Noname manuscript No.
(will be inserted by the editor)

Mark Assad, David Carmichael, Judy Kay and Bob Kummerfeld

Giving users control over location privacy

A study of user choices in release of personal information

the date of receipt and acceptance should be inserted later

Abstract Pervasive computing research makes it feasible to model people's location. However, there are challenges in effective *sharing* of location information, with support for user control, enabling people to choose the location information available, at the same time, providing information that is useful. We describe our exploration of these issues, in our MyPlace Locator, a system which has been operating for several months to report people's location within a closed community. It operated with complete disclosure of people's location. Because it is based on the accretion/resolution modelling system which supports a range of "resolvers" to provide different levels of privacy, we wanted to gain an understanding of how people would want to make use of such privacy control. Moreover, we wanted to see how this might differ between people who had extensive experience of MyPlace Locator and those who had none. This paper describes a study of the ways that people choose resolvers that apply different privacy levels to different groups of people. We conclude that the preferences chosen by the long term users of the system had a different character from the others, and that there is a range of classes of "resolvers" that seem to be valuable for defining privacy control for location information.

1 Introduction

The vision of pervasive computing is based upon the availability of information as it is needed, in the form that meets the needs and preferences of the individual. To date, one of the dominant themes of pervasive computing research has concerned modelling of location, largely dealing with the technical issues of collecting sensor and other information that can contribute to modelling a person's location [1].

Some research has been cognisant of the need to consider people's concerns about privacy [2]. So, for example, the BlueStar system [3] addresses privacy issues by keeping the high-resolution location information under the user's local control. There has also been some exploration of people's attitudes to the management of their location information [4]. However, there has been no work that systematically explores user control of sharing their own location information with others and the ways that people have used it. It is timely to explore these challenges.

Our MyPlace Locator service has been in use for two months. Its location modelling is based on Bluetooth proximity sensors and system activity sensors. It has been restricted to a small community of users. As a prelude to broader use, we wanted to improve user control. We wanted inform this step in two major ways. First, we wanted to understand just how that location information is used so that this would inform the design of information displays. This is important for the design of personalised control mechanisms: we want to ensure that we are aware of the uses that people make of the location information when it is presented uniformly for all users.

In addition, we wanted to seek the views of our existing users about the ways that they would like to be able to restrict their location information. We wanted to explore the design of an interface for people to specify their preferences for personalised control of the display of their location. In light of previous work that highlights the challenges of such interface design, for example [5], we wanted to study how people cope with an interface for specifying this personalisation.

The next section summarises related work. In Section 3, we introduce the MyPlace Locator system. Section 4 describes our study of people's personalisation preferences for that location information. Section 5 has our conclusions.

Smart Internet Technology CRC partially supported this project.

School of Information Technologies
University of Sydney, Australia
Tel.: +61-2-9351-5711
Fax: +61-2-9351-3838
E-mail: {niu, judy}@it.usyd.edu.au

2 Related Work

Location modelling has been a major focus of work in pervasive and context-aware computing, for example [6, 1,7,8]. Much of that work has acknowledged the importance of privacy and user control. A number of systems have noted that privacy was one of their architectural goals [9,10]. Indeed, at one extreme, Hazas and Ward [10] proposed only holding the location information on the user's own device. There is also a developing set of privacy principles for managing personal data in ubiquitous computing contexts [11]. These highlight the importance of the good interfaces that are essential if these principles are to be put into effect: it will be challenging to create such interfaces based on previous relevant experience, for example, in relation to P3P [5] and Lederer et al [12].

There has been some work about the ways that people make use of location information about other people. For example, ActiveMap [13] and the location display based upon the Olivetti Active Badge [6] show where people are. One illuminating study was conducted by Iachello et al. [14] over two weeks. Their eleven participants, in family groupings, made use of a location-aware mobile messaging service. Participants valued control of the release of their the location information, including being able to give inaccurate information. This gives some insight into the ways that people want to control release of their location information but not on how people make use of such information about others.

There is some indication of the use of location information for the "ActiveMap" [13] project which displayed pictures of users' faces on a building map. Location was determined by infrared badges and the map was available from both an information kiosk in a busy hallway, and as a desktop application, with the former getting far more use, by those within the department and outsiders. Some users raised privacy concerns, and the authors noted the potential benefits of being able to obscure one's location, for example leaving one's badge at their desk.

The issue of controlling location disclosure was explored by Lederer et al.[15] in an internet-based questionnaire completed by 130 people. They were asked to choose levels of released information in two hypothetical situations, working lunch and social evening, and for four classes of recipient, a spouse elsewhere, employer elsewhere, a nearby stranger and a nearby merchant. They found the recipient was more important than the situation. Notably this information did not come from actual use of a system that provided location information.

Patil and Lai [16] report a study of people's predicted privacy preferences for "mySpace", which allowed people to ask about others' location. Thirty six participants were asked how they would configure "mySpace", in terms of sharing of location, availability, calendar information and instant messaging (IM). This study indicates a preference for defining privacy preferences in terms of groups, such as "family" or work "team". Significantly, this work, like Lederer et al.[15] discussed above, involves hypothetical preferences as the participants had not actually used the system.

In summary, location is an important aspect of ubiquitous computing and the importance of privacy and control of release of location information is widely recognised. There have also some been studies of potential interfaces for managing release of privacy information and of people's predictions of how they might feel about release of their location data in systems that they have never used. However, there has not been a study of how people want to use location information about others. Nor has there been a study of the privacy preferences selected by people who have actually used a system that provides location information. Clearly, these interact: people need to be able to control the release of their location information and, at the same time, we need to understand how this interacts with the quality of location information that is needed if it is to be useful. It is this pair of inter-related issues that we explore in the remainder of this paper.

3 System Overview

The main interface to MyPlace Locator is a web page that allows users of the system to view their own and other people's location. This section describes the ways that MyPlace Locator models users' location and the way that it is displayed at the main MyPlace Locator web page.

MyPlace Locator uses two forms of evidence about people's location: Bluetooth Phones and Computer Activity Sensors. We chose these because both are readily available without any special hardware. This means it is straightforward for people to join the system by registering their Bluetooth-enabled phone, or installing a small sensor program on their computer. We have sensors in 16 locations within our building. Each of these constantly scans for any Bluetooth devices within the coverage area of a few nearby rooms. Computer system activity sensors register how long it has been since the user last used the mouse or keyboard. Both evidence sources have their limitations: a Bluetooth device may be left on a user's desk, or turned off when they have gone to another location.

MyPlace Locator has been designed to be extensible in its source of evidence about location. It is simple to add arbitrary new location evidence sources as they become available. For example, we have recently added detectors for Nike+ shoe sensors.

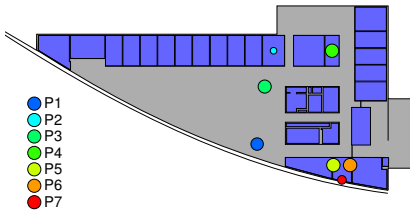
The reasoning about location is based on accretion/ resolution [17] and this allows a system to *accrete* arbitrary information about users and then to apply one of a selection of *resolvers* to interpret it. MyPlace Locator determines a user's current location through either sensing a Bluetooth device or by monitoring activity on a

computer. If both are available and conflicting, the *resolver* deals with this to determine a location value. In the current implementation, we use a simple Point resolver [17].

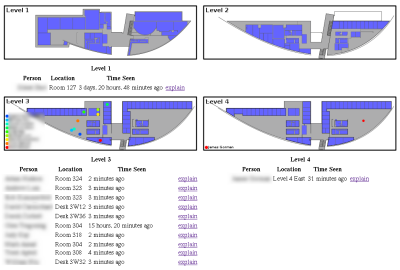
MyPlace Locator provides details of the location of all the people who have registered to this service. It has been running for two months and the current interface is shown in Figure 1. This displays the four floors of a building, with a list of the registered users either in the building or elsewhere. The enlarged display of a single wing at the left shows that the display includes a list of the people whose last location was determined to be on that wing. This is the anonymised list associating people's names with a coloured dot. That dot appears also on the map at the last location for that person. The size of the dot indicates the freshness of the data: so if there is recent evidence that the person was at this location, the dot is larger. As the most recent data becomes older, the dot shrinks.

The blurred location data at the left of the figure has four pieces of information for each person: their name, their most recent location, the freshness of the information and a link to an explanation.

The link labelled *explain* takes the user to a page with the full details of the last ten pieces of location evidence. So, for example, for an activity sensor, it would show the person, the location suggested by the evidence, how long ago the evidence was collected, the event type that created the evidence and the details of the computer that collected the evidence. If a person saw that their location was incorrect, they could use this information to check why it occurred.



(a) Detailed view of a single wing.



(b) Screen shot of the web interface.

Fig. 1 An example of a map that plots the location data collected by the MyPlace Locator on a floor plan of our building.

4 Study of use of location models

MyPlace Locator has been running within a closed group of 20 tracked users for the past two months. In this time it has been accessed 2747 times. People have used the system from both within the office building, and from home.

Users can only participate in the system if they explicitly register for it. Then, they need to take explicit action to associate each new evidence source with their own location model. So, for example, for each machine on which they want to run an activity sensor, they needed to install the sensor. Similarly, for each Bluetooth enabled device that they wanted tracked by the system, they needed to explicitly register that device. This means that the people who have their location modelled in the MyPlace Locator system had to opt-in to do so and had to then act to establish each source of evidence about their location. So, at one level, the users of MyPlace Locator had complete control of the evidence that goes *into* their location models.

However, when people joined MyPlace Locator, they were aware that they had no control over the release of the information about their location. Certainly, the system is password protected. But there is no process for consulting people before new users are added and so those who have chosen to participate in MyPlace Locator have no control of the *release* of location information.

The MyPlace Locator location modelling is based on the accretion/resolution representation [17] [4]. This was expressly designed for flexible control of the modelling and use of the information in the models. The mechanism for controlling release is the "resolver", which is responsible for interpreting the evidence available to return a value. Different resolvers may return different values. So, for example, one resolver may report Bob's location as a fine grained value, such as "common room"; another resolver may report his location as "at work".

Our goal is to enable people to choose how location information is revealed to other users of the system. To explore this, we first asked three existing users of our system to consider a prototype interface for expressing preferences for location information release. This, combined with previous literature, such as [12,13,14,16] informed our design of an interface for controlling release of location information.

In terms of the underlying representation and mechanisms, this interface enables a user to define which resolvers should be used for releasing their location to different people.

The interface is shown in Figure 2. As the instructions at the top of the screen indicate, we designed this to

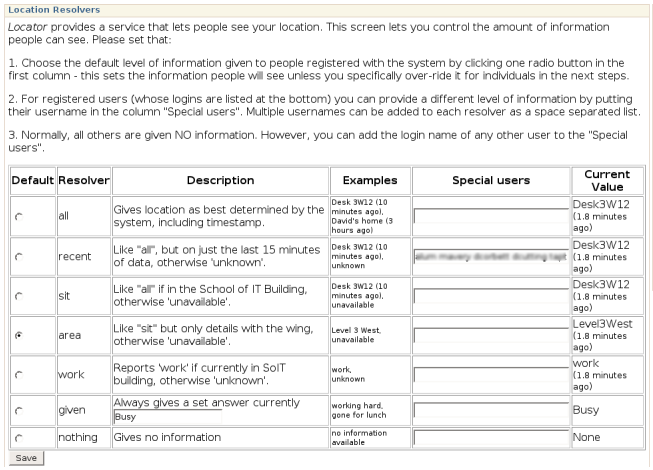


Fig. 2 Interface for selecting the resolver to be applied to each person.

allow three classes of control, starting from a very general policy and becoming increasingly specific to particular people. These levels correspond to the three numbered stages of using the interface, as described at the top of the screen.

First, the user chooses the *default* level of information to be provided to registered users. This aspect of the design was to ensure that it was easy for a person to set up a very simple policy that could be applied to most people. The user does this by clicking a button in the leftmost column.

For our particular system, this offers seven choices of resolver (or privacy policy), listed with the most liberal policy first and becoming increasingly vague about the user's location. The first option *all* corresponds to the system as it had operated for several months at the time of this study, releasing the finest grain and complete details of each user's location to all users of MyPlace Locator. Each of these policies is explained in the third column of the interface. In the figure, the fourth option "area" has been selected. This reports the user's location only at the level of the wing of the building if the user is in the building and, if they are detected elsewhere or there is no recent evidence about them, their location is provided as "unavailable".

In Step 2, the user can specify people who should be provided with a different level of information. To do this, they paste in the logins under "Special users". In the figure, the user has chosen several people who should get the second most open form of location information, *recent*. This list has been blurred for the image in this paper to obscure the names of the actual people selected. The *recent* resolver is identical to the *all* except that it only reports the user's location if the most recent evidence about it is from the last 15 minutes. This level of control is that it does not release older information and there are two reasons for this. Firstly, in discussions among users of MyPlace Locator, some had indicated that concern about people seeing old data had meant that they did not register some evidence sources. A second reason is that the users of MyPlace Locator had indicated that the main uses they made of the system only required recent information. For example, they sometimes wanted to find a particular person to discuss some work. Or they wanted to see who was present to have coffee. Since these uses of location only require the user's recent location, we designed the *recent* resolver to support that level of control.

The actual choices shown in the figure are representative of one approach to managing privacy. The default level of information released is rather restricted, indicating on the wing of the building but there is a list of individuals who are allowed the more detailed *recent* location.

The third step, or level of control, allows users to add other people, beyond the registered users.

Each resolver available corresponds to one row of the interface. To help people understand the options available, there are two forms of explanation. Each row has a short description of that option. In addition, there are also some illustrative examples and, in the rightmost column, the current value for this user is shown, as suggested in [16]. Not shown in the figure, there is also a column at the right with a list of all the registered users. This makes it easier to paste these into the *Special users* column.

The choice of the particular set of resolvers designed, and hence the options made available at this interface, was motivated by previous work [12,13,14,16]. So, for example, [16] and [12] indicate the value of allowing users to assign a certain policy to a group of users. We have discussed the reasoning behind the design of the resolvers for *all*, *nothing* and *recent*. The three resolvers *sit*, which reports exact locations within the building but no other information, *area* which reports location accurate to the wing of the building and *work* which indicates only if the user is at work, constitute a series of decreasing detail in the location reported. The remaining option, *given* enables the user to specify a fixed string that is to be given as the location: in the figure, we see it as the default value, *Busy*. The user could set the string to be a particular location.

Twenty-four users used this interface to show their preferred presentation of location information. We observed them using the interface, to gain usability information and to gain feedback on any other aspect that they identified. Table 1 summarises the results. They were asked to think aloud as they used the interface. This provided information both about usability challenges and about their reasoning as they used the interface.

The ten users in the top section were the registered and currently active users of MyPlace Locator: those below the line are users who had just been introduced to it. All participants were either students or staff at the

School of Information Technologies where the majority of the location sensors for MyPlace Locator are located.

The first column shows the user identifier. The second column, labelled *C*, shows the number of times the participant changed their preferences. These changes were made as participants reconsidered their choice of default or recalled additional users to specify separately. P18 and P24 made four changes as they reviewed their choices.

The third and fourth columns indicate the number and type of sensors that were registered for each participant: *B* shows whether the participant had a registered Bluetooth device and *S* shows the number of systems where a sensor had been installed for the participant. The next column shows the default choice of resolver made by each participant. The remaining columns indicate the number of people that a participant listed in the interface as *Special users* who should be provided with a different resolved location value. So, for example, P6 chose a different resolver for three people, allowing all others to see the value from the default resolver they had chosen, *sit*.

User	C	B	S	default	all	recent	other	none
P1	1	1	1	all	-	-	-	
P3	1	1	2	all	-	-	-	
P4	1	1	2	all	-	-	3	
P5	1	1	2	all	-	-	-	
P7	1	-	2	all				
P6	2	1	2	sit	3	-	-	
P9	1	1	2	recent	15	-	-	
P2	1	1	2	area	12	-	-	-
P10	2	1	2	area	-	11	-	-
P11	1	1	2	recent	-	-	3	1
P12	2	1	2	nothing	-	-	-	
P13	1	1	-	all	-	-	-	
P14	1	1	-	all	2	-	-	-
P15	1	1	-	recent	2	-	-	-
P16	1	1	-	sit	5	-	-	-
P17	1	1	1	recent	-	-	-	-
P18	4	1	2	all	-	-	-	-
P19	1	-	1	area	1	-	1	-
P20	2	-	1	all	-	-	-	-
P21	1	-	2	recent	-	-	-	-
P22	2	-	1	recent	-	-	-	-
P23	1	-	1	sit	-	-	-	-
P24	4	-	1	area	3	-	2	-
P25	2	1	2	work	-	-	-	-

Table 1 A summary of users' selection of resolvers.

We discuss the results from the experienced users first. All these people registered with the system when there was no choice about the information disclosed. They generally have more sensors. All but one had a Bluetooth phone and all but one had system sensors both at home and at work. Five chose 'all' as the default and two each chose 'recent' and 'area'. Even the 'sit' is still quite open, revealing all information available from sensors located at work.

Notably, P2 and P9 chose a more restricted default and then listed most of the currently registered users for *all* information. They explained that they were happy to release their location to the current users who they knew: however, they were concerned about new people joining the system.

Due to space limitations, the table coalesces the uses of the the third to sixth options available in the interface under the column headed *other*. P4 applied the *sit* resolver to three people and P19 did this for 1. P11 chose the *area* resolver for three people. P22 restricted two people to the *work* resolver. Notably none of the users opted for the fixed string *given* resolver.

The new users had a somewhat more diverse set of choices. Four chose 'all" and four more chose "recent", with two choosing to restrict location to the "building" and two restricting it to the "area" in the building. One chose the restrictive "work". One chose to reveal no information. When queried about it he stated that he got not benefit from revealing his location to others, even if they revealed theirs - if they wanted to find him they could come look at his desk, and if he was at home then he did not want to share that. This is exactly the prisoner's dilemma described in [18].

5 Discussions and Conclusion

This paper has reported a study of users choosing a set of policies for the management of *release* of information about their location by a sensor-based location modelling system and the MyPlace Locator interface. This is important on several levels. First, it will inform the design of interfaces that enable users to control the privacy of information in their own user models. this is especially for the case of components within the model like location, which are potentially sensitive but, at the same time, there is potential benefit in sharing the information. In the case of location, allowing others to access this at some level can facilitate social interaction and work.

For our work based on the accretion/resolution representation for user modelling, this work is important as we designed the interface as one means for the user to select resolvers to be used depending upon the person to whom the location is reported.

The design of our interface, based on both previous work and the input of the group of people who had been using MyPlace Locator for several months, had three main levels. The first, default, appeared to serve the needs of about half the participants: eleven of the twenty-four chose to simply rely on the default resolver.

About half the users chose the resolvers *all* and *recent*, which represents a protection of historic location but is otherwise as accurate as *all*. When we take account of both the default chosen and the explicit choice for selected people, these two resolvers accounted for all the choices for thirteen of the participants. Within this group, there is variability in the way they made these

choices. Nine chose *all* as the default and one participant (P14) then listed two people for the same resolver.

There were four strategies for selecting the set of resolvers to apply. The simplest, relying on a single default resolver, was chosen by thirteen participants, four being long term users of MyPlace Locator and nine new users. (In addition, P14 made choices that had the same effect.) Two participants chose a more open resolver for the default and then identified individuals who should have more information and two of these participants were the experienced MyPlace Locator users. Six participants used the opposite strategy, with the default more restricted and then one other, more open resolver for nominated people: four of these participants were the regular MyPlace Locator users. The remaining two participants (P19 and P24), both new users, chose a somewhat restricted default and then used two other resolvers to selectively control information release, with P19 giving one person more and one less than the default and P24 giving both more, but different levels.

Both the actions of the participants and their response to the interface indicate that the choice of resolvers offered was acceptable. Also, the mechanism for choosing resolvers seemed to be generally understood and usable.

There are some limitations in our study. Because of the nature of the location information, we needed to recruit participants who used the building with the Bluetooth infrastructure for supporting location modelling. This means that the participants are all computer scientists. In future work, we need to evaluate the usability of the interface for a broader range of users. This work also made use of a fixed set of resolvers. These appear to have been found useful and sufficient by our participants but in future work, we need to explore generalisations of the resolvers so that the approach can be readily mapped to other buildings and locations. The interface we evaluated was designed for small groups of users, a reasonable decision for a single workplace. However, we still need to evaluate our interface approach for larger numbers of people. Taking account of these limitations, this paper makes a contribution in presenting and evaluating an interface for users to select resolvers for use in releasing their location information, with support for differential privacy levels to be applied to different people. This work is also important for its evaluation based on users who had months of experience of MyPlace Locator as well as new users who were predicting how they would want it to operate.

Acknowledgements This work is partially funded by the Smart Internet Technology CRC.

References

1. Hightower, J., Borriello, G.: Location systems for ubiquitous computing. IEEE Computer **34** (2001) 57–66 1, 2
2. Beresford, A.R., Stajano, F.: Location privacy in pervasive computing. IEEE Pervasive Computing **2** (2003) 46–55 1
3. Quigley, A., Ward, B., Cutting, D., Ottrey, C., Kummerfeld, R.: Bluestar, a privacy centric location aware system. In: IEEE Position, Location and Navigation Symposium. (2004) 1
4. Assad, M., Carmichael, D.J., Kay, J., Kummerfeld, B.: Active models for context-aware services. Technical Report TR 594, The School of IT, The University of Sydney, Australia (2006) 1, 4
5. Ackerman, M., Cranor, L., Reagle, J. In: Privacy critics: UI components to safeguard user' privacy. ACM (1999) 1–8 1, 2
6. Want, R., Hopper, A., Falco, V., Gibbons, J.: The active badge location system. ACM Transactions on Information Systems **10** (1992) 2
7. LaMarca, A., Hightower, J., Smith, I.E., Consolvo, S.: Self-mapping in 802.11 location systems. [19] 87–104 2
8. Otsason, V., Varshavsky, A., LaMarca, A., de Lara, E.: Accurate gsm indoor localization. [19] 141–158 2
9. Priyantha, N., Chakraborty, A., Balakrishnan, H.: The cricket location-support system. In: Proceedings of the 6th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '00). (2000) 2
10. Hazas, M., Ward, A.: A high performance privacy-oriented location system. In: Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom), (2003) 216–233 2
11. Langheinrich, M.: Privacy by design - principles of privacy-aware ubiquitous systems. In: UbiComp 2001: 3rd Intl. Conf. on Ubiquitous Computing. (2001) 273–291 2
12. Lederer, S., Hong, J., Jiang, X., Dey, A., Landay, J., Mankoff, J.: Towards everyday privacy for ubiquitous computing. (2003) 2, 4, 4
13. McCarthy, J.F., Meidel, E.S.: Activemap: A visualization tool for location awareness to support informal interactions. In: Proceedings of the International Symposium on Handheld and Ubiquitous Computing (HUC 99). (1999) 158–70 2, 4, 4
14. Iachello, G., Smith, I.E., Consolvo, S., Abowd, G.D., Hughes, J., Howard, J., Potter, F., Scott, J., Sohn, T., Hightower, J., LaMarca, A.: Control, deception, and communication: Evaluating the deployment of a location-enhanced messaging service. In: Ubicomp. (2005) 213–231 2, 4, 4
15. Lederer, S., Mankoff, J., Dey, A.K.: Who wants to know what when? privacy preference determinants in ubiquitous computing. In: CHI '03 extended abstracts on Human factors in computing systems, (2003) 724–725 2
16. Patil, S., Lai, J.: Who gets to know what when: configuring privacy permissions in an awareness application. In: CHI '05: Proc. SIGCHI conference on Human factors in computing systems, New York, NY, USA, (2005) 101–110 2, 4, 4
17. Carmichael, D., Kay, J., Kummerfeld, R.: Consistent modeling of users, devices and environments in a ubiquitous computing environment. User Modeling and User-Adapted Interaction **15** (2005) 197–234 3, 4
18. Mansley, K., Beresford, A.R., Scott, D.: The carrot approach: Encouraging use of location systems. In Davies, N., Mynatt, E.D., Siio, I., eds.: Ubicomp, (2004) 366–383 4
19. Beigl, M., Intille, S.S., Rekimoto, J., Tokuda, H., eds. In Beigl, M., Intille, S.S., Rekimoto, J., Tokuda, H., eds.: UbiComp 2005: Proc. 7th Intl. Conf. on Ubiquitous Computing, Sept 11-14, 2005. Volume 3660 of LNCS., Springer (2005) 7, 8