Written Testimony of
Lorrie Faith Cranor
Associate Professor of Computer Science and of Engineering & Public Policy,
Carnegie Mellon University

United States House of Representatives, Energy and Commerce Committee
Subcommittee on Communications, Technology and the Internet, and
Subcommittee on Commerce, Trade, and Consumer Protection
Hearing on
The Collection and Use of Location Information for Commercial Purposes
February 24, 2010

Chairmen Boucher and Rush, Ranking Members Stearns and Radanovich, and members of the committees, I thank you for the opportunity to testify about privacy issues associated with the use of location information for commercial purposes.

My name is Lorrie Faith Cranor. I am an associate professor of computer science and of engineering & public policy at Carnegie Mellon University. I am also the director of the CyLab Usable Privacy and Security Laboratory at Carnegie Mellon. I am a member of USACM, the U.S. Public Policy Council of the leading professional society for computer scientists.

I have been conducting privacy research for over a decade. I have studied Internet users' privacy concerns, how they make decisions about privacy, and their use and comprehension of privacy policies.[1] Along with my colleagues and students, I have developed technologies and standard approaches for communicating about privacy online, including a search engine that provides information about website privacy policies[2] and a privacy "nutrition label."[3] I have also been involved in a Carnegie Mellon University project to develop a location-sharing service that allows

[1] http://cups.cs.cmu.edu/#privacy-decision

[2] http://privacyfinder.org/

[3] http://cups.cs.cmu.edu/privacyLabel/

users to control when, where, and with whom to share their location information.[4] We have used this system as a platform for our privacy research.[5]

I have been asked to testify about privacy issues associated with the use of location information for commercial purposes. I will first provide a brief overview of how location-based services work. Then I will discuss consumer perceptions of risks and benefits of location-sharing technology. Next, I will discuss privacy controls in location-sharing applications. Finally, I will discuss some of the policy implications of my research findings in this area. Much of my testimony here is based on a paper I co-authored last summer with Janice Tsai, Patrick Gage Kelley, and Norman Sadeh, which I have included as an appendix to my written testimony.[6]

Locating Technologies

Location-based services (LBS) offer a wide range of functionality, including: providing maps and local information to users, allowing users to share their locations with their friends, allowing people to track other people such as their employees or children, using player location information in electronic games, and providing location-based advertisements. These services use a variety of technologies to acquire a user's location based on the current location of the user's cell phone, computer, or other device. Some devices, such as smart phones, may use more than one locating technology. The following are locating technologies in common use today:

- **Global Positioning System (GPS)** locates a user through a device that triangulates a location based on signals it receives from a constellation of satellites. GPS is often unavailable indoors.

---

[4] http://www.locaccino.org/

[5] http://www.locaccino.org/science

[6] J. Tsai, P. Kelley, L. Cranor, and N. Sadeh. Location-Sharing Technologies: Privacy Risks and Controls. TPRC 2009, August 2009. http://cups.cs.cmu.edu/LBSprivacy/

- **Wireless positioning** locates a user by listening for signals of nearby WiFi access points and sending information about detected signals to a service that maintains a database of access point locations.

- **Cellular identification** locates a user by triangulating their position based on the cell towers within signal range of their mobile phone. Cellular providers can obtain location information of mobile phones in this manner even when the phones are not being used to place a call.

- **IP location** locates a user by looking up the Internet address of the user's device in a database that maps IP addresses to geographic locations. Internet addresses can be shared by multiple computers and may change over time. This technique typically provides only city-level location information.

Consumer Perceptions of Risks and Benefits of Location-Sharing Technology

In April 2009 we conducted an online survey to understand consumer perceptions of the risks and benefits associated with location-sharing services. Our non-random survey sample consisted of 587 respondents recruited through notices on websites that offered the opportunity to win a $75 gift card.

We showed survey participants a screen-shot of an online location-sharing service and asked them to list some benefits and some risks of using this technology. Then we described 14 scenarios that focused on benefits of location sharing and 10 scenarios that focused on risks of location sharing. For each scenario we asked participants to provide numeric ratings for the degree of harm or benefit they associated with each scenario. Participants rated finding people in an emergency as the scenario with the most significant benefit. Other highly beneficial scenarios included being able to track one's children, finding information based on one's location, checking to see if people are ok, and tracking relatives. Participants saw only limited benefit to using location-sharing technologies to meet new people

based on their location. On the risks side, participants saw great harm in scenarios involving stalking or revealing one's home address. They were also concerned about being found by people one wants to avoid, having others intrude on one's personal space, being found when one wants to be alone, being tracked by the government, and receiving location-based ads.

Overall, we found that most of our participants did not expect that location-sharing technologies would be all that beneficial to them, and they have significant concerns about their privacy when sharing their locations online.

Privacy Controls in Location-Sharing Applications

In August 2009 we evaluated 89 location-sharing applications and systems to determine the types of privacy protections each offered. Overall, we found that most of these applications provided fairly limited privacy controls and about a third of them did not provide readily accessible privacy policies on their websites. We reviewed the websites for these applications again in February 2010 and found similar results for the 84 services still in existence at that time. Privacy policies are notoriously difficult for consumers to understand, and many location-sharing services do not provide prospective users with a clear picture of how their location information will be used and shared before they sign up for the service. However, reading the fine print reveals that many location-sharing services store users' profile and location information indefinitely.

Some location-sharing applications have generic privacy policies that don't explicitly mention their use and sharing of location information. Others mention that they provide privacy controls, but in order for a consumer to see what controls are provided they have to actually sign up for and use the service. Only 18 of the 84 services examined in February 2010 mentioned privacy controls or security on the front page of their website (where they typically describe the benefits of their service and try to convince people to sign up for it).

We found that 76% of the applications had some form of privacy controls. However, most of these required users to visit or click multiple screens to reach the privacy settings. Most commercial systems had fairly basic privacy controls that allowed them to control whether their location would be made available publicly or would be made available only to designated friends. Some also had "invisible" modes where a user could prevent their location from being made available to anyone (other than the service provider itself). Few allowed people to choose to provide some locations on a less granular level such as neighborhood or city rather than street address or provided other fine-grained controls.

Some of the privacy controls that allow users to specify that their location information should be shared only with their friends rather than with the general public turn out to have exceptions. For example, many services have a simple privacy switch that can be set to "on" or "off." But in one service we examined, text positioned four paragraphs below the switch mentions "two exceptions" in which location information will be shared publicly even when the privacy switch is set not to share this information.

Our research at Carnegie Mellon University has explored the possibility of offering users more fine-grained and expressive privacy controls than typically found in commercial location-sharing systems. The Locaccino system, developed as part of our research, allows users to specify location-sharing rules based on time, location, and the person making a location request. For example, I have setup a rule that allows students to find my location when I am on campus so that they can determine whether I am in my office or teaching in another building. Another rule allows my family members to locate me at all times and locations. And another rule allows people I work with to locate me between 8 am and 6 pm on weekdays. Locaccino is not being used for advertising, but I could imagine a similar approach being used to control when and where location information is used for location-based advertising.

Our research has demonstrated that people have nuanced privacy preferences, and that providing them with the ability to control location sharing based on time and location offers substantial benefit over simpler privacy controls.[7] Of course, these more expressive privacy controls could become confusing and burdensome to users if not designed carefully to be easy and quick to use, with well-chosen, privacy protective default settings. We are currently exploring approaches to reduce user burden when using expressive privacy controls.[8]

Discussion

Our research suggests that Internet users are concerned about their location privacy, but that currently available location-sharing services do not, for the most part, do a good job informing them about how their location information will be used or provide users with expressive location privacy controls and privacy-protective default settings. Thus additional protections may be necessary.

While the CTIA Best Practices and Guidelines for LBS providers[9] offer a useful framework that requires notice and consent about location use and disclosure, they do not specify "form, placement, manner of delivery or content of notices," nor do they provide enforcement mechanisms or assurances that all LBS providers will follow them. Thus, while users may explicitly "opt-in" to a service by

---

[7] M. Benisch, P. G. Kelley, N. Sadeh, T. Sandholm, L. F. Cranor, P. Hankes Drielsma, J. Tsai. The Impact of Expressiveness on the Effectiveness of Privacy Mechanisms for Location Sharing. CMU-ISR Tech Report 08-141. http://reports-archive.adm.cs.cmu.edu/anon/isr2008/CMU-ISR-08-141.pdf

[8] P. Kelley, P. Hankes Drielsma, N. Sadeh, L. Cranor. User Controllable Learning of Security and Privacy Policies. *AISec 2008.* http://patrickgagekelley.com/file_download/1/aisec14-kelley.pdf

[9] Best practices and guidelines for location-based services. Version 3.18.08. CTIA Wireless Association (April 2 2008). http://www.ctia.org/business_resources/wic/index.cfm/AID/11300.

signing up for it, they may still not realize what they are getting themselves into. Users remain somewhat confused about the extent to which their location information may be shared and how they can control that.[10] And as the website Pleaserobme.com suggests, users may not fully think through the implications of broadcasting their location information to the public, or even be aware that a service makes their location information public.[11] Indeed, the CTIA Best Practices do not discuss the possibility that location information might be made public or recommend additional steps to be taken to notify users.

Even when users understand and are comfortable with the commercial uses of their location data, the use of this data without a warrant by law enforcement has troubling implications. Due to the way cellular technology works, the widespread use of cell phones enables large-scale round-the-clock surveillance of citizens. It is important that the storage of individual location data be minimized and that protections be put in place to limit when it can be disclosed to the government.

Finally, it is important to realize that techniques to de-identify or anonymize personal information may not be all that effective when it comes to location information. Even when a person is not identified by name or other commonly-used identifier, her location trails over time may be used to identify her. Since most of us go to a particular location for work each weekday and a particular location to sleep each evening, with only a few days of location trails information combined with

---

[10] L. Jedrzejczyk and B. A. Price and A. K. Bandara and B. Nuseibeh. I Know What You Did Last Summer: risks of location data leakage in mobile and social computing. http://computing-reports.open.ac.uk/2009/TR2009-11.pdf

[11] Pleaserobme.com is a website that displays publicly available location information from Twitter and Foursquare that indicates individuals who are not at home. The site creators write that their goal is to raise awareness of the risks associated with making personal location information available publicly. http://pleaserobme.com/why

other publicly available information it becomes possible to identify most people.[12] Thus, users who try to hide behind made-up names may still unwittingly be identifying themselves when they make their location information public. In addition, services that attempt to de-identify their users by removing their names before disclosing their location information may not be effectively anonymizing this data. Thus, it is important that privacy be considered from the beginning in the design of location-based services, and that users of these services are fully informed about the privacy implications of their use.

Thank you for inviting me to testify today. I look forward to answering your questions.

---

[12] P. Golle and K. Partridge. On the anonymity of home/work location pairs. Pervasive, 2009. http://xenon.stanford.edu/~pgolle/papers/commute.pdf

Appendix

J. Tsai, P. Kelley, L. Cranor, and N. Sadeh. Location-Sharing Technologies: Privacy Risks and Controls. TPRC 2009. Updated February 2010. http://cups.cs.cmu.edu/LBSprivacy/

Location-Sharing Technologies: Privacy Risks and Controls

Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, Norman Sadeh

Carnegie Mellon University
Pittsburgh, PA
jytsai@andrew.cmu.edu, pkelley@cs.cmu.edu,
lorrie@cs.cmu.edu, sadeh@cs.cmu.edu
Updated February 2010

Abstract. Due to the ability of cell phone providers to use cell phone towers to pinpoint users' locations, federal E911 requirements, the increasing popularity of GPS-capabilities in cellular phones, and the rise of cellular phones for Internet use, a plethora of new applications have been developed that share users' real-time location information online [27]. This paper evaluates users' risk and benefit perceptions related to the use of these technologies and the privacy controls of existing location-sharing applications. We conducted an online survey of American Internet users (n = 587) to evaluate users' perceptions of the likelihood of several location-sharing use scenarios along with the magnitude of the benefit or harm of each scenario (e.g. being stalked or finding people in an emergency). We find that although the majority of our respondents had heard of location-sharing technologies (72.4%), they do not yet understand the potential value of these applications, and they have concerns about sharing their location information online. Most importantly, participants are extremely concerned about controlling who has access to their location. Generally, respondents feel the risks of using location-sharing technologies outweigh the benefits. Respondents felt that the most likely harms would stem from revealing the location of their home to others or being stalked. People felt the strongest benefit were being able to find people in an emergency and being able to track their children. We then analyzed existing commercial location-sharing applications' privacy controls (n = 89). We find that while location-sharing applications do not offer their users a diverse set of rules to control the disclosure of their location, they offer a modicum of privacy.

1 Introduction

By 2009, at least 87% of the U.S. population owned cellular phones [3]. The proliferation of mobile devices and mobile Internet devices (including laptops) along with federal E911 requirements and the ubiquity of GPS-capabilities in mobile devices has spurred the development of location-sharing applications [27]. These technologies, also referred to as *mobile location* technologies, *social mobile* applications or simply *location-based services* (LBS), typically allow users to share their real-time or historical location information online.

Despite the increased availability of these location-sharing applications, we have not yet seen wide adoption [11, 23]. It has been suggested that the reason for this lack of adoption may be users' privacy concerns regarding the sharing and use of their location information [5, 14, 17, 23]. To explore these concerns regarding location-sharing technologies, we examine the use of LBS and research related to user's perceptions and use of location-sharing technologies in Section 1. Next, we investigate and enumerate the privacy controls offered by existing applications in Section 2. In Section 3, we present the results of an online survey to determine the magnitude of users' expected risks and benefits associated with these applications. Finally, in Section 4 we evaluate the ability of existing location-sharing technologies to address user's perceived risks and provide recommendations for controls to address users' privacy concerns.

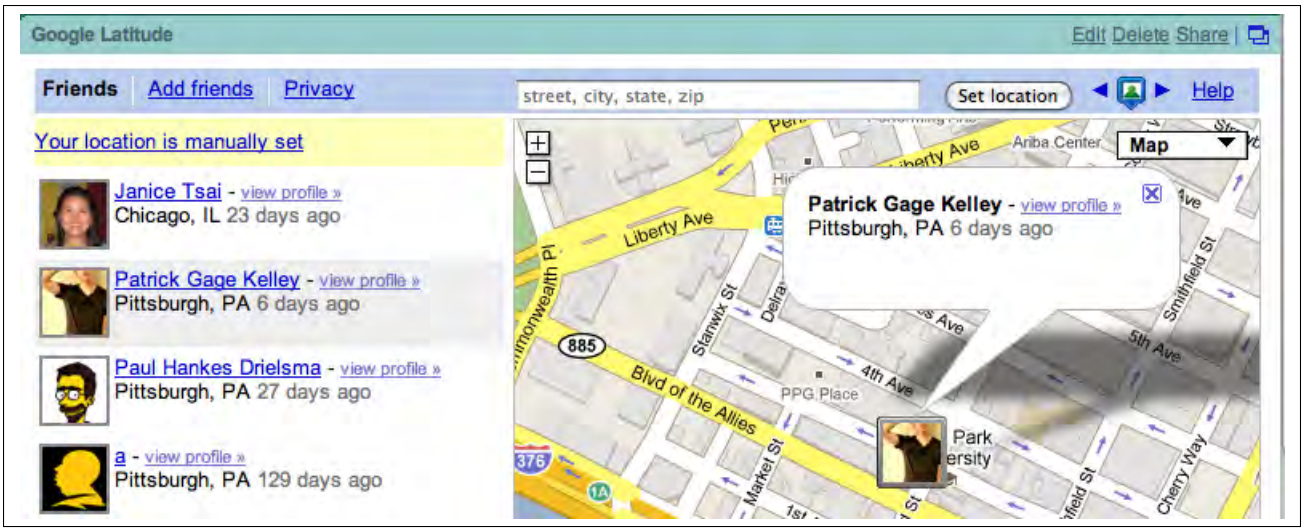

Fig. 1: The web interface for Google Latitude

1.1 Locating Technologies

The location-information shared by LBS may be text-based (e.g. "Andrew has been located at 5000 Forbes Ave., Pittsburgh, PA"), or it may be map-based, where the user's location is represented as a dot on a map as illustrated in Figure 1 and Figure 2. To display location information, users can manually enter a street address or longitude and latitude coordinates. Today, location information is more frequently acquired through automated means.

The following locating technologies are typically used to determine users' locations:

- **GPS:** The Global Positioning System (GPS), locates a user through a device that is in communication with a constellation of satellites. Triangulation by multiple satellites locates the device, making GPS the most accurate method for finding locations [27]. However, drawbacks include the lack of user-accessible GPS capabilities in most personal cell phones and the scarce availability of built-in GPS technology in commercial laptops. Additionally, GPS can be battery intensive and inconsistent or unavailable indoors.
- **Wireless positioning:** As urban areas become blanketed with both personal and public WiFi access points, users can be mapped according to the location of these access points. Through the process of "war-driving" access points, and mapping each broadcasting point to a GPS location [20], researchers and companies such as Skyhook Wireless[1] have created large databases with high location accuracy. While these locations are not always as precise as GPS, more people have wireless devices and location information can be pinpointed indoors.
- **Cellular identification:** At any given time, a mobile phone is likely in signal range of upwards of three cell phone towers, allowing a location to be triangulated if the locations of the cell towers are known. Some companies have partnered with telecom companies to use cellular data. One such company, AirSage[2] analyzes wireless signaling data to model traffic patterns.

[1] Skyhook Wireless. http://www.skyhookwireless.com/
[2] AirSage. http://www.airsage.com

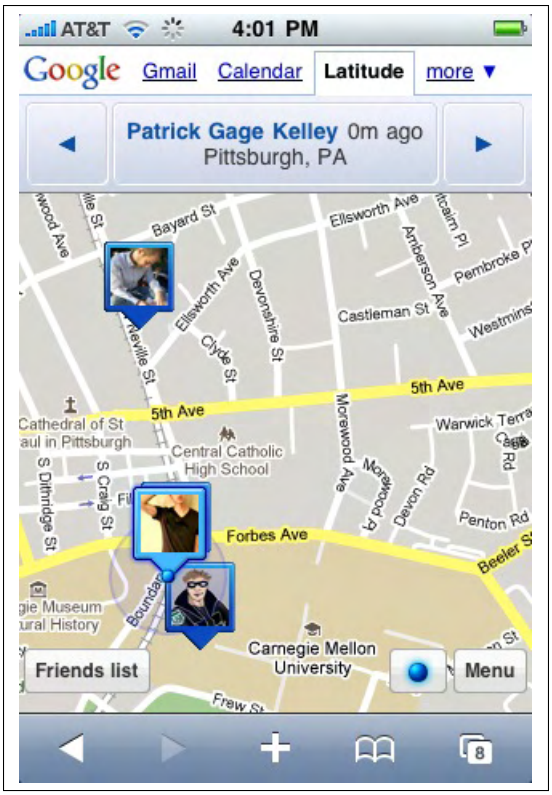

Fig. 2: The iPhone interface for Google Latitude

Loopt, a location-sharing service also leverages a cellular partnership with AT&T to provide always-on location information based on a user's iPhone [13].

– **IP Location:** Devices connected to an Internet network are provided with an IP address. IP addresses are limited in number; and based on the range, can be associated geographically [26]. (See the IP-to-Country Database.[3]) IP location is mostly used as a fallback when none of the above methods are available. The resolution of such lookups is commonly mapped to an area as large as a city.

1.2 Development Platforms for Locating-Technologies

Locating technologies are available for mobile phones, laptops, and internet-enabled mobile devices. There are three common ways for applications to pull location information:

– **Installed Software:** Users download and install software onto their cell phones or computers. Software determines the user's approximate location by one of the methods listed above and stores that data in a database or sends it to a location-sharing application. This transmission of coordinates may be automatic (e.g. a location ping is sent every 5 minutes) or it may require a "push" action to be initiated by the user (e.g. the user clicks a "Find me now" button).

[3] IP-to-Country Database. http://ip-to-country.webhosting.info/

– **Web browser:** In lieu of requiring the user to run a separate piece of software, several companies have developed location-finding web browser plug-ins. Applications that use this technology allow users to visit a website to be located, typically according to the users' wireless or IP location, based on an installed plug-in, such as Skyhook's web toolbar Loki.[4]
– **Location Broker:** APIs, (e.g. Yahoo!'s FireEagle[5] and Google Latitude[6]) allow developers to create applications that pull the user's location from a central provider. This allows application developers to entirely avoid any of the location lookup technologies, relying on a third party to provide location information.

1.3 Industry Best Practices

The worldwide revenues from mobile marketing are projected to reach $24 billion in 2013 [2]. It is understandable that the mobile or wireless industry would want to spur the adoption of location-sharing technologies. LBS may detect users' locations and offer them advertisements for businesses or services nearby. To address users' privacy concerns, CTIA, the International Association for the Wireless Telecommunications Industry,[7] issued Best Practices and Guidelines for LBS providers. These guidelines are meant to help LBS providers protect user privacy and rely on two of the Fair Information Principles (FIPs), *user notice* and *consent* .

The guidelines include the following [1]:

– **Notice:** First, LBS providers must inform users about how their location information will be used, disclosed and protected so that a user can make an informed decision whether or not to use the LBS or authorize disclosure.
– **Consent:** Second, once a user has chosen to use an LBS, or authorized the disclosure of location information, he or she should have choices as to when or whether location information will be disclosed to third parties and should have the ability to revoke any such authorization.

The CTIA guidelines do not specify the "form, placement, manner of delivery or content of notices" [1]. Generally, providers provide their statements regarding notice and consent in their posted privacy policies or terms of service.

1.4 Location Privacy Studies

Researchers have conducted studies to examine the usage of location-sharing applications and the privacy concerns raised by these applications. These studies have employed the experience sampling method (ESM) where users have carried devices to simulate location requests [4, 10, 19]. Other small laboratory experiments have involved small groups of participants who are members of existing social groups where people requesting locations were provided with automatic location disclosures [5, 9], or users responded via SMS with location information [16, 29]. Field studies

[4] Loki. http://loki.com/
[5] FireEagle. http://fireeagle.yahoo.net/
[6] Google Latitude. http://www.google.com/latitude/apps/badge
[7] The CTIA Wireless Association. http://www.ctia.org/

have been conducted by the authors and their colleagues, where we deployed a location-sharing application in a college campus community[30].

Research has shown that the primary dimensions of privacy concern surrounding the disclosure of this information include *context* and *use* [5, 6]. The willingness to share one's location and the level of detail shared depends highly on *who* is requesting this information [10, 21] (or knowing who is requesting this information [30]), and the *social context* of the request [9, 19]. Due to users' varied privacy concerns and preferences depending on the situation [21] or activity in which the user may be engaged [16], privacy controls need to be flexible [4, 28] and include a mechanism to provide plausible deniability [29].

In addition to the context of a location request, it is users' own perceptions of the *use* of one's location information that impacts their privacy concerns [6, 10]. For example, a user may be more concerned with an acquaintance requesting his or her location because they are unsure of *why* that information is being requested compared to users' lack of concern when sharing location information with people nearby to find restaurant recommendations.

1.5 Studies of Privacy Controls

Another cause of privacy concerns may be the lack of adequate controls for the disclosure of real-time personal information. Other studies have examined rules and the users desired diversity in the expressiveness of permissions in these types of systems [4, 7, 24]. In some cases, it may be enough for some users to simply create groups of contacts to assign permissions [15, 24], but others may require more flexibility in their rules [4] . In other research, it was found that a greater degree of rule expressiveness (e.g. being able to create group, time, and location-based rules) may increase the efficiency of allowing users to share information without violating their own personal privacy preferences [7], and that relationship-based default rules and machine learning techniques may reduce user burden in creating expressive rules [18, 25].

Based on this existing work, we delve into the design of commercial location-sharing systems and survey participants on their perceptions of the benefits and risks of specific scenarios of use for location-sharing systems.

2 An Evaluation of Privacy Controls in Location-Sharing Applications

We evaluated 89 applications, social networks, and APIs to evaluate their privacy controls. See the Appendix for a list of the applications. Our privacy and location-based services data is available online for download.

2.1 Method

We used a user-contributed online list of location-based services[8] as our directory of sites. In general, the sites on this list are social in nature. We found its completeness to be unparalleled across the web. We removed from consideration any sites that were not location-based services, or

[8] A list of Location Based Social Networking sites. http://bdnooz.com/lbsn-location-based-social-networking-links/. Last visited August 10, 2009.

sites that were offline or defunct (n = 10). This leaves us with a final set of 89 applications.[9] We did not consider "surveillance technologies."

To create our dataset, we completed a number of steps. First, we first visited the website for each application. We read the "About" page, frequently asked questions (FAQ), "Help" pages, and any other documentation available to search for explanations of their privacy controls. Additionally, we evaluated web interfaces, Facebook applications, and screen shots and descriptions of the iPhone application in the iTunes App Store. We evaluated the following features of these applications:

- **Date of launch:** While many of the current location-based services have been relaunched, rebranded, or generally attempted to "reboot" their service, we have tried to find the most accurate date of a first public, or widespread beta launch for each of the services. Many of these dates are based on news articles, press releases, and blogs that announced the opening of the service.
- **Privacy Policy:** We checked to see whether or not the website detailed their information practices (detailed in a privacy policy or included in a legal statement or terms of service).
- **Privacy Controls:** We noted any ability that allowed users to control access to their location information.
- **Notice:** Some systems notify users when others request their location, or make an activity log available to allow users to see who has requested and received their locations.
- **Immediately accessible privacy settings:** We noted whether or not the main interface allowed users to prominently see and access their privacy controls. For example, an application where one of the main tabs is labeled "Privacy" would fall under this category. An application that requires users to visit several pages or menus (e.g. Profile/Account/Settings/Privacy) does not.

2.2 Data Analysis

We constructed a datasetbased on our collection of the features listed above. In this section, we present the results of our analysis.

System Characteristics The primary purpose of the majority of these applications was for tracking friends or finding new ones. Other highlights included sites geared towards location-based dating, travel planning and sharing, and information seeking (e.g. finding local "hot spots"). One site even allows users to tag speed traps.

Of the 89 applications surveyed, 63 are available for use on mobile phones. Of those phone-based applications, the iPhone was the most popular development platform (40 applications). Application developers also created products for the Blackberry (32), phones that use the Android OS (21), or other phones (34). These numbers include services that developed a mobile formatted web version of their application and are not mutually exclusive. For example, a single service may have an iPhone application, a Blackberry application, and an Android application.

The architectures of the location-sharing applications fell into two categories:

- **Open:** Users can be found by friends and strangers.

[9] Note: One of the applications included on the list, Locaccino, was developed by the authors.

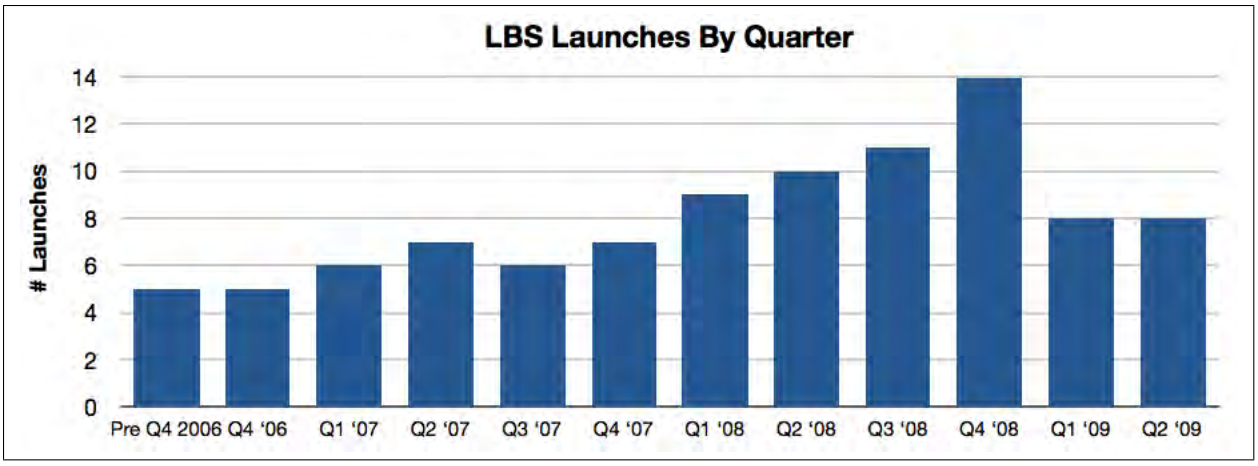

Fig. 3: The number of location-sharing applications launched each quarter (includes 89 applications evaluated in our study and 7 defunct applications).

– **Closed:** Users may only be requested by "friends" on the system. In this case, users much have already granted the requester access (e.g. by accepting a friend request).

Of the surveyed applications, five did not allow users to request other users' location information; but allowed users to seek information about places or landmarks; and two are location-sharing APIs. Of the remaining sites, 29 are closed systems, and 52 are open systems.

Rate of Creation The development of location-sharing applications has steadily increased over time as shown in Figure 3. Several new technologies may have spurred the development of location-sharing technologies. These include the launch of Yahoo's FireEagle platform (Q1 2008) and the iPhone SDK[10] with its Core-Location framework (Q3 2008).

The rate at which location-based services were introduced to the market increased from 5 per quarter at the end of 2006 to 14 per quarter at the end of 2008. After the economic downturn in 2008 the rate of introduction slowed, but new services continue to be introduced in 2009 at a rate of at least 8 per quarter. This overall growth leads us to believe two things. First, the development-side technologies are in place for location-based services and social networks to be created, and there are not unsolvable technical issues in the way of growth. Second, there do not seem to be strong market leaders who are prohibiting others from entering the market. Even with large players like Google, and established brands like Loopt, we have not seen any one of these technologies spread to a large section of the populace (however, finding active user data for any of these services has proven to be difficult).

Privacy Controls Due to the sensitive nature of real-time location information and the existence of guidelines recommending clear notice to users, one would expect all location-sharing applications to detail their policies for the collection and use of personal information. Instead, we found only

[10] iPhone Dev Center. http://developer.apple.com/iphone/

Category	Yes	No	Unknown	Not Applicable
Privacy Policy	66.3% (59)	33.7% (30)	-	-
Privacy Controls	76.4% (68)	16.9% (15)	1.12% (1)	5.62% (5)
Accessible Privacy Settings	16.9% (15)	75.3% (67)	2.25% (2)	5.62% (5)

Table 1: An overview of the proportion of applications that have privacy policies, privacy controls, and explicit privacy settings.

66% of the applications had privacy policies at all. For those services that did have privacy policies, the majority collect and save all data (e.g. locations, personal information entered into one's profile, and identifying web information such as one's IP address) for an indefinite amount of time. Only one, Mologogo[11] explicitly stated that it deletes GPS data after one month. Another interesting exception is Google Latitude which stores only the most recent location update.[12]

Our review of location-sharing applications reveals that the majority do have some form of privacy controls (76%). However, the majority of those privacy controls are not easily accessible from the main page or home page of the application itself. For the applications we reviewed, over 70% required users to visit or click multiple screens before they reached the privacy settings (see Table 1). This lack of immediately accessible privacy controls may be a result of the small amount of screen real estate available to application developers, especially in the case of mobile phones. For example, there was one case (Rummble[13]), included in the "Yes" category for accessible privacy settings in Table 1, where the web interface for the system had a link to the privacy controls, but the iPhone interface did not.

The types of privacy controls for the location-sharing applications are the following:

- **Blacklist:** Users are able to block specific individuals from viewing their location. (Found in 15.7% (14) of services.)
- **Friends Only:** This whitelist-based control restricts access to users denoted as a "Friend." By default, closed systems are considered friends only. (Found in 49.4% (44) of services.)
- **Granularity:** This advanced control allows users to instruct the system to provide a less detailed location to the person requesting information (e.g. "Andrew is in Pittsburgh, Pennsylvania.") (Found in 12.4% (11) of services.)
- **Group:** This restriction allows users to define access based on groupings of users. (e.g. Allow everyone in the "college friends" group to view my location.) (Found in 12.4% (11) of services.)
- **Invisible:** This feature may also be termed the "Private," "Only me," or "No one" setting. Users continue to send location data, but their locations are not divulged. (Found in 34.8% (31) of services.)
- **Location-based rules:** This restriction allows users to define locations in which their location-information may be revealed. For example, users may tag a location as "Work" or select an area on a map, and their location information is revealed to anyone who requests them when they are at that location. (Found in 1.12% (1) of services.)

[11] Mologogo. http://www.mologogo.com/

[12] Privacy (Google Latitude). https://sites.google.com/a/pressatgoogle.com/latitude/privacy

[13] Rummble. http://www.rummble.com/

- **Network:** This restriction allows the user to select existing communities to whom their location may be revealed. For example, user may join a geographical network or an interest-based community with whom they wish to share their location. (Found in 12.4% (11) of services.)
- **Per-request permissions:** Users must specifically review each location request, and decide whether or allow or deny the request prior to the location being revealed. (Found in 2.25% (2) of services.)
- **Time-based rules:** Users may define durations of time and days of the week during which their location may be revealed (e.g. from 10 am to 3 pm). (Found in 1.12% (1) of services.)
- **Time-expiring approval:** Several systems allow users to set a specific time frame (e.g. 1 hour) during which a link to the map of their location is "live." During this time frame, the recipient of the location message may view the map. After the expiration of this time, the link will no longer be accessible. (Found in 2.25% (2) of services.)
- **No restrictions:** Anyone is able to view the user's location. (Found in 16.9% (15) of services.)
- **Not Applicable:** Privacy controls do not apply. (Valid for 5.62% (5) of services.)
- **Unknown:** We were unable to find information about the privacy controls. (1.12% (1) service.)

In general, we see that the "Friends Only" and "Invisible" restrictions are the most prevalent. Of the 89 applications we reviewed, only four provided explicit notice to the user regarding who had requested their location. Aka-Aki,[14] Locaccino,[15] and Mobiluck[16] provide request logs to the user so they can view "Who's Viewed Me," Sniff[17] sends out a text message notification providing the name of the person making the request, and HeyWay[18] requires the user to explicitly approve or reject each location request (providing the name of the requester making the request). The native Loki browser plug-in explicitly asks the user if an application is making a request can access that information, but does not provider the name of the person making the request. Only one specific application Locaccino[19] had time-based and location-based rules.

3 Location-Sharing Risk/Benefit Analysis

We conducted an online survey to understand the magnitude of the risks and benefits associated with location-sharing services.

3.1 Method

For an individual user to accept a technology, an acceptable balance of personal risk and benefits must be established [12]. To understand these risks and benefits, we investigated the perceived-risk attitude or the expected value of location-sharing risks and benefits towards the use of location-sharing technologies. This evaluation takes into account the willingness or likelihood of engaging in the activity as a function of its expected benefit or harm [8]. We conducted an online survey to

[14] Aka-Aki. http://www.aka-aki.com/
[15] Locaccino. Note: the authors of this paper were also involved in the development of this application. http://www.locaccino.com
[16] Mobiluck. http://www.mobiluck.com
[17] Sniff. http://www.sniffu.com/
[18] HeyWay. http://niftybrick.com/heyway.html
[19] Locaccino. http://www.locaccino.org

capture users' perceptions of how likely certain scenarios would be if they used location-sharing scenarios and the magnitude of benefits or risks related to each scenario.

Recruitment In April 2009, we solicited participants to complete a survey to examine their personal perceptions about location-sharing technologies. Online announcements were posted on the "Volunteers" section of craigslist.com for major metropolitan areas of the United States and in online sweepstakes websites, recruiting individuals over the age of 18. The survey was available online for two weeks. We raffled a $75 Amazon.com gift certificate as the incentive for participation.

Demographics The final survey sample consisted of 587 respondents. Although 655 people completed the survey, respondents who completed the survey in under 4 minutes were eliminated from the final dataset. Due to the number of questions in the survey, we believed that anyone who answered in under 4 minutes was simply clicking through the survey, rather than reading and responding to the questions. Participants' ages ranged from 18 to 79 years of age (M = 35.7), and 61% were female. The respondents were fairly well educated, with 43.8% indicating that they had college degrees and 29.1% having graduate degrees. In general, most people (72.4%) had heard of technologies that allow people to share their locations with others.

3.2 Survey Data Analysis

Technology Use At the beginning of the survey, an example of an online-location sharing technology was presented to the study participants. A screen shot of of a map with a thumbnail of a person's picture pinpointed on the map was displayed, indicating that the person had been located with this technology (see Figure 4). Participants were asked to list some benefits and risks or dangers associated with this technology.

Some examples of benefits listed by our respondents are the following:

- Give out directions quickly to friends and family.
- Able to track loved ones and opportunity to surprise someone for a special event.
- People you know can find you, parents can track their kids, facilitates a rendezvous.
- Serendipitous encounters.
- Remote awareness of friends and relatives.

Some examples of dangers listed by our respondents are the following:

- Anyone could know exactly where you are - there is no privacy - anyone could find you at any given time.
- If someone intends to do you harm, they would find you easily.
- An unwanted person will find you and stalk you. It is not safe. You have no control.
- Location history could be harvested for stalking or marketing.
- People could find out if no one was home.

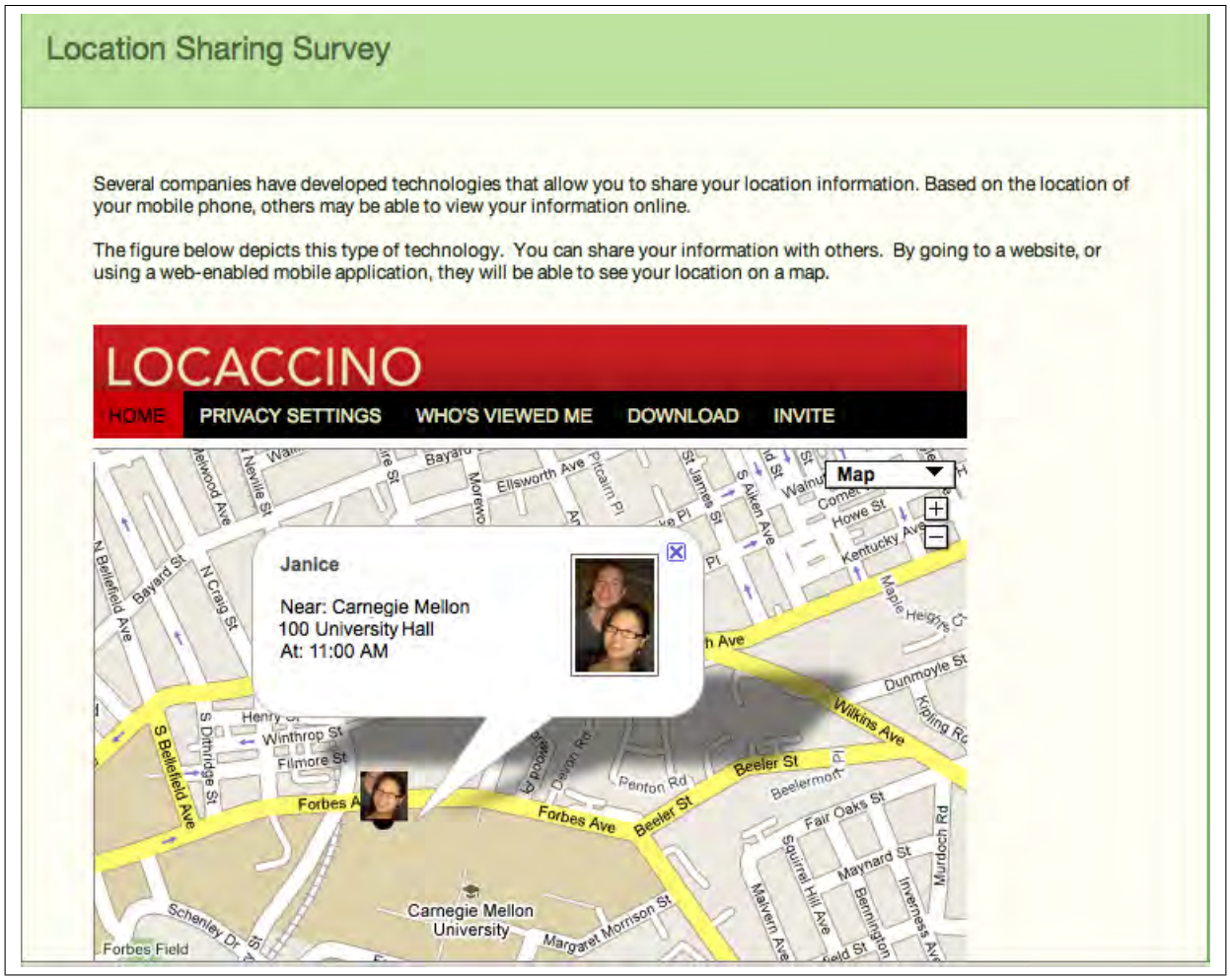

Fig. 4: A screen shot of the location-sharing interface presented to our survey participants

Respondents were asked a series of 7-point Likert scale questions asking them to rate the usefulness of location-sharing technologies (ranging from *not useful* (1) to *extremely useful* (7)), their privacy concerns surrounding their use of these technologies (ranging from *not concerned* (1) to *extremely concerned* (7)), and the risk of using these applications (ranging from *the risk far outweighs the benefit* to *the benefit far outweighs the risk*). These questions were asked both at the beginning and end of the survey to determine if participating in the survey altered users' opinions.

The results reveal that people's first impression of location-sharing technologies is that they are mostly not useful. After taking the survey, which included various usage scenarios, people's opinions changed slightly, and they found the technology slightly more useful. They also became more concerned about allowing others to view their locations at the end of the survey. Participants' attitudes about the risk of using location-sharing technologies slightly outweighing the benefits did not change: they felt that the risk still outweighed the benefits. See Table 2 for mean values and paired t-test p values.

Item	Before	After	t statistic	p value
Usefulness	3.72	3.94	-3.91	$<$**0.001**
Concern	5.15	5.42	-4.66	$<$**0.001**
Risk	3.27	3.33	-1.01	0.31

Table 2: Participants' responses to 7-point Likert scale questions regarding the usefulness (*not useful* (1) to *extremely useful*) (7), concerns associated with allowing others to view your location (*not concerned* (1) to *extremely concerned* (7)), and the risk of using location-sharing technologies (*the risk far outweighs the benefit* (1) to *the benefit far outweighs the risk* (7)) at the beginning and end of the survey. The degrees of freedom for the paired t-tests is 586.

Item	M	t statistic	p value
You	3.84	-1.84	0.07
Family	3.67	-3.78	$<$**0.001**
Friends	4.30	4.05	$<$**0.001**
Company/Employer	3.63	-4.52	$<$**0.001**

Table 3: Participants' responses to 7-point Likert scale question regarding the likelihood of the use of location-sharing technologies (very unlikely (1) to very likely (7)). The responses are compared in a t-test to the midpoint (4). The degrees of freedom for the t-test are 567.

In the survey, we also asked participants about how concerned they were about controlling access to their location on a scale of *not concerned* (1) to *extremely concerned* (7). We found that participants were extremely concerned about having control (M = 6.17).

We also asked participants to rate the likelihood of the use of location-sharing technologies by him or herself, their family, their friends, or their company or employer. Based on a 7-point Likert scale ranging from *very unlikely* (1) to *very likely* (7), we find that people think it is unlikely that their families and employers will use location-sharing technologies. As for themselves, they are neither likely nor unlikely to use the technologies, but think that they friends are more likely to use these types of applications. The responses to this question and their comparison to the midpoint of the scale are summarized in Table 3.

Gender Differences Dividing participants by gender, we see that men find location-sharing technologies slightly more useful than women do, but men still find these technologies neither useful nor useful. Women are also much more concerned with allowing others to view their locations, tend to feel that the risk of using these technologies far outweighs the benefit, and do not find it likely that they will use these technologies. These responses are detailed in Table 4.

Scenarios We asked participants to rate the likelihood of the occurrence of the scenarios below on a 7-point Likert from very unlikely to very likely. Each scenario is also rated as a harm or a benefit. For each of the harms scenarios, participants were asked to rate each harm from a scale from *not*

Item	Female	Male	t statistic	p value
Usefulness	3.77	4.20	-2.78	**.006**
Concern	5.60	5.14	3.73	$<$**0.001**
Risk	3.07	3.72	-4.19	$<$**0.001**
Likeliness of Use	3.56	4.26	-3.8	$<$**0.001**

Table 4: Participants' responses to 7-point Likert scale questions regarding the usefulness (*not useful* (1) to *extremely useful*) (7), concerns associated with allowing others to view your location (*not concerned* (1) to *extremely concerned* (7)), the risk of using location-sharing technologies (*the risk far outweighs the benefit* (1) to *the benefit far outweighs the risk* (7)) at the end of the survey, and the likeliness of use by the respondent. The degrees of freedom for the two-sample t-tests is 585.

harmful at all (1) to *extremely harmful* (7). For each of the benefits scenarios, participants were asked to rate each benefit on a scale from *no benefits at all* (1) to *great benefit* (7).

The responses to the scenarios are detailed in Table 5 and Table 6.

There were several scenarios in which people would be extremely likely to benefit from such services: finding people in an emergency, finding information based on location, and finding (tracking) their children. Based on the survey results, people also seem to realize that using location-sharing technologies will likely open them to receiving advertisements based on their location, being intruded upon, as well as accidentally revealing the location of their homes.

Level of Privacy Concern We sought to determine the level of privacy concerns that people perceive when they are sharing their information online by asking several privacy scale questions. These privacy scale questions are based on an instrument developed by Malhotra et al. to measure Internet Users' Information Privacy Concerns (IUIPC) [22]. The IUIPC scale defines several groupings of concern, including control, awareness of privacy practices, collection of information, errors, unauthorized secondary use, improper access, and global information privacy concern; and consists of 27 questions. Based on a pilot test where we correlated the use of Facebook, an online social network, and the use of its privacy settings, we selected a sampling of 6 questions. Based on these questions, we calculated a "Privacy score" for each respondent. This score is an average of the ratings of the following six statements presented to the users, rated on a 7-point Likert scale, ranging from *strongly disagree* (1) to *strongly agree* (7). The higher the privacy score, the more concerned the person is about their privacy.

Participants were asked to rate the following statements:

- It is very important to me that I am aware and knowledgeable about how my personal information will be used. (IUIPC Awareness)
- I'm concerned that online companies are collecting too much personal information about me. (IUIPC Collection)
- Online companies should have better procedures to correct errors in personal information. (IUIPC Errors)

Scenario	Likelihood	Benefit
Finding people in an emergency	5.64	5.97
Finding information based on your location	5.29	4.99
Keeping track of the location of children in your family	5.17	5.18
Checking people's locations to make sure they are ok	4.98	5.05
Finding nearby friends for social activities	4.76	4.36
Using people's locations to coordinate a meeting	4.67	4.34
Keeping track of elderly relatives	4.66	5.11
Keeping track of where you've been	4.65	3.84
Coordinating family activities	4.59	4.39
Finding a coworker who is running late for a meeting	4.42	4.03
Coordinating ride sharing or carpooling	4.38	4.29
Having fun with locations	4.35	3.47
Recruiting people to participate in activities	4.01	3.83
Finding new people with similar interests	3.49	3.46

Table 5: Benefits-based location-sharing scenarios and their likelihood and magnitude of benefit ratings based on survey results, ordered by highest likelihood.

- Online companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information. (IUIPC Unauthorized secondary use)
- Online companies should take more steps to make sure that unauthorized people cannot access personal information in their databases/servers. (IUIPC Access)
- I am concerned about threats to my personal privacy today. (IUIPC Global Concern)

To determine if this scale was internally reliable, we compute a Cronbach's α score for this set of questions. This statistic allows us to determine if the items, together, measure a consistent viewpoint. A set of items with a Cronbach's α score of above 0.70 is considered to be reliable. We found this 6-item scale for assessing users privacy concerns regarding online companies to be reliable, with a Chronbach's α of 0.85.

To determine if the privacy score had any relation to users' use and perceptions of location-sharing technologies, we examined their correlations. We see that the higher the privacy score, the more likely it is that users will feel that the risks of using location-sharing technologies outweigh the benefits (Risk After, $r(586)$ = -0.23, p <.0001); that they would be less likely to use such technologies ($r(586)$ = -0.12, p = 0.004); and feel that this technology is not useful (Usefulness After, $r(586)$ = -0.11, p = .007). Additionally, users with higher privacy scores were older ($r(586)$ = 0.23, $p < .0001$), more concerned about privacy (Concern After, $r(586)$ = 0.41, $p < .0001$), and more concerned about controlling access to their location($r(586)$ = 0.39, $p < .0001$).

Expected Values of Risks and Benefits To examine the ranking of the scenarios, we computed an expected value for the risk variable by multiplying the likelihood perceptions by the magnitude

Scenario	Likelihood	Harm
Being bothered by ads that use your location	5.27	4.68
Having people intrude on your private space	5.15	5.51
Revealing the location of your home	5.11	5.93
Being found by someone you don't want to see	5.10	5.56
Being found when you want to be alone	5.07	5.08
Revealing activities you are participating in	4.83	4.17
Being stalked	4.75	6.32
Having the government track you	4.62	5.38
Being judged based on your location	4.35	4.50
Having your boss spy on you	4.21	5.15

Table 6: Risk-based location-sharing scenarios and their likelihood and magnitude of harm ratings based on survey results, ordered by highest likelihood.

of the risk (harms) or benefit. This value allows us to compare within the sets of scenarios that are considered harms and those that are considered benefits.

Within each set of harms and benefits, the expected value for the risk (or benefit) of each was compared to the other harms or benefits with paired t-tests to determine which scenarios are significantly distinct from each other ($p < 0.05$). The relative rankings for the benefits and risks as determined by their expected value are summarized in Table 7 and Table 8.

Evaluating each expected benefit, one sees that, by far, the most significant benefit is being able to find people in an emergency. The next distinct benefit is being able to track one's children. Finding information based on one's location, checking to see if people are ok, and tracking relatives are the third set of distinct benefits. The least valued expected benefit of location-sharing technologies is finding new people based on one's location.

The greatest expected harms derived from the use of location-based technologies are revealing one's home and being stalked. People perceive that being found by people one wants to avoid and having others intrude on one's personal space are the next set of situations associated with these technologies. Being found when one wants to be alone, being tracked by the government, and receiving ads based on one's locations are the third set of distinct harms. It seems that people are the least bothered by the risks of being judged based on one's location and revealing activities that one is participating.

Analysis of participants with children One potentially useful scenario for location-sharing technologies is keeping track of children in one's family. We asked participants to list the number of children they had, and divided our participants into two categories: those who have children and those who do not. The group with children includes those with adult children. Demographics are summarized in Table 9. We see that having children does have an impact of one's perceptions of these technologies.

Participants with children rated location-sharing technologies significantly more useful at the beginning of the survey as compared to participants without children ($M_{WithChildren}$ = 3.93 vs.

Ranking	Scenario
1.	Finding people in an emergency
2.	Keeping track of the location of children in your family
3.	Finding information based on your location
3.	Checking people's locations to make sure they are ok
3.	Keeping track of elderly relatives
4.	Finding nearby friends for social activities
4.	Using people's locations to coordinate a meeting
4.	Coordinating family activities
5.	Coordinating ride sharing or carpooling
5.	Discovering that a friend from out of town is visiting
6.	Keeping track of where you've been
6.	Finding a coworker who is running late for a meeting
7.	Recruiting people to participate in activities
7.	Having fun with locations (e.g. games, pranks)
8.	Finding new people with similar interests

Table 7: The relative rankings of benefits obtained from the use of location-sharing technologies.

$M_{WithoutChildren}$ = 3.59, t(585) = -2.17, p = 0.03). After taking the survey, both groups felt the same about location-sharing technologies being neither useful nor not useful ($M_{WithChildren}$ = 4.08 vs. $M_{WithoutChildren}$ = 3.85, t(585) = -1.5, p = 0.13).

When asked about the likelihood of use of these types of technologies, participants with children were significantly more likely to feel that they, their families, friends and employers would be likely to use these technologies as compared to people without children. See Table 10 for details of survey results and t-tests.

Examining the responses to the scenarios, we see that participants with children derived greater expected benefit, as compared to respondents without children from the following scenarios: checking people's locations to make sure they are ok, coordinating family activities, keeping track of the location of children in your family, keeping track of elderly relatives, and finding new people with similar interests. Those with children also had a greater amount of expected risk from being bothered by ads that use their location, being tracked by the government, and revealing activities they are participating in. These differences are detailed in Table 11.

For respondents with children, being able to track their kids becomes the top benefit, tied with being able to find people in an emergency. Even when we control for age and gender, we find this to be the case.

4 The Ability of LBS Applications to Address Users' Perceived Risks

As location-based services proliferate in numbers but not in users [11, 23], we examined the ability for these location-sharing applications to address users' privacy concerns. We see that the number of applications has been increasing and companies have developed platforms that make it easier for

Ranking	Scenario
1.	Revealing the location of your home to people you do not want to give your address to
1.	Being stalked
2.	Having people intrude on your private space
2.	Being found by someone you don't want to see
3.	Being found when you want to be alone
3.	Having the government track you
3.	Being bothered by ads that use your location
4.	Having your boss spy on you
5.	Revealing activities you are participating in
5.	Being judged based on your location

Table 8: The relative rankings of risks related to the use of location-sharing technologies.

Item	Without Children	With Children
Gender	Fem: 218, Male: 147	Fem: 140, Male: 82
Avg. Age	30.9	43.7

Table 9: Participants characterized by whether or not they have children or do not have children.

others to create applications that leverage location information. Based on the results of our survey, we see that people still do not find these location-sharing technologies all that useful, and they are still concerned about their privacy when sharing their locations online. In general, people still believe that the risks of sharing their locations online outweigh the benefits.

Based on our analysis of the risks associated with these technologies, we now examine the existing privacy controls of these technologies and investigate the ways in which these controls can address users' major concerns. We also suggest additional methods of addressing users' concerns.

4.1 Addressing risks with privacy controls

To determine if privacy controls are effective in location-sharing technologies, we first examine users' greatest expected risks.

As enumerated in Table 8, we see that the top ranked expected risks are the following:

- Revealing the location of your home to people you do not want to give your address to
- Being stalked
- Having people intrude on your private space
- Being found by someone you don't want to see
- Being found when you want to be alone.
- Having the government track you.
- Being bothered by ads that use your location .

Below, we examine how location-based applications' privacy controls address these concerns.

Item	Without Children	With Children	t statistic	p value
You	3.67	4.11	24.01	$<$**0.001**
Family	3.32	4.26	28.36	$<$**0.001**
Friends	4.27	4.36	26.52	$<$**0.001**
Company/Employer	3.48	3.87	26.21	$<$**0.001**

Table 10: Participants' responses to 7-point Likert scale question regarding the likelihood of the use of location-sharing technologies (very unlikely (1) to very likely (7)) for people without children and with children. The degrees of freedom for the t-test are 585.

Item	Without Children	With Children	t statistic	p value
Okayness Checking	25.0	29.9	-4.06	$<$**0.001**
Coordinating Family Activities	20.5	26.1	-4.65	$<$**0.001**
Tracking Children	26.1	34.6	-6.18	$<$**0.001**
Tracking Relatives	24.2	29.9	-4.12	$<$**0.001**
Finding New People	13.0	16.0	-2.8	**0.005**
Bothered by Ads	24.7	27.7	-2.35	**0.02**
Tracked by the Government	25.3	28.0	-1.98	**0.05**
Revealing One's Activities	20.1	22.4	-2.08	**0.04**

Table 11: Participants' expected benefits and risks based on if they have children or if they do not have children. The values were calculated by multiplying the likelihood ratings of each secenario with its rated risk and benefit. Degrees of freedom for the two-sample t-tests are 585.

Blacklist: With blacklists, users are able to block specific people with whom they do not wish to reveal this location. This restriction allows users to protect against revealing the location of their homes, block known stalkers and people they do not wish to see. If users are active in managing and updating their blacklists, they may also reduce the ability to having people intrude on their space, and avoid being found when they want to be alone. Unfortunately, in the last two cases, users must spend the effort and time to add people to a blacklist, and must remember to remove people from the blacklist once they want to be found again.

Friends Only: By solely allowing all friends to access users' locations, this protects users from being stalked (users may remove their stalkers from their friend lists). Unfortunately, this control does not protect from being found by friends when one wants to be alone or being found by someone who is a friend, but whom you may not wish to see. To deal with these concerns, users may manage their friend lists by adding and removing friends as they see fit.

Granularity: Allowing the location-sharing application to only provide general information (e.g. neighborhood, city, or state) about one's location mitigates the risks (except for being bothered by ads and and being tracked by the government). Unfortunately, by only providing a wide range of possible locations, this also negates the benefits provided by location-sharing applications.

Group-based rules: Allowing people access to your location by dividing them into groups mitigates several privacy concerns. These group-based rules allow users to protect the location of their homes, to hide themselves from stalkers, and to avoid people they do not want to see. Based on how large one's group is and how active they are in assigning people to groups may also reduce, but not eliminate the risks of having people intrude on their private space and being found when they want to be alone.

Invisible: By going invisible, the user reduces the risks listed above except for that of being bothered by location-based ads and government tracking. The user can significantly reduce the risk of being stalked or of being found by people they don't want to see, but they also reduce the benefits of these services. To most effectively deal with the risks, they must be very active in turning invisible mode on and off, which places a significant burden on the user.

Location-based rules: Defining access by location allows the user to effectively protect the location of his home or spaces in which one needs private space or alone time. These rules may also block known stalkers at locations they do not wish to reveal. By continuously updating these rules, users may effectively address most of the risks, but this requires users to regularly update their rules.

Network: A network is typically larger than a group (e.g. the Chicago network). This may make it easier for users to define rules, but may not be an effective means in protecting them from the risks listed above. By defining network based rules, one prevents the general public from locating them, but may not keep stalkers within their network from finding them, or it may not prevent others from finding the location of their home, or preserving their personal space and alone time.

Per request permission: Requiring users to approve of each location request reduces the risks listed above except for that of being tracked by the government and being bothered by ads. Unfortunately, this method requires that users be interrupted, and this may become too burdensome on the user.

Time-based rules: Basing restrictions on time allows users to create restrictions to protect the locations of their homes (assuming they are home at regular times). Time-based restrictions can also protect users from being intruded upon, being found, and allows them to be be alone at certain times of day or days of the week.

Time-expiring approval: Allowing users to specifically permit others to locate them mitigates most risks (excluding government tracking and being served with advertisements based on their location). Unfortunately, allowing users to be the only ones to "push" location information also negates most of the top benefits of location sharing (e.g. one would not be able to find someone in the case of an emergency when they need to wait for the user to make his location available for a small period of time).

No restrictions: Having no rules allows users to be located by anyone. This opens them up to all the benefits as well as the risks of using location-sharing technologies.

We see that the rules that allow users to mitigate the greatest risks are the following:

- Blacklist
- Granularity

– Group-based rules
– Location-based rules
– Time-based rules

Each of these rules alone, including the burden on the user, does not address the largest expected risks of using location-sharing technologies. We find that location-sharing technologies offer limited flexibility in their privacy controls. It is rare that systems give users the ability to specify expressive rules to control the sharing of their location information. Furthermore, there are no commercially available systems that offer anywhere near as powerful a control set as one could imagine: with the ability to specify rules based on specific users and groups of contacts, to control access based on time and location, to return locations at varying granularities, and to become invisible or obfuscate locations in extreme situations. There is one system, Locaccino, developed by the authors their university, that offers time, location, and group based rules, as well as invisibility. A combination of all of these rules would be the most effective in addressing users' privacy concerns.

Another factor that has been mentioned briefly is user burden. In some cases, it would be possible for the user to toggle being invisible on and off all day, based on that day's events. Unfortunately, in our experience, people easily forget to do this. Once the location-sharing software is up and running, it is easier to leave it running; otherwise, once people go offline or invisible, they are likely to leave the software in that setting. Similarly, in systems that do offer a myriad of privacy controls, methods must be developed to help users create rules based on their daily schedules, and regular and irregular interactions with others.

4.2 Discussion

By defining the relative value of users' expected risks and benefits regarding the use of location-sharing services, we develop an understanding users' privacy concerns. We see that, in general, industry guidelines do not address these concerns, and the privacy controls in existing applications do not comprehensively address these concerns. In this paper, we have provided recommendations for sets of privacy control that may assist developers in addressing users' privacy concerns.

Based on the current perceptions of benefits and harms of location-sharing technologies at this time (noting that perceptions of risks in this area may evolve or shift), the primary risks can be addressed or mitigated by the design of the location-sharing technology. Based on the current restrictions offered by location-sharing technologies, we find that these risks may not be addressed, in full, by the current palette of available privacy controls. Instead, location-sharing applications may want to consider making more expressive privacy controls available to their users. With more expressive controls, people may become more comfortable with sharing their location information and find more value in these services. Additionally, future work must be done to determine how to reduce user burden. A balance must be found between expressiveness and usability or with offering users complex and detailed privacy controls and making these controls easy to use.

Another matter to consider is that of users' evolving privacy concerns. Currently, we find that users' still do not find location-sharing services useful. This may be due to the lack of usage in general. Without a critical mass of users, current users are unable to reap the benefits of being

able to find their friends or to track family members. As more and more people adopt these types of technologies, and peer opinion about these technologies becomes more favorable, the level of concern that people feel may diminish. Additionally, we find that it is younger people or people with children who are more interested in location-sharing applications and are more likely to adopt these services.

Appendix. Location-Sharing Applications

As of 2/20/10

Open Systems: Users can be requested by people with whom they do not have a connection (i.e. Strangers)

Closed Systems: Users must be "Friends" or connected to one another

***** Application also has time and location-based access restrictions

Application	Creation Date	URL	Push / Pull	System	Accessible Privacy	Privacy Policy Aug 2009	Privacy Policy Feb 2010	Policy Mentions Location	Home Page Mention	Black-list	Explicit Request	Friends	Gran-ularity	Group	In-visible	Network	Time Expire	None	N/A	Un-known
Aka-Aki	03/01/07	http://www.aka-aki.com/	Push	Open	No	Yes	Yes	Yes	Yes			X			X					
Belysio	08/22/08	http://www.belysio.com/	Pull	Open	No	Yes	Yes	Yes	No			X			X	X				
Bliin	10/17/06	http://www.bliin.com/	Pull	Open	No	No	No	--	Yes			X			X					
Bluemapia	06/17/08	http://www.bluemapia.com/	Push	Open	No	No	No	--	No						X					
Blummi!	10/18/08	http://www.blummi.com/	Pull	Open	Unknown	No	No	--	No				X							
Brightkite	04/01/07	http://www.brightkite.com/	Push	Open	Yes	Yes	Yes	Yes	No			X	X	X	X	X				
Buddy Beacon	11/10/06	http://where.com/buddybeacon/	Pull	Open	No	Yes	Yes	Yes	Yes	X										
BuddyCloud	04/01/08	http://www.buddycloud.com/cms/	Push	Open	No	No	No	--	No				X							
BuddyMob	12/01/08	http://www.buddymob.com/	Push	Open	No	No	No	--	No									X		
Buddyway	08/11/08	http://www.buddyway.com/	Push	Open	No	No	No	--	No									X		
Buzzd	02/06/08	http://buzzd.com/	Pull	Open	No	Yes	Yes	No	No			X			X					
Carticipate	03/08/08	http://www.carticipate.com/	Push	Open	No	Yes	Yes	No	No									X		
Centrl	03/16/07	http://centrl.com/	Pull	Open	No	Yes	Yes	Yes	No			X				X				
CitySense	06/09/08	http://www.citysense.com/	Pull	N/A	NA	Yes	Yes	No	No										X	
ComeTogethr	10/01/08	http://www.cometogethr.com/	--	Open	Yes	Yes	**Missing**	--	No			X		X	X					
Dopplr	07/01/07	http://www.dopplr.com/	Push	Closed	No	No	No	--	No			X								
EagleTweet	04/04/09	http://eagletweet.com/	Push	Open	No	No	**YES**	Yes	No											
FindbyClick	12/21/06	http://www.findbyclick.com	KILLED NOVEMBER 2009			No													X	
FindMe	03/18/08	http://electricpocket.com/findme/	Pull	Open	No	No	No	--	No						X					
FireEagle	08/12/08	http://fireeagle.yahoo.net/	Pull	API	Yes	Yes	Yes	Yes	Yes				X		X	X				
Flaik	11/26/07	http://www.flaik.com/	Pull	Open	Unknown	No	No	--	No											X
Footprint History	02/01/09	http://www.footprinthistory.com/	Push	Closed	No	Yes	Yes	No	Yes			X								
FourSquare	03/13/09	http://foursquare.com	Push	Closed	No	Yes	Yes	Yes	No			X								
Foyage	12/01/08	http://i.foyage.com	Pull	Open	No	No	No	--	No						X					
Friends on Fire	03/13/09	http://apps.facebook.com/on-fire/	Pull	Closed	Yes	Yes	Yes	Yes	Yes			X	X							
GeoMe	10/01/08	http://www.geo-me.com	Push	Closed	No	Yes	Yes	Yes	No			X								
GeoSpot	03/12/08	http://www.geospot.com/gs/Home	Push	N/A	NA	Yes	Yes	No	No										X	
GeoUpdater	12/10/08	http://linuxinside.org/geoupdater/	Push	Closed	Yes	Yes	Yes	No				X	X			X				
Google Latitude	02/04/09	http://www.google.com/latitude	Pull	Closed	Yes	Yes	Yes	Yes	Yes	X		X								
Groovr	12/29/06	http://www.Groovr.com	KILLED JANUARY 2010			Yes						X		X						
Gympse	05/22/09	http://www.glympse.com/	Push	Closed	Yes	Yes	Yes	Yes	No			X					X			
GyPSii	03/06/08	http://www.GyPSii.com/	Pull	Open	No	Yes	Yes	Yes	No			X			X					
HeyWay	06/17/09	http://niftybrick.com/heyway.html	Push	Closed	No	No	No	--	Yes		X	X		X		X				
HiMyTribe	08/07/09	http://www.himytribe.com/	Push	Closed	No	No	No	--	No			X		X						
ICloseby	01/30/08	http://www.icloseby.com	Push	Open	No	No	No	--	No	X										
iPling	06/29/07	http://www.iPling.com	Push	Open	No	Yes	Yes	Yes	No				X							
Ipoki	12/18/07	http://www.ipoki.com/	Pull	Open	Yes	Yes	Yes	Yes	No			X			X					
IRL	04/19/09	http://corp.irlconnect.com	Pull	Open	No	No	**YES**	Yes	No									X		
LightPole	01/01/07	http://www.lightpole.net	KILLED OCTOBER 2009			Yes													X	
Limbo	08/01/07	http://www.limbo.com	Push	Open	No	Yes	Yes	No	No	X				X						
Locaccino*	03/01/09	http://www.locaccino.org	Pull	Closed	Yes	Yes	Yes	Yes	Yes			X		X		X				
Locatik	05/22/08	http://www.locatik.com	Pull	Open	No	Yes	Yes	Yes	No									X		
Locatrix	04/08/09	http://www.locatrix.com	CUT FROM LIST - Parent			Yes				X		X	X		X					

Locle	10/01/08	http://www.locle.com	Pull	Closed	No	No	No	--	No	X		X								
Loki	04/09/07	http://www.loki.com	Pull	API	No	Yes	Yes	Yes	No		X									
Loopt	11/16/06	http://www.loopt.com	Pull	Closed	Yes	Yes	Yes	Yes	No	X		X				X				
Map My Tracks	12/23/07	http://www.mapmytracks.com	Push	Open	No	Yes	Yes	No	No									X		
MapMe	07/01/08	http://www.mapme.com	Push	Open	No	Yes	Yes	Yes	No			X			X	X				
Match2Blue	12/21/08	http://www.match2blue.com/cms/	Push	Open	No	Yes	Yes	Yes	No									X		
Meet Now Live	04/01/08	http://www.meetnowlive.com	Push	Open	No	Yes	Yes	Yes	No									X		
MeetMoi	11/25/08	http://www.meetmoi.com	Pull	Open	No	Yes	Yes	No	No				X							
Microsoft Vine	04/28/09	http://www.vine.net/default.aspx/	Push	Closed	Yes	Yes	Yes	Yes	No			X		X						
Mizoon	10/02/08	http://www.mizoon.com/	Push	Open	No	No	No	--	No									X		
Mobilaris	11/01/03	http://www.mobilaris.com	CUT FROM LIST - Parent			No									X					
Mobiluck	09/01/07	http://www.mobiluck.com	Pull	Open	Yes	Yes	**NO**	--	Yes	X		X			X					
Mologogo	10/01/07	http://www.mologogo.com	Pull	Open	No	Yes	Yes	Yes	No						X					
Moximiti	09/26/08	http://www.moximity.com	KILLED NOVEMBER 2009			Yes						X								
MyGeoDiary	09/17/08	http://www.mygeodiary.com	Push	Open	No	Yes	Yes	Yes	Yes						X					
MyGeolog	12/10/08	http://www.mygeolog.com/	Push	Open	No	No	No	--	Yes						X	X				
Myrimis	09/04/07	http://www.Myrimis.com	Pull	Closed	No	Yes	Yes	No	Yes			X								
Now Here	03/22/08	http://www.nowhere.de/	Push	Closed	No	No	No	--	No			X								
Nulaz	04/10/08	http://www.nulaz.net/	Pull	Open	No	Yes	Yes	No	No			X			X					
Plazes	08/16/04	http://www.Plazes.com	Push	Open	No	Yes	Yes	Yes	Yes			X				X				
Pocket Life	12/16/08	http://www.pocketlife.com	Pull	Closed	No	Yes	Yes	Yes	Yes			X		X	X					
Quiro	09/01/06	http://www.myqiro.de	Pull	Closed	No	Yes	Yes	Yes	No			X			X					
Rummble	12/13/07	http://www.Rummble.com	Push	Open	Yes (Web), No (Phone)	Yes	Yes	Yes	No			X			X					
Shizzow	03/05/09	http://www.shizzow.com	Push	Open	Yes	Yes	Yes	Yes	No	X					X					
Skobbler	09/28/08	http://beta.skobbler.de/	Pull	Open	No	Yes	Yes	Yes	No					X						
Skout	01/16/09	http://www.us.skout.com	Push	Open	No	Yes	Yes	Yes	No	X					X					
Sniff	04/01/08	https://www.sniffu.com/us/	Pull	Closed	No	Yes	Yes	Yes	Yes	X		X			X					
Snikkr	05/21/09	http://www2.snikkr.net/	Pull	Open	No	No	**YES**	Yes	Yes						X		X			
Sociallight	10/19/05	http://socialight.com/	Pull	Open	No	Yes	Yes	Yes	No			X								
Sparrow	02/12/09	http://clickontyler.com/sparrow/	Push	Open	No	No	No	--	No									X		
Spot Adventures	05/21/09	http://www.spotadventures.com	Push	Open	No	Yes	Yes	No	No						X					
SpotJots	01/29/08	http://www.spotjots.com/	Push	Open	No	No	No	--	No									X		
The Grid	12/30/07	http://www.thegrid.co.za/	Push	Closed	No	Yes	Yes	Yes	No			X								
TownKing	07/04/07	http://www.townqueens.com/	Push	Open	No	No	No	--	No									X		
Trackut	10/08/08	http://www.trackut.com	Pull	Closed	No	Yes	Yes	No	No			X								
Trapster	04/01/08	http://www.trapster.com	Push	N/A	NA	Yes	Yes	No	No										X	
Tripit	06/27/07	http://www.tripit.com/	Push	Closed	No	Yes	Yes	No	No			X								
Troovy	06/10/07	http://troovy.com/bc/vancouver/	Push	Open	No	No	No	--	No									X		
Twibble	03/17/08	http://www.twibble.de/	Push	Open	No	No	No	--	No									X		
Twinkle	04/01/08	http://tapulous.com/twinkle/	Push	Open	No	Yes	Yes	Yes	No									X		
Twittelator	07/11/08	http://www.stone.com/Twittelator/	Push	Open	No	No	No	--	No	X										
WeNear	07/01/08	http://www.wenear.com/	Pull	Closed	No	No	No	--	No	X		X			X					
Whereis Everyone	07/03/08	http://everyone.whereis.com/	Pull	Closed	No	Yes	Yes	No	Yes	X		X	X		X					
WhereYou GonnaBe	04/18/08	http://www.whereyougonnabe.com	Pull	Closed	No	No	No	--	No			X								
Whrrl	10/23/07	http://whrrl.com/	Push	Open	No	Yes	Yes	Yes	No					X						
Zhiing	10/18/08	http://zhiing.com/	Push	Closed	No	Yes	Yes	Yes	No			X								

* Application also has time and location-based access restrictions

- **Creation Date** While many of the current location-based services have been relaunched, rebranded, or generally attempted to "reboot" their service, we have tried to find the most accurate date of a first public, or widespread beta launch for each of the services. Many of these dates are based on news articles, press releases, and blogs that announced the opening of the service.
- **Push/Pull** Most services use one of two approaches to location sharing, either users post their location at times they feel comfortable "checking in" to a specific place (push) or have their location stored, ideally near real-time, so that it can be requested by friends (pull). Most pull systems allow users to push their location, especially if their phone or settings prohibit automatic updating.
- **System** Most services also use one of two system models. Closed systems require users to be "friends" with each other, while an open model allows users to be requested by anyone in the system. This is separate, though not unrelated, to public sharing.
- **Accessible privacy settings** We noted whether or not the main interface allowed users to prominently see and access their privacy controls. For example, an application where one of the main tabs is labeled "Privacy" would fall under this category. An application that requires users to visit several pages or menus (e.g. Profile/Account/Settings/Privacy) does not.
- **Privacy Policy** We checked to see whether or not the website detailed their information practices (detailed in a privacy policy or included in a legal statement or terms of service). We checked this information both in August 2009, and February 2010.
- **Policy mentions location** We checked to see if the privacy policies explicitly mention location information, geographic data, etc.
- **Home page mention** We also check to see if the product/application homepages made any mention to privacy, security, user control, or something that would give users a sense of control over their information. Privacy policy links did not count.
- **Blacklist** Users are able to block specific individuals from viewing their location.
- **Per-request (explicit) permissions** Users must specifically review each location request, and decide whether or allow or deny the request prior to the location being revealed.
- **Friends Only** This whitelist-based control restricts access to users denoted as a "Friend." By default, closed systems are considered friends only.
- **Granularity** This advanced control allows users to instruct the system to provide a less detailed location to the person requesting information (e.g. "Andrew is in Pittsburgh, Pennsylvania.")
- **Group** This restriction allows users to define access based on groupings of users. (e.g. Allow everyone in the "college friends" group to view my location.)
- **Invisible** This feature may also be termed the "Private," "Only me," or "No one" setting. Users continue to send location data, but their locations are not divulged.
- **Network** This restriction allows the user to select existing communities to whom their location may be revealed. For example, user may join a geographical network or an interest-based community with whom they wish to share their location.
- **Time-expiring approval**: Several systems allow users to set a specific time frame (e.g. 1 hour) during which a link to the map of their location is "live." During this time frame, the recipient of the location message may view the map. After the expiration of this time, the link will no longer be accessible.
- **No restrictions**: Anyone is able to view the user's location.
- **Not Applicable** Privacy controls do not apply.
- **Unknown** We were unable to find information about the privacy controls.

- **Time-based rules** (not shown) Users may define durations of time and days of the week during which their location may be revealed (e.g. from 10 am to 3 pm).
- **Location-based rules** (not shown)This restriction allows users to define locations in which their location-information may be revealed. For example, users may tag a location as "Work" or select an area on a map, and their location information is revealed to anyone who requests them when they are at that location.

References

1. Best practices and guidelines for location-based services. *CTIA Wireless Association* (April 2 2008). http://www.ctia.org/business_resources/wic/index.cfm/AID/11300.
2. Mobile marketing revenue to hit $24 billion in 2013. *ABI Research* (January 14 2008). http://www.abiresearch.com/abiprdisplay.jsp?pressid=1037.
3. Wireless quick facts. *CTIA Wireless Association* (2008). http://www.ctia.org/media/industry_info/index.cfm/AID/10323.
4. ANTHONY, D., KOTZ, D., AND HENDERSON, T. Privacy in location-aware computing environments. *IEEE Pervasive Computing 6*, 4 (2007), 64–72.
5. BARKHUUS, L., BROWN, B., BELL, M., HALL, M., SHERWOOD, S., AND CHALMERS, M. From awareness to repartee: Sharing location within social groups. In *CHI '08* (April 2008), pp. 497–506.
6. BARKHUUS, L., AND DEY, A. Location-based services for mobile telephony: a study of users' privacy concerns. In *INTERACT'03* (2003), pp. 702–712.
7. BENISCH, M., KELLEY, P., SADEH, N., SANDHOLM, T., CRANOR, L., HANKES-DRIELSMA, P., AND TSAI, J. The impact of expressiveness on the effectiveness of privacy mechanisms for location sharing. Tech. Rep. CMU-ISR-08-141, Carnegie Mellon University, December 2008. http://reports-archive.adm.cs.cmu.edu/anon/isr2008/CMU-ISR-08-141.pdf.
8. BLAIS, A.-R., AND WEBER, E. A domain-specific risk-taking (dospert) scale for aduct populations. *Judgement and Decision Making 1* (2006), 44–37.
9. BROWN, B., TAYLOR, A., IZADI, S., SELLEN, A., KAYE, J., AND EARDLEY, R. Location family values: A field trial of the whereabouts clock. In *Ubiquitous Computing (Ubicomp '07)* (2007), Springer-Verlag, pp. 354–371.
10. CONSOLVO, S., SMITH, I., MATTHEWS, T., LAMARCA, A., TABERT, J., AND POWLEDGE, P. Location disclosure to social relations: Why, when, & what people want to share. In *CHI '05* (2005).
11. CORVIDA. What's plaguing your mobile social network? *ReadWriteWeb* (May 15 2008). http://www.readwriteweb.com/archives/whats_plaguing_your_mobile_soc.php.
12. FISCHHOFF, B. Acceptable risk: A conceptual proposal. *Risk: Health, Safety & Environment 1* (1994), 1–28.
13. FROMMER, D. Loopt location to update in the background on iPhone. *Business Insider* (September 4 2009). http://www.businessinsider.com/loopt-to-run-in-the-background-on-iphone-2009-6.
14. HOLSON, L. Privacy lost: These phones can find you. *New York Times* (October 23 2007). http://www.nytimes.com/2007/10/23/technology/23mobile.html.
15. HSIEH, G., TANG, K., LOW, W., AND HONG, J. Field deployment of IMbuddy : A study of privacy control and feedback mechanisms for contextual IM. In *Ubiquitous Computing (Ubicomp '07)* (2007), pp. 91–108.
16. IACHELLO, G., SMITH, I., CONSOLVO, S., ABOWD, G., HUGHES, J., HOWARD, J., POTTER, F., SCOTT, J., SOHN, T., HIGHTOWER, J., AND LAMARCA, A. Control, deception, and communication: Evaluating the deployment of a location-enhanced messaging service. In *UbiComp 2005* (2005), Springer-Verlag, pp. 213 – 231.
17. JUNGLAS, I., AND WATSON, R. Location-based services. *Communications of The ACM 51*, 3 (March 2008), 65–69.
18. KELLEY, P. G., HANKES DRIELSMA, P., SADEH, N., AND CRANOR, L. F. User-controllable learning of security and privacy policies. In *AISec '08: Proceedings of the 1st ACM workshop on Workshop on AISec* (2008), ACM, pp. 11–18.
19. KHALIL, A., AND CONNELLY, K. Context-aware telephony: Privacy preferences and sharing patterns. In *CSCW '06* (2006).
20. KIM, M., FIELDING, J. J., AND KOTZ, D. *Risks of Using AP Locations Discovered Through War Driving*. Springer Berlin / Heidelberg, 2006, pp. 67 – 82.
21. LEDERER, S., MANKOFF, J., AND DEY, A. K. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI '03* (2003), no. 724-725.
22. MALHORTA, N., KIM, S., AND AGARWAL, J. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information Systems Research 15*, 4 (2004), 336–355.
23. MCCARTHY, C. The mobile social: Not ready for prime time? *News.com* (February 13 2008). http://www.news.com/8301-13577_3-9870611-36.html.
24. PATIL, S., AND LAI, J. Who gets to know what when: Configuring privacy permissions in an awareness application. In *CHI '05* (2005), pp. 101 – 110.
25. RAVICHANDRAN, R., BENISCH, M., KELLEY, P. G., AND SADEH, N. M. Capturing social networking privacy preferences: Can default policies help alleviate tradeoffs between expressiveness and user burden? In *Proceedings of 2009 Workshop on Privacy Enhancing Technologies* (August 2009).
26. ROBERTS, P., AND CHALLINOR, S. IP address management. *BT Technology Journal 18*, 3 (July 2000), 127–136.
27. SADEH, N. *M-Commerce: Technologies, Services, and Business Model*, 1st ed. Wiley, 2002.
28. SADEH, N., HONG, J., CRANOR, L., FETTE, I., KELLEY, P., PRABAKER, M., AND RAO, J. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing* (Forthcoming 2008).

29. SMITH, I., CONSOLVO, S., LAMARCA, A., HIGHTOWER, J., SCOTT, J., SOHN, T., HUGHES, J., IACHELLO, G., AND ABOWD, G. Social disclosure of place: From location technology to communication practices. In *Pervasive '05* (2005), Springer-Verlag, pp. 134 – 151.
30. TSAI, J. Y., KELLEY, P., DRIELSMA, P., CRANOR, L. F., HONG, J., AND SADEH, N. Who's viewed you?: the impact of feedback in a mobile location-sharing application. In *CHI '09: Proceedings of the 27th international conference on Human factors in computing systems* (New York, NY, USA, 2009), ACM, pp. 2003–2012.