, such as Apple iPhones and Google Android phones, makes LSNs much more accessible to mobile users. A recent study shows that the social network sites are among the top mobile Web destinations [1], and it is expected that LSN services will attract 82 million subscribers and reach $3.3 billion revenues by 2013 [2].

On one hand, accessing LSNs from mobile phones provides greater spontaneity to facilitate serendipity for people to meet up. An one-year-long study of an early LSN, Dodgeball, shows that it can be used for a variety of purposes and may lead to social molecularization, influencing people's experiences and movement through a city in a collective manner [3]. On the other hand, such utility comes with dangerous security risks. For example, by analyzing the location shared by a user, whether she is at an airport or a supermarket, it is easy to know that the user is not at home; thus, she may be a potential target of burglary [4].

In this article we first provide an overview of several popular LSNs that leverage users' shared location information to bring new services to their social life. Our short survey focuses on comparing their location-sharing features and discussing how these LSNs deal with privacy issues. To understand how real-world users share their location in LSNs with serious privacy implications, we collected 21 months of data traces from Brightkite to analyze its users' location-sharing behaviors. The statistical results indicate that users of different ages, genders, mobility patterns, or regions show different online behaviors of sharing their location with the public. To the best of our knowledge, this is the first large-scale empirical study of location-sharing behaviors from a real-world LSN.

Location-based Online Social Networks

Dodgeball

Dodgeball is one of the first LSN services, founded in 2000 by Dennies Crowley and Alex Rainert. Google acquired Dodgeball in 2005 and shut down the service in 2009. Before Dodgeball was shut down, its service was available in 22 U.S. cities [3]. Dodgeball relied heavily on short message service (SMS) to allow users to "check in" at venues within cities, announcing where they were at the moment. Users texted their location to the service, which then notified them of their friends, friends of friends, and interesting venues nearby. By changing settings using the service's website, the users could receive SMS alerts when their friends or their friends of friends checked in within a 10-block radius. The check-ins were not collected and posted as public commentary on the website.

[1] *http://www.facebook.com/press/info.php?statistics*

0890-8044/10/$25.00 © 2010 IEEE

Instead, they were read as individual SMS messages and stored on the individual mobile devices. Therefore, it was up to each user to determine the message's persistence. Dodgeball did not use GPS or other embedded technology to track users' locations. Instead, users had to explicitly tell Dodgeball where they were by sending SMS messages to the service.

Brightkite

Brightkite is an LSN service operated by a Denver-based startup founded in 2005. Its primary service is letting users post and share updates with their friends or the public. User updates could be via a text note limited up to 140 characters, a photo, or a check-in (announcing a location). The typical usage scenario is that the user checks in when she comes to a new location. All note and photo updates are associated with the location of the user's latest check-in. Brightkite assumes that the user stays at the same location until she checks in somewhere else. There are three access levels for each update. The user can set her updates to be visible to everyone, to her friends only, or private (no sharing).

Brightkite provides a number of interfaces, including web, SMS, and email, to let users easily access the service. The 140-character limitation of the text notes is suitable for the SMS. Brightkite also has native applications on many smartphone platforms, which leverage GPS or other on-device technologies for automatic location sensing. Thus, a user can simply select a venue from a list of nearby places provided by Brightkite, which is much easier than having to manually type her current venue on the phone as Dodgeball requires.

Brightkite users can search updates that are visible near a particular location. For example, a user can search all photos posted nearby with keyword "bar." The users can also propagate their updates to external services such as Facebook, Twitter, and Flickr. This feature effectively extends the utility of Brightkite. For example, although Facebook has not provided a native location-sharing feature, a user can link her Brightkite check-ins to share with her Facebook friends. The user must, however, use Facebook's privacy control settings to determine who can see her location updates.

Loopt

Loopt is another mobile-based LSN that was founded in 2005 and currently only serves U.S. users. Loopt provides a map view of the user's current location and nearby friends, places, and events. Pins on the map represent users' check-in locations and can be associated with text notes or photos. Unlike Brightkite, a user's updates in Loopt can only be seen by her friends. On the other hand, Loopt does allow public sharing by providing HTML code for the user's journal page, which can be embedded in external websites such as Google Blogger and LiveJournal. The embedded journal page shows the user's location history and updates in an animation. The user can also propagate her updates to external services such as Facebook.

Loopt provides native applications on many smartphone platforms. Loopt has partnered with carriers to obtain users' locations; thus, its applications can work on phones without GPS. Unlike Dodgeball and Brightkite, by default Loopt does not require its users to explicitly check in. Instead, it continuously tracks users' locations either through the carrier or from the mobile application without user input. The limitation of this "tracking" approach, compared to Dodgeball and Brightkite, is that the location is an estimation, and the service typically cannot distinguish at which venue the user is.

Loopt automatically shares the user's location with her friends, or only some of her friends as specified by the user. A recent iPhone version, however, allows the user to disable live location tracking and only update current location by manually typing an address. Loopt also has a separate mobile dating-like application, "Loopt Mix," which allows the users to create public profiles and chat with other nearby users.

Foursquare

Foursquare is a relatively new LSN, founded in 2009 by previous Dodgeball founders. Using Foursquare is like playing a game. The users make check-ins at venues, and they are then awarded points and sometimes "badges." By making more check-ins, the user can earn badges like "Newbie," "Adventurer," "Explorer," or "Superstar." If a user has more check-in days at a venue than anyone else in the past 60 days, she becomes the "Mayor" of that venue. Foursquare has partnered with many bars, cafes, and restaurants to reward the Mayor with free drinks or other specials. The strategy of giving interesting badges and rewarding with specials encourages users to stick to the service and make frequent check-ins. Foursquare has grown rapidly recently, and has obtained more than 1.7 million total users and signs up about 100,000 new users per week.

By default, a user's location updates can only been seen by her friends. Similar to other LSNs, however, Foursquare users can link their location check-ins with Facebook and Twitter. For example, we saw more than 230,000 Foursquare users publish their location updates on Twitter, despite recent press on potential security risks of such public location leakage [4].

Gowalla

Gowalla is another game-like LSN that was launched in Austin, Texas, in 2009. Gowalla also adopts a check-in model to have its users announce their location. By checking in at a venue, the user may receive virtual items and earn points, which may also give the user stamps (similar to Foursquare badges). A Gowalla "trip" consists of a set of locations, and by checking in at all of them the user can complete the trip. This is often considered a useful feature for tourists.

Unlike many other LSNs, the Gowalla iPhone application does not have privacy settings, and it appears that the user can see her friends' location updates, the leaderboard of any location, and the check-in history of any location by all users. The location leaderboard contains the top users who checked in at that location. The user can also browse her friends' complete check-in history and carried virtual items. On the other hand, Gowalla's main website shows the complete check-in history of all its users to the public, which is often criticized by its users.

Google Latitude

In April 2009 Google launched its "Latitude" service that provides basic LSN functions tightly integrated with Google Map. Like Loopt, Latitude can automatically sense the user's location and share it with her friends, who can see her current location on the map. Latitude allows its users to disable live tracking and update location by manually typing an address, or hide their current location from all friends. Latitude users can also enable "history" feature so that their location updates can be analyzed to provide additional values. For example, the user can set up an email or SMS alert if her friends are nearby, but only when the user is at an unusual place, or at a routine place at an unusual time (e.g. to avoid unnecessary alerts from coworkers at the workplace). Although Latitude does not provide a way for its users to link their location updates with other popular OSNs such as Facebook, it does allow its users to embed a location page on their blog and website or to automatically show their location as Google Talk status.

	Location sensing					Location sharing			
	Check-in	Tracking	Venue	Verification	Granularity	Private	Friends only	All users	External
Dodgeball	[×]		×				×		
Brightkite	[×]		×		×	×	×	×	×
Loopt	×	[×]				×	[×]		×
Foursquare	[×]		×			×	[×]		×
Gowalla	[×]		×	×			[×]		×
Latitude	×	[×]				×	[×]		×

Table 1. *Feature comparison of LSNs (bracket indicates default option).*

Comparison of the LSNs

The above list of LSNs is not meant to be comprehensive. There are many other emerging location-based services and applications that integrate social networking features, such as SCVNGR, GyPSii, and MyTown. The LSNs we chose, however, cover a variety of location sensing and sharing features. Table 1 summarizes the comparison of these LSNs.

All six LSNs provide check-in modes so that users can manually input their current location, while by default Loopt and Latitude automatically track and share users' locations. All LSNs except earlier Dodgeball have mobile applications that can leverage on-device positioning on modern smartphones to sense the user's current location. Brightkite, Foursquare, and Gowalla can then prompt the user with a list of nearby venues to check in. With venue-based check-in, a user's location updates come with more context, such as whether she is at a restaurant or a post office. Tracking-based approaches such as Loopt and Latitude usually cannot automatically determine a user's current venue due to inaccurate location sensing (GPS does not work well in cities and indoors).

Most LSNs allow the users to check-in at an arbitrary location, even hundreds of miles away from their actual current location. One advantage of this flexibility is to allow the user to check-in at a remote location and see what is going on there. On the other hand, such "fake" check-in may confuse the user's friends and skew LSN service providers' user analytics, which can be used for recommendations and targeted advertisements. At this time, only Gowalla checks the user's actual location, using on-device location sensing, and only allows the user to check-in at a venue not far from the sensed location. Foursquare also checks the user's current location, but still allows her to check-in at a remote venue. It will, however, give fewer points for such check-ins. Currently only Brightkite allows its users to control check-in location granularity. Namely, the user can check-in using a city name, such as "Boston, MA," instead of a particular venue or address.

All LSNs provide some controls to the users on how to share their location. Dodgeball allows its users to receive check-in alerts from friends and friends-of-friends who are nearby. It is unclear whether the user can limit her check-ins to be known only to her friends, as the service is no longer available. Brightkite provides per-check-in control on who can see that check-in. If the user chooses to share the check-in with only friends, the next check-in will be defaulted to be seen by friends only as well. Only Brightkite allows the users to share their location with all other users in the network.

By default the other four LSNs only share the user's location with her friends, though the user can also choose private check-ins except Gowalla. Loopt also allows its users to share their location with only a subset of their friends. Gowalla allows the user to browse who checked-in at a location at what time, even if they are not friends. On Gowalla's main website, every user's complete check-in history is public, which is probably not what the user has intended for. All LSNs, except Dodgeball, allow their users to explicitly link their location updates with external services, such as Facebook, or public websites.

Location Privacy in LSNs

Sharing user information in OSNs naturally raises privacy concerns. Most OSNs ask users to give personal information in their profiles, which usually include age, gender, and email address. Some users choose to hide certain parts of the profile, such as their gender, or supply fake data, such as abnormally small or large values of their age [5]. These behaviors indicate the users' privacy concerns, as they do not want to expose real information to the public or to the OSN providers.

Although location sharing is the key to enable many interesting LSN features, its privacy implication is significant. As modern GPS-equipped smartphones may be able to detect accurate position up to the meter level, sharing location becomes even more problematic. For example, by analyzing a user's location history, we may figure out how many times she went to the hospital in the past year, thus being able to derive her health condition to some degree. If a user checks in regularly, we may easily infer her home location as near the place of the most frequent updates posted at night or on the weekend. Additionally, her home location may imply her annual income level. There are several recent studies analyzing both the privacy design and privacy leakage of emerging mobile social networks [6, 7].

As discussed above, most LSNs provide some controls to users to protect their location updates, such as by disabling live tracking and only checking in when the users want to. The users can also choose to hide their check-ins from the public or even from their friends. On the other hand, we do see many users publish their locations to the public, such as by linking their check-ins to Twitter, despite recent press on the potential risks of leaking current locations [4]. Similarly, Gowalla continues to grow despite the fact that all users' check-in histories are available on its website to the public and search engines. Thus, it is interesting to study the location-sharing behaviors in LSNs, which may help us better understand the social phenomena of LSNs as they grow.

	Male	Female	Unspecified
Proportion (%)	61.55	15.88	22.66
Average PoPU	0.1226	0.1502	0.1464

Table 2. *Females have more privacy concerns.*

Privacy Protection Behaviors

We are interested in empirically studying how users share their location updates with the public. Sharing location with the general public is quite different than sharing with the user's friends, and it comes with serious privacy risks. In particular, we studied Brightkite, which provides an application programming interface (API) so that we can collect enough data for analysis. Next we focus our discussion on the analytical results. Note that we do not claim these results to be generalizable to all LSNs, but they do provide some insights on how location is shared in reality.

Data Trace Collection

Brightkite provides a RESTful API for integrating with third-party applications. The interface is implemented using HTTP query, so an application sends a specified HTTP request and the website sends back an XML (or JSON) response. Using this API, we can collect all public updates and the users' profile information for analysis.

We collected the user updates posted between March 21, 2008 and December 15, 2009. There were 4,460,161 public updates posted by 74,722 users. Besides the updates, we also collected all those users' friends lists and their profile information, including age, gender, and so on.

Privacy Settings

In Brightkite the user can choose to share an update with the public, with her friends only, or with nobody (private mode). If an update is shared with friends only or not shared at all, neither the public updates stream on Brightkite nor our collected data trace show this update. On the other hand, each user's profile indicates how many updates have been made by that user in total, including updates not shared with the public. So by comparing the number of updates we collected (public updates) with the number of total updates indicated in the profile, we can calculate the proportion of protected updates (PoPU), which is in the range from 0 to 1. The larger PoPU value indicates that the user hides her updates more frequently from the public, thus indicating that she is more conscious of her location privacy.

PoPU over Different User Groups

In Brightkite there are 61.55 percent of users claiming to be male in their profile, 15.88 percent of to be female, and 22.66 percent of users chose to hide their gender information. We calculated the average PoPU over the different gender groups, and show the result in Table 2. Female users clearly have larger PoPU values, suggesting that they are more privacy conscious, which is consistent with other studies.

Figure 1 shows the average PoPU of the users over different ages. We assigned zero to the users who left the age value empty or filled the age with an abnormal value (less than 9 or larger than 99) in their profile. Surprisingly, there are 58.9 percent of users chose to hide or forge this information. It is clear that these users have more privacy concerns, and their average PoPU is larger than any other age group's. The PoPU of users who gave their age information steadily increases from teenaged to middle-aged users. The right-most point indicates the average PoPU of all users older than 50. Older

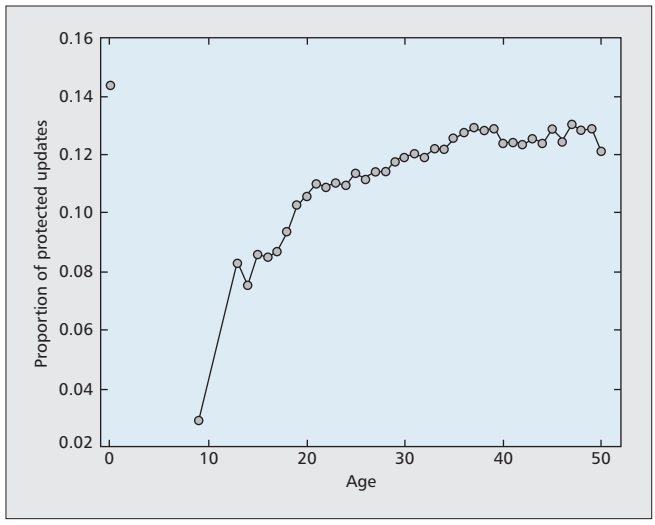

Figure 1. *Older users have more privacy concerns.*

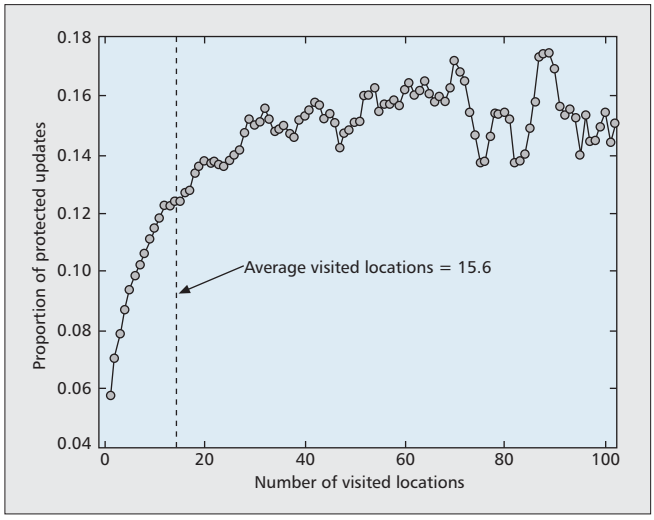

Figure 2. *Mobile users have more privacy concerns.*

users tend to have relatively stable families, friends, and social relations. It seems that they prefer to share updates with users they already know and hide their location updates from the public.

To identify mobile users in Brightkite, we count each user's unique check-in locations, which include her explicit check-in and associated locations with text notes or photo updates. The average number of unique locations over all users is 15.6. Figure 2 shows the average PoPU corresponding to user groups with different unique locations. The PoPU increases with the number of users' unique locations when the number of unique locations is less than the average value. As users become more mobile, meaning the number of unique locations is larger than average, they tend to have similarly high PoPU values.

Brightkite provides multiple interfaces to let users access its services. We categorized the users by their majority access method and also calculated the average PoPU of each user group. Figure 3 shows the statistical results, in which "sms" means that the update was sent through text messaging and "mobile" means that the update was sent from mobile devices other than iPhones, Androids, and BlackBerrys. We found that mobile device users, especially iPhone users, tend to share their updates with friends instead of with the public, as their average PoPU value is two times larger than that of web users.

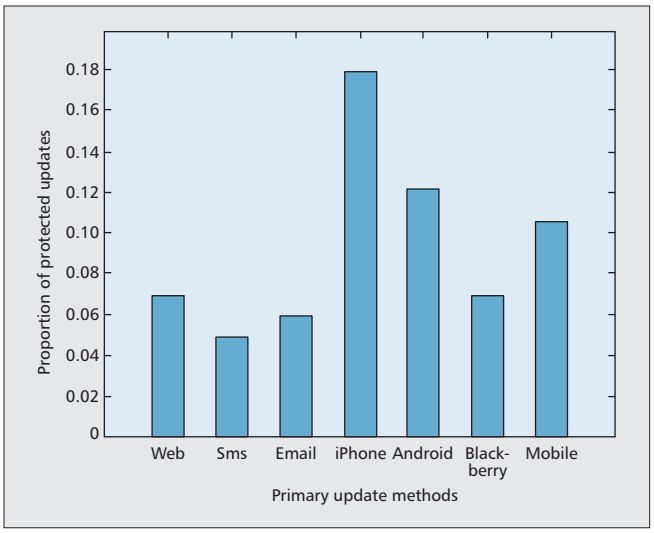

Figure 3. *Smartphone users have more privacy concerns.*

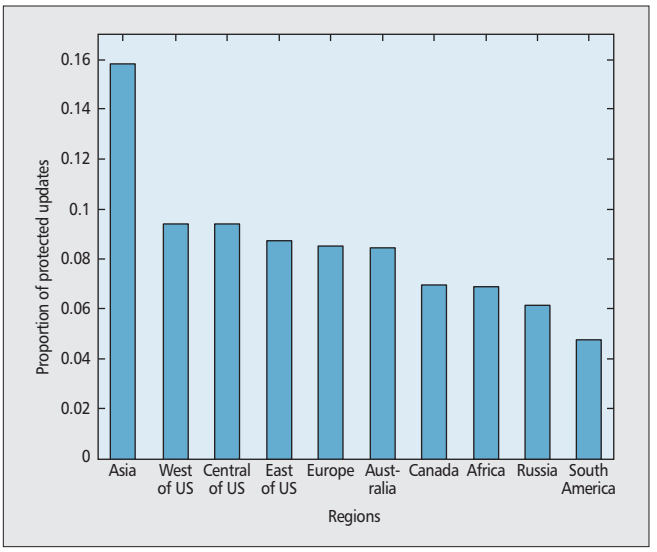

Figure 4. *Asian users have more privacy concerns.*

Users' privacy concerns not only depend on how they use the LSN, but also relate to users' geographical regions. We used the location information associated with users' updates and identified the users' geographic regions. We split the world into 10 regions, which could be areas, countries, or continents, and categorized users' updates by those regions. We split the United States into three regions using the three time zones. The region containing the most updates from a user is considered to be that user's home region. The 10 regions, in decreasing order of number of Brightkite users, are East United States, Central United States, Europe, Western United States, Asia, Australia, South America, Canada, Africa, and Russia. The top four regions contained 83.77 percent of the users. Figure 4 shows the average PoPU of user groups from different regions. Asian users (5.69 percent of total users) have the strongest privacy protection behaviors, as their average PoPU value is much larger than any other region.

Since one of the motivations for using LSNs is interacting with friends, we believe that users may have similar privacy concerns when sharing location. We calculated the average PoPU of each user's friends. Figure 5 shows the average PoPU of friends corresponding to user groups who have different PoPUs. It is clear that for those users who always use Brightkite in public mode (x equal to 0), the average PoPU of their friends is also very low. As the users' own PoPU increases, their friends' PoPUs increase as well. Even though the curve flattens in the range of x = 0.5–0.7, the overall tendency is increasing, and the highest value of friends' average PoPU corresponds to the users with the highest PoPU value.

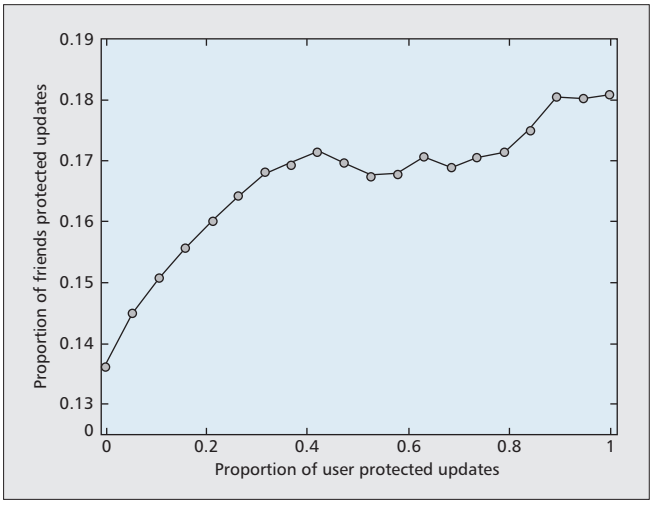

Figure 5. *Privacy concerns are similar with friendship.*

Related Work

Obtaining user location can enable many interesting ubiquitous computing applications, and the privacy trade-offs need to be carefully studied. Harper conducted an interview-based qualitative study to understand why early adopters want to wear location-tracking devices [8]. Barkhuus provided two case studies indicating that users' privacy concerns decrease when actually using location-based services [9]. Consolvo *et al.* studied which factors are most important for the user to be willing to disclose her location to a requesting social relation. Hsieh *et al.* designed and evaluated privacy mechanisms for an instant messaging application that allows users to share their location and other contextual information [10]. Sadeh *et al.* designed and evaluated a set of rich location-sharing policies used in a friend-finder mobile application [11]. Unlike previous studies focusing on research prototypes, Krishnamurthy and Wills studied privacy leakage in existing commercial mobile social networking applications [7]. Compared to existing work, our study has focused on how users share or hide their location check-ins with the general public using a large-scale data trace collected from a commercial LSN.

Conclusion

We provide an overview of several LSNs, which allow users to share their locations as a new interaction method that bridges physical and social worlds. The location sensing and sharing features of these LSNs are compared. In particular, we used trace-based analysis to study how real-world users share privacy-sensitive location information. We found that users' privacy concerns are correlated with their age, gender, mobility, and geographic regions. Friends tend to have similar privacy concerns and exhibit similar location-protection behaviors. We have also done extensive analysis and modeling of user classification and friendship modeling using this data trace, and the results can be found in [12, 13].

References

[1] "Social Networking and Craigslist Top Mobile Destinations," *Reporter Wireless and Mobile News*, Mar. 2009.
[2] *Location-Based Mobile Social Networking*, ABI research study, Nov. 2008.
[3] L. Humphreys, "Mobile Social Networks and Social Practice: A Case Study of Dodgeball," *J. Computer-Mediated Commun.*, vol. 13, no. 1, article 17, 2007.
[4] F. Lardinois, "PleaseRobMe and the Dangers of Location-Based Social Networks,"*ReadWriteWeb*, Feb. 2010.
[5] W. Gauvin *et al.*, "Measurement and Gender-Specific Analysis of User Publishing Characteristics on MySpace," *IEEE Network*, Special Issue on Online Social Networks, June 2010.
[6] G. Chen and F. Rahman, "Analyzing Privacy Designs of Mobile Social Networking Applications," *Proc. Int'l. Symp. Trust, Security and Privacy for Pervasive Applications*, Shanghai, China, Dec. 2008.
[7] B. Krishnamurthy and C. Wills, "Privacy Leakage in Mobile Online Social Networks," *Proc. 3rd Wksp. Online Social Networks*, Boston, MA, June 2010.
[8] R. Harper, "Why People Do and Don't Wear Active Badges: A Case Study," *Computer Supported Cooperative Work*, vol. 4, no. 4, Dec. 1995.
[9] L. Barkhuus, "Privacy in Location-Based Services, Concern vs. Coolness," *Proc. Wksp. Location System Privacy and Control*, Glasgow, U.K., 2004.
[10] G. Hsieh *et al.*, "Field Deployment of IMBuddy: A Study of Privacy Control and Feedback Mechanisms for Contextual IM," *Proc.UbiComp 2007*, Innsbruck, Austria.
[11] N. Sadeh *et al.*, "Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application," *Personal and Ubiquitous Computing*, vol. 13, no. 6, Aug. 2009.
[12] N. Li and G. Chen, "Analysis of a Location-Based Social Network," *Proc. Int'l. Symp.Social Intelligence and Networking*, Vancouver, Canada, Aug. 2009.
[13] N. Li and G. Chen, "Multi-Layer Friendship Modeling for Location-Based Mobile Social Networks," *Proc. Int'l. Conf.Mobile and Ubiquitous Systems: Computing, Networking and Services*, Toronto, Canada, July 2009.

Additional Reading

[1] S. Consolvo *et al.*, "Location Disclosure to Social Relations: Why, When, & What People Want to Share," *Proc. ACM CHI 2005*, Portland, OR.

Biographies

NAN LI (nli@cs.uml.edu) completed his Ph.D. in computer science at the University of Massachusetts Lowell in 2010. His research interests include social networks, mobile computing, and social applications. He received his M.Eng. in communication and information systems in 2004 and his B.S. in electronic and information science in 2001, both from Peking University. For more information see http://www.cs.uml.edu/~nli/.

GUANLING CHEN (glchen@cs.uml.edu) is an assistant professor of computer science at the University of Massachusetts Lowell. He is also affiliate faculty of the Institute for Security, Technology, and Society (ISTS) at Dartmouth College. His research interests include wireless networks, mobile computing, and social applications. He has published over 30 refereed journal and conference papers, and his work is supported by the National Science Foundation and the Department of Homeland Security. After receiving his B.S. in computer science from Nanjing University in 1997, he completed his Ph.D. in computer science from Dartmouth College in 2004. He was an I3P Fellow before he joined the faculty of the University of Massachusetts Lowell in 2005. For more information see http://www.cs.uml.edu/~glchen/.