A Lightweight Approach to Managing Privacy in Location-Based Services

Tom Rodden[1,] Adrian Friday[2], Henk Muller[3], and Alan Dix[2]

1. The School of Computer Science and Information Technology
The University of Nottingham
Jubilee Campus, Wollaton Road
Nottingham NG1 8BB
United Kingdom
tar@nottingham.ac.uk

2. Computing Department
Faculty of Applied Sciences
Lancaster University
Lancaster
LA1 4YR
adrian@comp.lancs.ac.uk,
Alan.Dix@hcibook.com

3. Computing Department
Merchant Venturers Building
University of Bristol
Bristol
BS8 1UB
Henk.Muller@bristol.ac.uk

ABSTRACT

Location-based services (LBS) and context-aware systems typically exploit the tracking of people to offer personalised services. Examples of these sorts of applications include allowing vulnerable people to summon help to their current location, providing personalised guidance, ordering a taxi and finding the nearest cash point. To provide such services, information about the users' location needs to be published to one or more service providers (possibly third party organisations.) Key factors in the acceptance of such systems are preservation of control and awareness of dissemination of this information; people using these services do not want to be under surveillance. The fundamental difference between tracking and surveillance is who is in control. There is little or no provision for access control to location information in current systems.

In this paper we offer a scheme whereby users can reveal their position to trusted parties whenever they want to, and retain control over the dissemination of their position to others. Furthermore, our scheme does not compromise the ability of the service provider to offer their services to users or gather statistical and demographic information on the systems' usage.

INTRODUCTION

During the last few years we have witnessed an increasing turn to location and positioning as an integral part of the interaction with mobile systems. Over the last decade researchers have explored how location based interaction and communication might be used to support novel interactions. Prominent examples include:

- Intelligent guides that make recommendations or provide guidance to nearby products and services, e.g. find a nearby cash point, restaurant or theatre. Indeed, many research prototypes have been constructed based on this principle [2,23].

- Intelligent environments that allow people who work and live together to be aware of the location and activities of others. A considerable amount of this work is undertaken as part of ubiquitous computing [1]. The general model is that by exploiting users' location a supporting infrastructure can provide a reactive environment that responds to the activities of those who inhabit them.

- The development of location based services that tailor services to the needs of users. For example, the ordering of taxi or delivery can exploit the location information provided by the users' technology. A number of commercial ventures are currently considering the deployment of the first generation of these systems [24].

- Applications to support the Elderly, infirm or vulnerable. These systems allow users to have their location monitored to offer a 'panic alarm' facility. Upon pressing a panic button, or perhaps triggered by observations of the person's movements (or lack of movement) an alarm condition could be signalled, summoning help. Examples of this form of tracking are seen in the work on the aware home at Georgia Tech [12] and industrial research endeavours such as Cooltown [6]. In fact, commercial GPS panic alarms are already on the market [17].

- A number of 'social' and entertainment applications including location based games that allow people to play "on the street" games [18].

This is clearly a far from exhaustive set of applications. Others include Emergency notification and dispatch; Fleet tracking; Information services such as traffic, weather, Yellow Pages; Road management by remote control; Zoned billing and numerous other possibilities.

This broad and growing class of applications relies on the ability to track and monitor the position of users and to make use of this position information to drive the application. Recent advances in wide area positioning technologies based on mobile telephony and GPS has started to encourage commercial applications that are based on user tracking and location based services on a much wider scale [3,20]. The diversity of possibilities has led to location based services currently been seen by many as one of the major growth sectors in mobile services and one of the cornerstones of future 2.5G and 3G telephony systems.

A key component in wider deployment of such services is the development of appropriate software platforms to allow decoupling of the technologies that provide location information (e.g. Cell of Origin, Time of Arrival, Angle of Arrival, Enhanced Observed Time Difference or Assisted GPS) and the value added service providers. We would also argue that development of these software platforms needs to pay close attention to the demands of users if they are to be widely accepted.

Location based systems have not emerged without some controversy both within the research communities that have produced them and society more generally [22]. Location based services and the tracking of users have raised issues of privacy much more than any other form of computer technology. It is not unusual for the general public to view technologies that make their position available to others as massively intrusive, often pointing to Orwell's vision of big brother [20] to highlight their mistrust in such systems.

The tension between the potential benefits to accrue from the location based systems and the issues of privacy these systems highlight to users, presents researchers and the developers of future platforms with a real dilemma. How do we develop these technologies in such a manner that the privacy concerns can be addressed to the satisfaction of future users?

This paper considers how we may provide support for privacy in this important class of systems. Our particular focus is on providing users with simple mechanisms that allow them to control the disclosure of their location. We present a simple framework and a generic, cheap to compute algorithm that has been designed to shift the balance of control over dissemination of location information from the service provider to the users of the system. Significantly, we believe our scheme does not compromise the needs of the service provider to be able to provide services and generate revenue through the provision of such services but does provide users with the reassurance they seek in order to subscribe to these systems.

In the next section we consider the issues of privacy that have emerged as a result of existing experiences within location based systems. We then present our general approach and illustrate how this may be used in a number of scenarios. We conclude by reflecting on the scalability and storage implications of our approach.

LOCATION AND PRIVACY

The rapid growth in ubiquitous and pervasive computing and the development of associated applications has seen a corresponding rise in privacy concerns. Understanding the various social and technical issues generating the rising concerns in privacy is itself a complex matter and it is not clear that we yet full understand the different issues involved in technology and privacy [22]. In this section we wish to consider the particular issues of privacy that surrounding location based technologies and how we may wish to design for these issues.

Perhaps the most well known studies of privacy and location surround the work undertaken by Harper et al at Xerox [8,9]. These studies highlighted the issues raised during initial experiments with the Active Badge System at two research labs. While the badges were initially met with some resistance by users and concerns of privacy where acknowledged, this was not universally the case.

The point that Harper makes is that the issues of privacy are not simply a product of the technology but rather the ways in which the technology is used. In particular, he highlights that one of the labs exploited the technology to meet a particular demand, while the purpose of the location technology was considerably less clear. These two classic studies strongly suggest that the root of the concern was not that ones location was known but that users felt unsure for what purpose this location information was being recorded and how this information was to be used.

Thus the issue of privacy for location based technology becomes one of providing the technology in manner that provides users with significant levels of control. In particular, the technology needs to give those whose location is being tracked mechanisms that allow them some understanding about and control over who is using this information. Without this control, a significant asymmetry exists in the relationship between those carrying the technology (the observed) and those who make use of the information it provides (the observer.)

This notion of asymmetry also underpins the work by Jian et al on the development of a framework for privacy within Ubiquitous computing [10]. Building upon earlier work within economics, Jian et al highlight the problematic issues that emerge from the power imbalance within "Asymmetric Information" arrangements. They suggest that the key to managing privacy within ubiquitous computing is the principle of minimum asymmetry. They define the principle of minimal asymmetry as:

"A privacy aware system should minimize the asymmetry of information between the ***data owners*** *and* ***data collectors*** *and* ***data users****, by:*

- ***Decreasing*** *the flow of information from data owners to data collectors and users*
- ***Increasing*** *the flow of information from data collectors and users back to data owners"*

At first glance realising this principle for location based systems is problematic in that we need to provide a continual stream of location values to an infrastructure in order that our context can be inferred and exploited by data users. However, without some attention to this principle, it is difficult to see how we may attend within the technological infrastructure to the concerns of privacy surrounding this technology.

Although these information limiting principles will be the main drivers of the service described in this paper, we also recognise that it is not sufficient to ensure 'privacy' in a wider sense.

One fundamental is that privacy is not maintained simply by limiting or minimising information flow. One problem is that privacy is not monotonic [6] – sometimes less information can be more private than more. For example, the press by only reporting part of a story may make it more newsworthy but less acceptable for the subject. This is also central to the early work on video privacy on which Jian et al's work indirectly draws. One of the key principles in Bellotti and Sellen [3] is feedback – knowing what is being given to whom. Maximising this feedback can be as important as minimising the outflow – even when anonymised. Indeed in Dix [6] we find an example of road usage monitoring, where counting the number of cars passing is completely anonymous; yet the data may be used to make implications about further traffic development which those actually using the road would find objectionable.

Adams, based on previous work, lists three factors for privacy, all of which emphasise the richness of the concept:

- *Information sensitivity*: This is not just a matter of private/not private, different people in different circumstance may regard the same information as more or less valuable to be private.
- *Information receiver*: Trust of the recipient is central to people's acceptance of monitoring, so (re-enforcing the feedback discussion) knowing who may use information is crucial.
- *Information usage*: Adams reflects concerns in both Bellotti & Sellen [3] and Dix [6] that the purpose of use is also critical. Indeed this is a key element of the UK Data Protection legislation.

In this paper, we do not focus on the wider concerns of information sensitivity or usage of the location information that we have highlighted. Rather, we focus on providing a simple mechanism to allow users to manage the flow of information through a simple and scaleable encoding technique.

Key to the approach we suggest is packaging location based data in a way that allows users to control who can readily understand the information. In particular, we make a separation between the location data stating a device is at a given location, the time the position data was obtained and the user the data is associated with. Our encoding focuses on providing this data in a manner that cannot be understood until the data owner has given permission. The need for this explicit communication ensures that this arrangement meets the principle of minimum asymmetry and ensures a balance of control between the person whose location is being tracked and those who would seek to use this information.

In the following section we outline the key elements of our approach and show how this simple separation allows users increased access and control over the use of their location information.

A PRIVACY ORIENTED LOCATION FRAMEWORK

Irrespective of the technologies involved in gathering and recording users' location, a system tracking location over time must record and represent three key pieces of information:

- The location of the user (in a given coordinate system)
- The time at which the location of the user was observed
- The identity of the user (a unique identifier)

Our approach to managing privacy exploits this underlying structure of location-based systems. Essentially, an observer must possess all three of these components *simultaneously* in order to know where a given user currently is with any degree of certainty.

Any single component in isolation provides very little information to an observer. For example, given the location samples in isolation the observer is merely able to determine that locations have been visited at some point in time. Since the identity relationship of the data cannot be resolved; the observer cannot know whether successive location samples belong to the same or any other user of the system. If the time relationship between the samples cannot be established, then the observer cannot dependably construct a path a given user has followed nor their speed or direction. Identity without time or location does not help our observer locate the person, just their registration with the system. The time that the samples are taken is possibly the least useful component in isolation.

Knowing two of these elements increases the amount we can know, but is still limited. Given location and identity the observer can establish all the locations visited by every user. However, without time, the path that the user has taken can only be inferred probabilistically. Significantly, assuming a reasonable number of samples, the observer cannot know which of the sampled locations the user is currently at, nor even if the location information is recent enough to be of relevance. Location and time offers the observer the ability to infer where users of the system have been. Analysis of trends in this data might yield potential paths with some degree of probability. However, without identity, the sampling interval or margin of error in the sample data, and the potential for paths to cross would limit the usefulness of this data. Lastly, identity and time taken together without location only allows the observation of the system's usage over time.

The more components an observer is able to ascertain at one time, the greater the information revealed about the user. An observer who possesses location and time and is able to affirm the user's identity using other means (correlating against other telemetry or observational data, for example) may be able to periodically establish the user's location. However, the key to establishing where our user is *at any* given time is only through knowing who the person is and having the ability to chain these measures together. In fact, the user's identity is the key to understanding this location information and controlling its disclosure. The association of identity with the other elements of location underpins our approach to the management of privacy in location-based systems.

Basic Approach

Let us start by considering the ways in which location based systems tend to be currently considered. In most approaches we can distinguish three parties in our system that correspond to the principle of minimal asymmetry outlined in the previous section:

- **The holder** *(the data owner)* is someone who carries a personal wearable device, such as a mobile phone.

- **The location service** *(the data collector)* provides a location service to the holder. The service provider can at any time establish where a holder is. This could be by means of triangulation with mobile phone devices, or through an external tracking device.

- **The third party** *(the data user)* is an organisation that makes use of the information and may provide a location-based service to the holder. It will normally obtain location data from the service provider.

Most existing arrangements are based on the location service passing location information onto the third party. (figure 1).

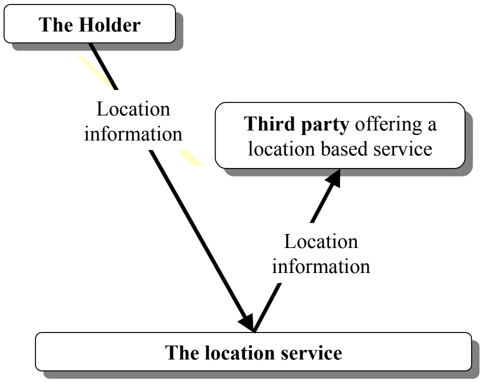

Figure 1: the current asymmetrical arrangement

Under this arrangement the holder tends not to have any control over the third parties using the location information collected by the location service and often may not be informed even that third parties are using this information. This asymmetrical arrangement significantly differs from the ideal suggested by Jian et al [10]. We wish to alter this arrangement to provide a much more symmetrical flow of information for location based systems.

Our premise is that the holders should have full control over their own location information. However, by the same token, the service provider may not want to yield total control over this location data because it has commercial value and can be sold on to third parties to provide value added services (providing the holder agrees that this is what should be done.) What is important is that this disclosure is understood by the user and that a symmetrical relationship is reached between the user and the observer.

The scheme that we propose requires that rather than storing the position and identity of each holder (c.f. the home location register in GSM), the system provider instead stores at any time a triple of the form:

(Location, Time, Pseudonym)

- The Location is a holder's location in a given coordinate system.
- The Time is the time that the holder was at that location.
- The Pseudonym is a unique number that is related to a holder for a given time interval. It is up to the holder to choose a random number **X** to be used as their pseudonym. At any given time a user may have a number of active pseudonyms.

In order to prevent collisions we must pick **X** from a suitably large space (a 128-bit number would provide ample encodings.) The number **X** must be a 'true' random number, not generated using a pseudo random sequence – note that this is not an unreasonable requirement as mobile devices should easily be able to gather entropy to seed random number generators (a process they often perform anyway since the key exchange protocols used in encryption rely on random data.)

Managing the disclosure of the Pseudonym **X** allows the holder to control the disclosure of their location information and establishes a more symmetric arrangement. The holder knows at any given time that they have given others permission to observe them by telling them the pseudonym they are currently using.

Essentially the only way for a third party to make use of the location information associated with a given holder is to enter into some form of service agreement where the mapping the between the holder's identity and the random number pseudonym is provided as part of the agreement. This more symmetrical data arrangement is shown in figure 2.

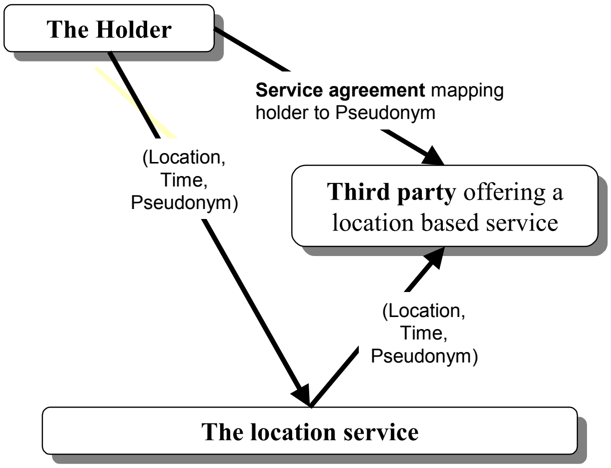
The Holder
Service agreement mapping holder to Pseudonym
(Location, Time, Pseudonym)
Third party offering a location based service
(Location, Time, Pseudonym)
The location service

Figure 2: A symmetrical location service

The holder may choose to change the random number used as the Pseudonym at any time allowing them to alter the set of third parties to who they have disclosed their location information.

Supporting location based service agreements

This basic arrangement allows the holder to establish simple location-based service agreements with third parties. For example, let us consider a simple scenario where a user (the holder) requests a taxi to their current location from a taxi service (the third party) by pressing a button on their mobile device.

1. *The mobile device will pick a pseudonym*, **X'**, and will inform the service provider that this is an active pseudonym for the holder. This will cause the service provider to log location information from the holder under **X'**.

2. *The pseudonym **X'** is provided to the third party* as part of the agreement with the taxi service. The taxi service can then query the service provider to find out the holder's location. Note that the taxi service can keep querying the position until the holder decides to change their pseudonym at which point they can no longer find any information on the holder.

3. *The holder changes the pseudonym to complete the service agreement* when the taxi collects them. Changing the pseudonym essentially revokes the taxi firm's access to their location information.

Note that this solution is elegant, because the service provider is a “trusted party”. The taxi company picks the position information up from the service provider in the knowledge that this is a genuine request.

In order to allow us to be involved in more than one service agreement at any given time we need to register our active pseudonyms with the service provider. In order to prevent unauthorized access, the pseudonym should be encrypted with a key that is provided to the third party.

In the case of our taxi example where we are dealing with a third party **T** would generate a key $K_{T.}$ We would then store pairs (**T**, Enc(K_T, **X’**)) allowing the third party to retrieve the pseudonym at will. Note that while **T** could pass on **X’** to other providers illegally, we have not revealed the user’s true identity, nor allowed access to location data other than that scoped by its association with **X’**. In a ‘real’ system, one might expect additional legal protection to further reduce the likelihood of such abuses.

Managing group service agreements

A common use of location-based system is to allow a larger group of people to track where we are. This is for example useful for people who are on their way to a meeting or across a sales team. This means that we need to consider how best to support location service agreements that involve multiple parties. One approach would be to select a pseudonym **X’** for the service agreement as we did for a single transaction, and pass it on to all people who we want to allow to track us. This will work, but only in a limited way and raises some new demands. If a day later we want to allow one more person to know where we go, but we do not want to reveal to this new person where we have been, then a new pseudonym **X”** has to be picked, which has to be sent out to all people again. In addition, a new pseudonym will have to be chosen with some regularity, in order to prevent our traces from becoming tractable.

Essentially we need to allow the location service to provide a mechanism that allows the third parties involved in a location-based service agreement to be dynamically altered. Changing the pseudonym associated with the service agreement whenever we alter the set of third parties involved allows us to manage the level of disclosure across the group involved but we need to reduce the cost of this change.

Allowing the location service to store the mapping between our active pseudonyms and those we have disclosed these to provides a low cost way to manage this process. Let us illustrate the flexible group management process with a simple example.

- We can give three groups of people A, B and C, keys K_A, K_b and K_c respectively.

- We then store pairs (A, Enc(K_A,X)), (B, Enc(K_b,X)) and (C, Enc(K_c,X)) so that these groups can, on demand, retrieve the holders latest value for X, allowing them to find out where we are.

- If we ever want to change the pseudonym associated with the service agreement, we will simply update the encrypted pseudonyms at the service provider, allowing all people to retrieve our new pseudonym. At any time we can revoke permissions to a third party by changing the pseudonym and not updating the encrypted values within the stored pair for that party.

The main aim of our approach has been to develop an arrangement for location based services based on a more symmetrical flow of information, allowing the user some control over the dissemination of their location information. We have done this by making the holder a key member of any location service agreement. In order to be able to track the location of a user, a third party needs to be given an active pseudonym from the user. This means that the data owner has control over the disclosure of his location information to third parties and users may consequently be more likely to accept these forms of technology.

SCALABILITY AND DEPLOYMENT

In order to support our system, the location service will have to store all the location triplets and be able to update holder’s pseudonyms when required. In addition, it should provide the encryption service for stored pseudonyms. It is reasonable to question why the service provider would wish to provide this registration service, and whether this service can be provided in a scalable manner.

We estimate that the amount of work to be performed is minimal; only when the mobile device communicates with the service provider is there any work that needs to be performed. Data storage overhead is minimal, consisting of a couple of bytes per location sample, since only differences from the previous signal need to be stored. Precise location estimates requiring more computations can be computed on demand, for example when the taxi is about to pick someone up.

Importantly, these services do not have to be provided for free. Text messages are charged between £0.05 and £0.10, and are very popular, and it would not be unreasonable to charge holders a nominal fee, say £0.01, for changing their identity and managing the service level agreement. There is a value for holders to be anonymous when they use location-based services, so we recommend combining these charges transparently into the cost of the service itself. In addition, service providers can charge third parties a nominal fee for providing location information.

Because all the data is stored in anonymised form, the service provider can sell data off to third parties without fear of compromising the subscribers. For example, pure location information is useful in identifying hot spots, popular traffic routes, and utilisation of services. Tracks of data can be used by recommender systems for data mining purposes without requiring precise identity. If they choose, a person can supply a non-anonymous track of data in order to obtain a precise recommendation.

As this information is provided in aggregate form, it reduces the threat of compromising the privacy of any individual. However, while aggregate information is clearly a lot less sensitive than personal information it still requires some care. First, it may be possible to reconstruct individual data from aggregate data. This has been demonstrated to be a problem in census data which in many countries is publicly available.

For example, you may be able to ask for the age distribution in households in a particular area of a town. By asking multiple queries of this sort it can be possible to recreate the raw data. As a simple example, imagine there were only three houses (A,B,C) and you obtained the average of A&B, B&C and A&C, it is then easily possible to find the individual household data. This possibility to compromise statistical data has been widely studied but can be solved by randomly perturbing the summary data [12].

Even where the aggregate data does not allow individual data to be recovered, it may be unacceptable to the original data subjects depending on the purpose to which it is being put. This is exactly the case in the example already cited from [6]: Imagine a parent driving their child a short distance down a busy road to school each morning because the road is too busy for the child to walk. Their journeys add to the recorded traffic usage and lead the planning authority to increase the size and speed of the road – exactly the opposite of what the parents would want.

How to protect against data mining attacks or miscommunication of the usage of location data is outside the scope of this paper. However, introducing statistical variance to further anonymise location samples is not incompatible with our approach. We have also assumed in our target application domain that the user is well aware of how their location data is to be used (e.g. by personally opting-in to specific, well understood services.)

RELATED WORK

The use of pseudonyms to protect identity in location based systems in not new. Hauser and Kabatnik [10] as part of the NEXUS project [18], suggest a scheme involving virtual identities (VIDs) as principles which are similar to our pseudonyms. The scheme, based on public key encryption differs from our scheme in that VIDs are assumed to be long lived, and thus trust relationships are established using digital certificates. The NEXUS system can support the notion of 'area queries' in addition to the location of individuals.

Our system is significantly more lightweight than that proposed by Hauser and Kabatnik, and differs fundamentally in that our pseudonyms are completely transient.

Leonhardt and Magee [15] propose a scheme in which identity can be protected through a sequence of chained idempotent filters governed by a rich formal policy language. In their scheme policies governing access control, visibility and anonymity may be stated allowing potential implementation in a distributed fashion. Policies may be specified over individuals or groups of users. Our approach does not preclude the use of such policies to control the dissemination of pseudonyms and control contract negotiation with location based service providers.

Kesdogan et al [13] propose a method in which temporary pseudonymous identities are used to protect the identity of users in the GSM system. A Pseudo-Mobile Subscriber Identity (PMSI) is assigned by a Home Trusted Device (HTD). The user registers with the GSM using their PMSI and the location of the mobile terminal is associated with the user's pseudonym. When an incoming phone call occurs, the real identity must be revealed to allow placement of the call. To solve the potential availability problem the HTD function may be delegated to a trusted third party. In this approach, the pseudonyms are changed synchronously at regular intervals. Partial pseudonyms are distributed across a group of trusted parties to prevent inference of links between the pseudonyms.

A central tenet of our approach is allowing the user to determine when their pseudonymous identity is changed, a key different of our approach is thus that pseudonym management is assumed to be controlled on the user's end-terminal. We have not as yet specifically aimed to address issues of badly behaved third parties who collaborate to try to affirm our identity or contiguous movements – such attacks are difficult however as the user can change their pseudonym at will and (with the group enhancement we suggest) limit the distribution of this new identity.

SUMMARY

In this paper we have proposed an arrangement for location based services that provide users access to location based services while providing mechanisms that provide them with some protection of their privacy. Key to our approach has been arranging the service in such a manner that facilitates user control over disclosure of their location information.

In order to achieve this we have adopted the principle of minimal asymmetry suggested by Jian et al [10] and structured recording of location information in such a way that third parties who wish to exploit location information for a given user need to reach a service agreement in order to have full access to the location based information.

The suggested arrangement is designed to be both simple to implement and to be readily understood by end users. It is important that the model provided to the end user is readily comprehensible in order to provide the level of reassurance needed to encourage the take up of location based systems, given the current resistance to this class of system.

REFRENCES

1. Abowd, G.D. and Mynatt, E.D, Charting Past, Present, *and Future Research in Ubiquitous Computing*, in ACM Transactions on Computer-Human Interaction, Vol. 7, (1), 2000, pp. 29-58.

2. Adams, A. and Sasse, M. A (1999a) “Privacy issues in ubiquitous multimedia environments: Wake sleeping dogs, or let them lie?” in Proceedings of INTERACT’ 99, Edinburgh. pp. 214–221

3. ARC Group, “Over 40% of Operators’ Mobile Data Services Revenues in 2007 will be Location Based”, Survey Report, 19th August 2002, London, U.K. http://www.arcgroup.com

4. Bellotti, V. and Sellen, A. “Design for privacy in ubiquitous computing environments.” In Proc. of the European Conference on Computer-Supported Cooperative Work, 1993. pp. 77–92.

5. Cheverst, K., Davies, N., Mitchell, K., Friday, A. and Efstratiou, C. Developing a Context-Aware Electronic Tourist Guide: Some Issues and Experiences. in Proceedings of Chi ‘2000, ACM Press, The Hague, Netherlands, 2000, 17-24.

6. Dix, A. J. (1990). “Information processing, context and privacy.”, Human-Computer Interaction - INTERACT’90, Ed. D. G. D. Diaper G. Cockton & B. Shakel. North-Holland. pp. 15–20.

7. Cooltown http://cooltown.hp.com/cooltownhome/

8. Harper, R. 1992. Looking at Ourselves: An Examination of the Social Organization of Two Research Laboratories. *Proc. ACM Conf. Computer-Supported Cooperative Work CSCW’92* (Toronto, Ontario), 330-337. New York: ACM.

9. Harper, R., Lamming, M. & Newman, W. 1992. Locating Systems at Work: Implications for the Development of Active Badge Applications. *Interacting with Computers*, 4 (3), 343-363.

10. Hauser, C. and Kabatnik, M., “Towards privacy support in a global location service”, Proceedings of the IFIP Workshop on IP and ATM Traffic Management (WATM/EUNICE 2001), pp. 81-89, Paris, September 2001.

11. Jiang X., Hong J, Landay J “ Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous computing” in proceedings of Ubicomp2002, LNCS, 2498, Springer Verlag, pp 176-193.

12. Jonge, W.d. (1983). “Compromising statistical databases responding to queries about means.” ACM Trans. on Database Systems, 8(1) pp. 60–80.

13. Kesdogan, D., Reichl, P., Junghärtchen, K., “Distributed Temporary Pseudonyms: A New Approach for Protecting Location Information in Mobile Communication Networks”, Proceedings of the 5th European Symposium on Research in Computer Security (ESORICS 98), Springer, Louvain-la-Neuve, September 1998.

14. Kidd, Cory D., Robert J. Orr, Gregory D. Abowd, Christopher G. Atkeson, Irfan A. Essa, Blair MacIntyre, Elizabeth Mynatt, Thad E. Starner and Wendy Newstetter. "The Aware Home: A Living Laboratory for Ubiquitous Computing Research" In the Proceedings of the Second International Workshop on Cooperative Buildings.

15. Leonhardt, U., Magee, J., “Security Considerations for a Distributed Location Service”, Journal of Network and Systems Management, Vol. 6, No. 1, September 1998.

16. Location based Services Portal http://www.lbsportal.com/

17. Magnavox MobilePal+GPS http://www.mobile911alarms.com/MobilePAL/MobilePAL_GPS.htm

18. NEXUS – An Open Global Infrastructure for Spatially Aware Applications, http://www.nexus.uni-stuttgart.de

19. Nicklas, D,. Pfisterer, C. Mitschang, O, “Towards Location-based Games “ Proceedings of the International Conference on Applications and Development of Computer Games in the 21st Century: ADCOG 21; Hongkong Special Administrative Region, China, November 22-23 2001.

20. Open GIS Consortium, “OGC’s OpenLS Initiative: Building a Foundation for Location Services”, http://www.openls.org

21. Orwell, G. 1949. *Nineteen Eighty-Four.* London: Martin Secker & Warburg.

22. Palen L., Dourish P “Unpacking “Privacy for a networked society” for a Networked World “, submitted to CHI 2003.

23. Randell C., Muller., H. “The well mannered wearable computer”. *Personal and Ubiquitous Computing*, pages 31--36, February 2002.

24. Where on Earth http://www.whereonearth.com/