Large Scale Evaluation of User Privacy on Deployed National Mobile Networks

Blaine A. Price
Computing Research Centre
The Open University
Milton Keynes, UK MK7 6AA
+44 1908 653 701
B.A.Price@open.ac.uk

Mike Richards
Computing Research Centre
The Open University
Milton Keynes, UK MK7 6AA
+44 1908 654 023
M.Richards@open.ac.uk

ABSTRACT

The overwhelming majority of Western Europeans over the age of 10 own and regularly carry a GSM (2G cell phone) phone. Most of these can be described as general purpose programmable computers, so the age of ubiquitous computing (ubicomp) has arrived. Ubicomp introduces new privacy concerns, the most relevant of which is location privacy. In this poster we describe a system which allows UK GSM phone users to accurately determine their location with a high degree of accuracy virtually 100% of the time at no cost. We describe how we are deploying large scale studies of user attitudes to location privacy and exploring usability of privacy interfaces across a large diverse population.

1. OVERVIEW OF WORK

Ubiquitous computing (ubicomp) is a reality in Western Europe: the continent already possesses one of the highest penetrations of GSM (2G cell phone) phone usage in the world with equally high levels of geographic coverage. The overwhelming majority of people over the age of 10 years are able to use a rich variety of services delivered through inexpensive, familiar, and ubiquitous handheld devices. Mobile telephone handset capabilities range from being able to communicate with the network as a kind of dumb terminal using asynchronous text messages (GSM) to having embedded general purpose computers able to make video calls or transmit data at high speeds (GSM or UMTS SmartPhones).

Ubicomp introduces one new privacy concern: the release of location sensitive data. Ubicomp devices can determine (and therefore release) their location through a variety of means. RFID tags or active badges can be used within buildings which are fitted with an infrastructure to detect them, but this is expensive and hardly ubiquitous. Ubicomp devices containing a global positioning satellite (GPS) receiver are able to determine their location to a high degree of accuracy, but these are currently relatively expensive and only work outside buildings in areas that are not very built up. As recent work showed (LaMarca et al., 2005), GPS coverage for average individuals is poor because of the amount of time spent indoors.

LaMarca et al. (2005) describe a third method for ubicomp device positioning: using radio beacons "in the wild" (PlaceLab, an open source location determining system: see www.placelab.org). Beacons in the wild refer to fixed private omnidirectional short range radio sources with unique IDs which include IEEE 802.11 (WiFi), Bluetooth, and GSM transmitters. The approximate location of these transmitters is mapped by volunteers wandering around (wardriving) with GPS units and receivers which log the user's location at the time they are able to receive a signal and this is recorded as the location of the beacon. This map is then distributed with the location determining applications which currently run on laptops, PDAs and certain Nokia mobile telephones. User applications are then able to triangulate their location by measuring the strength of all of the beacons "visible" at a given time and comparing this to the apparent positions of the beacons. In contrast with the poor coverage of GPS location determination, GSM beacon triangulation gives near 100% coverage in urban areas. While Bluetooth and WiFi beacons have a range of between 10 and 100 metres respectively, GSM transmitters can have a range of thousands of metres. This means that the wardriving technique can give very inaccurate beacon location information for GSM beacons.

GSM network operators and third parties currently sell location based services using the inverse of the PlaceLab method described by LaMarca et al.: they calculate position by triangulating the phone location relative to the cell towers which are able to see the phone. A wide range of services are available including interfaces for parents to track their children and business to track their mobile sales force in order to deploy the appropriate person for a given task.

The European Union (EU) and Japan have both had laws in place to govern mobile location privacy which has resulted in a large range of applications being deployed in each jurisdiction. However, the emphasis on operators releasing user location only with explicit consent has let to a poor user interfaces for control of privacy: in general, the users can either make themselves visible to everyone or no one.

Our previous work (Price et al., 2005) surveyed recent work in ubiquitous computing (ubicomp) privacy interfaces and identified a number of issues affecting them, including the influence of regulation. Like Milberg et al. (1995), we noted the general information systems relationships between nationality, cultural values, personal privacy concerns, and privacy regulation. We examined some of the differences in national/cultural values and the effect regulation has on ubicomp privacy interfaces. Our initial studies showed that user concerns for privacy differed between Europeans (where strong privacy regulation is in place) and US studies where there are fewer regulations. This suggested that a detailed study of European attitudes to location privacy was warranted.

Our survey also showed that most previous studies of ubicomp privacy have involved small user groups using prototype interfaces. This suggested to us that large scale user studies of functioning interfaces would be an important contribution to understanding the privacy requirements of ordinary ubicomp users.

Within Western Europe, the UK situation is unique in that GSM cell tower locations are in a public database, coverage is very dense, and market penetration is extremely high. By building this database into the PlaceLab system we are able to create user applications on GSM phones to accurately determine their location and give the user the power to release or withhold it to other users or systems without involving network operators or any additional expense. In other words, we can put ubicomp location services in the hands of a large portion of the UK population at no expense to the user. We call this "location determination using radio beacons in civilization".

Previous ubicomp privacy studies used small non-representative samples of users including students, academics, and their friends because specialist (usually expensive) hardware was required. We propose to use a large representative sample of the UK population drawn from our student base. The Open University has over 200,000 adult students studying part time at a distance. Most of these are in the UK and represent the full socioeconomic and geo-demographic range of the population. We are currently surveying several thousand as to their attitudes towards certain privacy issues. We will then deploy a variety of location privacy interfaces to test usability and examine the changing user requirements and attitudes toward privacy as they use location-based services. In later studies, we plan to have the client software collect data automatically and transmit it directly to our server so that we do not have to question the user or interfere with their use of the telephone.

Lessig (1998) noted that privacy affected by laws, norms, market forces, and architecture. In our previous work (Price et al., 2005) we commented on the differences between strong and weak regulation of privacy. We suggested that "social translucence" (Erickson et al., 2002) was a norm that required user control of location privacy. It is clear that within Europe that market forces are driving users to adopt location aware ubicomp devices. This leaves architecture as the factor remaining for system design to either constrain or permit user control of privacy. By adopting the PlaceLab approach of putting the location determination in the hands of the user rather than the network operator, we are creating an architecture which permits user control of privacy. By using this architecture and performing iterative large scale usability tests, we believe we can move the study of privacy in ubiquitous computing out of the laboratory and into the mainstream.

2. REFERENCES

Erickson, T., Halverson, C., Kellogg, W. A., Laff, M., & Wolf, T. (2002). Social Translucence: Designing Social Infrastructures that Make Collective Activity Visible. *Communications of the ACM, 45*(4), 40-44.

LaMarca, A., Chawathe, Y., Consolvo, S., Hightower, J., Smith, I., Scott, J., Sohn, T., Howard, J., Hughes, J., Potter, F., Tabert, J., Powledge, P., Borriello, G., & Schilit, B. (2005). *Place Lab: Device Positioning Using Radio Beacons in the Wild.* Paper presented at Pervasive2005: the Third International Conference on Pervasive Computing, Munich, to appear.

Lessig, L. (1998). *The Architecture of Privacy.* Paper presented at the Taiwan Net'98, Taipei, Taiwan.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM, 38*(12), 65-74.

Price, B. A., Adam, K., & Nuseibeh, B. (2005). Keeping Ubiquitous Computing to Yourself: a practical model for user control of privacy. *International Journal of Human-Computer Studies,* (to appear).