CS 626

A Survey on Location Privacy

Reynold Cheng

Department of Computer Science, Purdue University.

Email: ckcheng@cs.purdue.edu

Abstract

Due to the rapid development of positioning technologies such as GPS, cell-phones and RF-IDs, location-based applications have been increasingly popular in these few years. While these applications promise to bring convenience (e.g., m-commerce) and safety (e.g., locating victims in emergency), they also raise the concern of location privacy. In particular, since our locations can be tracked at any time in any place, our private information such as where we have been at what time can be revealed without our consent. In this survey, we study location-privacy related problems in a pervasive computing environment. We investigate how legislations define and protect location privacy. We further discuss how privacy laws are enforced through privacy policies. We also address the issue of how location information can be "unlinked" from a person's identity through the use of anonymizers.

Keywords: location-based services, location privacy, privacy policies, anonymity, pseudonymity.

1 Introduction

Positioning technologies have undergone rapid developments in recent years [18, 21, 7]. As an example, the Global Positioning System (GPS) consists of a constellation of satellites, through which an object can identify its location accurately. The Global System for Mobile Communication (GSM) technology, a dominant standard in Europe, uses cellular base stations to compute the location of a wireless handset. More recently, the radio frequency identification (RF-ID) technology is gaining popularity, where a RF-ID tag, a small chip, responds to radio field emitted from a reader by sending back its identification information [12, 21]. Indeed, these wireless location technologies represent a fast-growing market, with an estimation of a $3.9 billion budget in 2004 [18].

These technologies enable a new class of applications known as *Location-Based Service* (LBS). An important example of LBS is the E-911 application in U.S. (correspondingly E-112 in Europe), where by using GPS, the location of a caller from cell phone can be identified in an accuracy of 125m in emergency [7]. Another application is the use of sensors placed along the side of a road to facilitate autonomous driving. Positioning technologies also help wireless carriers to maintain their systems. For example, the signal quality of each cellular station is monitored, and areas where the signal quality is poor can be identified quickly [21].

LBS has also been popular in the business domain [21]. RF-ID tags are now being used on things like razors in large departmental stores for the purpose of inventory management.LBS motivates personalized advertising too.For instance, advertisement on discounts can be sent to a person carrying a GPS-enhanced cell phone when she is walking near a shop. Thanks to positioning technologies, new applications like Pay-by-phone and Parking-by-phone allow customers to buy goods and services more easily.

These numerous examples demonstrate the potential of LBS applications in providing safety, convenience and new business opportunities. However, LBS also raises a new concern – intrusion of *location privacy*. According to [3], location privacy is defined as “ability to prevent other parties from learning one’s current or past location”. The fact that positioning technologies obtain accurate and timely information about location of a person can lead to invasion of personal privacy. For example, a service provider can track the whereabouts of a user and discover her personal habits. An employer can also find out whether her employees went to sensitive places such as AIDS clinic or a nightclub. Service providers may also give location information to unknown parties. A real-life example is BTexact’s Erica system, which allows third-party applications to access sensitive information about customers, including billing information and location information [3]. If location information is in improper hands, a person can be in physical danger since he may be found easily. It is feared by many that positioning technologies will ultimately create a “complete surveillance society”, where the movement of each citizen is scrutinized [21, 7, 3, 10, 9]. Preventing location privacy from being invaded is thus an issue of utmost importance.

Location privacy can be protected by simply shutting down the devices used for LBS. However, the convenience and usability of LBS may be severely limited. The more challenging question of upholding location privacy while maximizing the benefits of location services simulataneously is not easy to answer. In this survey, we study several measures that attempt to address this issue. The first solution protects privacy through legislations. The second class of solutions allows a user to specify privacy policies (e.g., Alice allows Bob but not Eve to know her location). Access is granted if a user's privacy preferences can be met by the location handling policies of service providers. It is assumed that service providers will obey their location handling policies, or else face legal consequences. The third group of solutions do not trust service providers. Instead, they use a trusted middleware called *location anonymizer* to “blur” location information before it is sent to service providers, so that location information cannot be related to the user.

The rest of this paper is organized as follows. In Section 2, we study how legislations in different countries protect location privacy. We then discuss the issues of specifying and automatically evaluating privacy policies in Section 3. We study different types of location anonymizers in Section 4. In Section 5 we briefly discuss organizations that work on location privacy issues. We conclude the survey in Section 6.

2 Protecting Location Privacy Through Legislations

In this section, we summarize the basic principles for handling location information properly, and discuss legislations in different countries that adhere to these principles [15, 16]. We also outline the problems related to enforcement of privacy laws.

2.1 Principles for Handling Location Information

Location information was classified as a type of *Customer Proprietary Network Information* (CPNI) in section 222 of the US's Communications Act of 1934. A CPNI is a kind of personal information, where carriers have to keep confidential, and cannot use or disclose without a prior authorization from customers [5].

The basic principles for handling location information in order to preserve personal privacy are stated in the four Fair Information Principles (FIP), drafted by the Organization of Economic Co-operation and Development (OECD) [15]:

1. **Collection limitation:** Location information of a target user should only be collected when that information is necessary for provision of a service.

2. **Consent:** A LBS has to seek the agreement of the user before her location can be collected. Furthermore, the consents given can be withdrawn at any time easily and free of charge. This is also called the **opt-in** principle where the user has to give his/her agreement before data is collected or disclosed.

3. **Usage and disclosure** has to be limited according to the consent given. If the LBS does not need to know the true identity of the user, pseudonyms (i.e., fake names) should be used.

4. **Security safeguards:** When the requested service is completed, location data has to either be erased or made "aggregate" (i.e., make the data impossible to identify a particular person).

These principles serve as basic guidelines for organizations and countries to draft regulations for handling location data. It is worth notice that all these principles can be superseded with the authority of law under special circumstances, e.g., emergency calls and lawful intercept.

2.2 Privacy Laws in Different Countries

The European Union countries proposed the 95/46/EC directive, one of the most important privacy laws [16]. Its basic principle is to provide citizen with adequate privacy, while allowing information to flow freely within the EU member states. The latest effort in 2000, called "The Directive on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Section", prohibits data collection without *opt-in* consent [15]. Also, all EU member states have to follow these directives. Another important point is that when personal information of EU citizens are exported or processed in non-EU countries, the personal information is to be kept at the same level of privacy. This requirement has created pressure for higher personal privacy standards in non-EU countries (including the U.S.).

THE U.S. passed the Privacy Act of 1974, another piece of influential privacy-related legislation, which requires fundamental principles such as transparency, collection and use limitations and security [16]. The privacy laws in U.S. has a subtle difference from the EU privacy law: while the EU member states practise the *opt-in* principle, the US privacy laws often practise the *opt-out* principle, where a service provider can activate the service without asking the user. According to [15], the U.S. does not have comprehensive privacy protection law for the private sector, and does not have an independent oversight agency for privacy. Instead, sectoral laws and self-regulation have been used. Recently, the U.S. has shown more concern for location privacy: in 2001, the Location Privacy Protection Act [5] has been passed, with a spirit similar to FIP.

Other Countries like Canada, Australia, New Zealand, Latin America and Japan have also been working actively on their own versions of location privacy laws [15].

2.3 Issues of Privacy Laws

Legislation undoubtedly provides a powerful and inexpensive mean of governing privacy. However, as we can see, each country has its own definition of privacy laws. When a LBS is tailored to work under the laws of a particular country, it may have to be changed in order to work legally in another country. In some cases, LBS are used across different countries (e.g., positioning a person in an international flight). In such scenarios it may be safer to design the service to fit one of the strictest privacy directives e.g., the EU directives [15].

Another important question is: how do these privacy laws impact the usage of a LBS? How does a user specify her consent before using a service? Will it be a nuisance for a user to evaluate a service provider's privacy statements every time before she uses the service? In the next section, we will examine these issues in more detail.

3 Location Privacy Policies

Whether a person's privacy is violated often depends on her preferences, and her agreement with the LBS involved. For example, Alice may agree with her employer that her position can be monitored only during office hours. The Blocker RF-ID tag scheme proposed in [12] allows RF-ID tags from refusing to respond to radio signals from certain service providers chosen by the user. On the other hand, a service provider can also have its own location information handling policies e.g., keeping location information for two days after the service is completed, selling location information to trusted third parties, etc. In this section we study in detail how users and service providers specify location privacy policies. We also discuss how this is done in a pervasive environment – an environment connected with mobile devices.

3.1 Specifying Location Privacy Policies

As Spreitzer and Theimer [20] points out, a user “should have control over who may know their whereabouts”. This view motivates them to develop a decentralized location query architecture, where each user is represented by a *user agent*. A user agent provides a mechanism for a user to specify control over information release e.g., how frequent should a location information be given, and who may gain access to it. They implemented the architecture in the Active Badge Tracking System, where users can choose not to respond to location request if they do not want to, by manipulating controls in their “active badges” – location sensors similar to RF-ID tags.

The issues of allowing users to specify their own privacy policies are further studied by Snekkenes [19] and Myles et al. [16]. Snekkenes listed four essential elements in formulating a location privacy policy: location of the object, identify of the object, the time this observation occurs, and the speed of the object [19]. The authors also proposed a policy language for specifying these privacy requirements.

Each LBS specifies its privacy policies on how location information is collected, how it is used, and how it is passed to third parties [15]. Before a location information can be used by the LBS, the LBS’s policies have to be verified that they comply with the user’s privacy preferences. An interesting question is: how should this verification be realized? A trivial implementation is whenever location information is needed, the LBS sends a message containing its location handling policy to the user. If the user thinks that the policy does not violate his privacy, he will click an “I agree” button. This can be a big nuisance for the user! Indeed, Myles et al. noticed that while there exists a need for users to determine their privacy preferences, it is also necessary to minimize the burden for them to specifying and clarifying policies [16]. They proposed an architecture called *LocServ* to verify privacy policies automatically.Their main idea is to construct a middleware called *validators* between the LBS and users. These validators collect the privacy preference profiles of the user and privacy policies of the LBS, and perform comparison on behalf of the user, so that the user is free from verifying the LBS’s privacy statements. The policies are expressed based on expanding the functionalities of P3P created by W3C. P3P is a XML policy specification language which provides a machine-readable form of privacy policies for Web sites [4].

A system similar to LocServ called *pawS* is described in [13], where P3P is also used as a foundation for describing machine-readable privacy policies. The primary difference between these two architectures is that while pawS allows users to protect their privacy at the time they activate a service, LocServ verifies privacy at the time only when a LBS request location data from users, either in a solicited or unsolicited manner.

3.2 Location Privacy Policies for Pervasive Environments

It is envisioned that LBSs will be executed in a *pervasive environment*. The definition of pervasive computing, according to IBM, is “personalized computing power freed from the desktop, enabling information access anywhere, anytime, on demand” [11]. Network and wireless technologies are used to connect numerous devices to provide an uninterruptible service. In such an environment, providing location services while protecting privacy presents new challenges. First, there may not be a single point that needs protection. For example, a person's location can be identified by the location of her laptop, her cell phone or a calendar file in the server describing when he is going to have a meeting. Secondly, location information can change in granularity while flowing from one node to another. Thirdly, the devices in the pervasive environment may be managed by different entities, instead of a single administrator. The problem of managing privacy in such an environment is thus more difficult.

Hengartner and Steenkiste [10] studied the issues of location privacy policies in a pervasive environment for location services. They studied two fundamental types of queries: user query, for querying the location of a specified user, and room query, for querying the information of users at a specified location. A user can specify location access policies for these queries, based on information granularity, location, users, and durations when the information is valid. Issues of trust between service providers and users, transferring access rights, resolving between conflicting policies, and keeping policies private are also addressed. A system is implemented to demonstrate such concepts, where SPKI/SDSI certificates are used for expressing location policies and trust. The main advantages of the system is that since certificates are stored distributively, no centralized node is necessary and thus there is no bottleneck. Also, each service is allowed to maintain access control independently. Due to the user of certificates, no identity of location seekers are required, so that users unknown to the system can also use the services. Finally, a single certificate can support group access. For example, Alice can specify her friends to access her location in a single certificate.

Hengartner and Steenkiste further extended their ideas to a more general pervasive environment, which not only handle people's location information, but also other pieces of information (e.g., where is free pizza?) [10]. Since devices are networked in an intricate manner to provide services, the authors proposed that privacy policies should be defined at an abstract level, called "information level" e.g., "Bob can access my location", instead of the more primitive "node level" e.g., "Bob can access my location provided by cell phone and PDA." This avoids the need for the user to specify policies in fine details. Further, when the information of an entity can be derived from another (e.g., the information about the people locator can be derived from the laptop locator), the privacy policies of the entity can be automatically transferred to another one. The authors proposed a policy description language to specify access grants, and an information description language to describe relationship between information sources. They also discussed an access control mechanism to transfer policies between entities, based on their information relationships.

3.3 The Problems of Privacy Policies

In all the works we have discussed in this section, it is assumed that each LBS provider is willing to conform to the privacy policies they provide. It is also implicitly assumed that providers are technologically competent in defending their client's privacy. For example, they must have good security mechanisms to prevent attackers from compromising their servers and steal location information. In essence, users *trust* that service providers behave what they describe in the privacy statements. This is not unreasonable, as an LBS provider faces legal consequences if it fails to fulfill its promises on location handling policies [16].

However, legislation and privacy policies may not be very useful against a malicious service provider, who is destined to break the privacy laws anyway. Also, since LBS are relatively new applications, it is doubtful whether privacy laws are effective enough. Moreover, attackers can steal information from the provider. The root of these problems is that users trust these services too much. In the next section, we discuss alternative solutions that attempt to protect the user and lower the amount of user's trust on LBSs. They also eliminate the burden of users from evaluating service providers' tedious privacy policies.

4 Anonymizing Location Information

Instead of trusting the LBS, an alternative solution to protect privacy is to *anonymize* information before it is dispatched to service providers. An example of anonymizer products can be found in [2], where the main idea is to remove information that can be traceable to users, such as network address, user ID etc, so that a user can surf the web with her identity hidden. For LBS applications, however, removing these pieces of information may not be enough. For example, by matching the user's location information with a map, the service provider can still identify the user if the location is her home or garage, etc. Thus, location information also needs to be anonymized to make it difficult to associate with the user's identity. In general, location information can be anonymized by reducing temporal and spatial resolutions of location information (called *location cloaking* [7]). In this section we discuss in detail how this can be done in more detail.

4.1 Classification of Location-Based Services

The process of anonymizing location information differs, depending on whether the identity of a user is known to the LBS. According to [3], LBS applications can be classified as follows:

1. **Non-Anonymous:** This kind of applications does not work without knowing a user's true identity. A typical example is: "When I am inside the CS building, let my class project groupmates know where I am".

2. **Anonymous:** This application class works with location information only, and does not require a user's identity. For example, in querying a LBS about the price of a coffee when approaching a coffee shop, a user only needs to supply her location to the LBS.

3. **Pseudonymous:** This type of applications needs to know the identity of a user, but it can use the user's pseudonym, rather than her real identity. An example is: "When I walk past a computer kiosk, display my emails". The LBS can use the user's pseudonym, rather than her real name, to retrieve her emails.

In the rest of this section, we explain how location cloaking works in anonymous and pseudonymous applications.

4.2 Location Cloaking for for Anonymous Applications

Gruteser and Grunwald [7] described an central anonymity server connected to both the users and the LBS. Both users and the LBS trust the server. Users send their encrypted location data to the server, which then decrypts them and "cloaks" the location data before sending them to the LBS.

Specifically, let (x,y,t) be the location (x,y) at time t sent by the user to the anonymity server. Using the *cloaking algorithm*, the anonymity server outputs a *cloaking tuple* $([x_1,x_2],[y_1,y_2],[t_1,t_2])$ to a LBS, where $([x_1,x_2],[y_1,y_2])$ is the rectangular area within which (x,y) is found, between the time interval $[t_1,t_2]$. In essence, the LBS receives location information of a coarse granularity from the anonymity server, so that location privacy of the user is protected.

How do we know the cloaking tuple is good enough for protecting location privacy? To answer this question, the authors introduced a metric known as k-anonymity to measure the degree of privacy provided by the cloaking tuple. This metric measures between time interval $[t_1,t_2]$, the number of users, k, at the same spatial vicinity $([x_1,x_2],[y_1,y_2])$. Thus a larger value of k indicates more difficulty in linking a location to a particular user. To use their system, a user informs the anonymizer a value, k_{min}. The anonymizer, upon collecting other users' location information, uses the cloaking algorithm to compute the cloaking tuple such that k_{min}-anonymity is achieved. In this way, a LBS obtains location information with reduced resolution of time and space. Also, since at least k_{min} users are guaranteed to be located inside the region, it becomes more difficult for the user to be traced. This idea is extended to the sensor network environment, where a distributed version of the cloaking algorithm is used, with each sensor computing partially the cloaked location in a hierarchical organization of sensors [8].

4.3 Location Cloaking for Pseudonymous Applications

Recall that a pseudonymous application associates a piece of location data with a fake user identity (called pseudonym). Despite this, it is still possible for an adversary to recover the true owner of the location. This can be done easily by tracking the location record of the user. When the user is observed to stay at a certain place for a long time, and that place corresponds to that user's office or home, her identity can be easily revealed even though he is using a pseudonym!

The root of this problem is that the pseudonym is not changed while the user is accessing the LBS. One simple solution is to rename the pseudonym for a user frequently enough, so that the path of the user cannot be traced [3]. However, if location information is supplied to the LBS in sufficiently high temporal and spatial resolution, one can still associate old and new pseudonyms.

Beresford and Stajano [3] proposed a solution for the above problem. Like Gruteser, they assume there is a trusted middleware system to help users to hide their identities. The middleware collects users' locations periodically. The geographical area is partitioned into *application zones* and *mix zones*. Each application zone is a region registered by a LBS, and the middleware sends the location of the user to the LBS whenever she steps into the region. A mix zone is a region not registered by any LBS. When a user steps into the mix zone, her pseudonym is renamed. Therefore, when she enters an application zone, her identity will appear different to the application. As an analogy, the mix zone is like a black box; people entering it come out with new faces. This makes it hard for viewers outside the black box to trace a particular person. The degree of privacy is defined in similar way as in Section 4.2: the *k-anonymity set*. This metric indicates k users are in the mix zone during an update period. A large value of k implies a higher degree of privacy. Again, a user can specify its minimum requirement, k_{min}, and the middleware only sends her location to the LBS when a k_{min}-anonymity set is obtained.

Pseudonyms are also used in routing protocols for preserving location privacy. Al-Muhtadi et al. studied how to provide anonymous communication between two users in a pervasive environment without revealing their location information to any intermediate routers [1]. A “mist-routing” protocol was proposed, where pseudonyms are used in routing tables. In [14], Lee et al. devised a location privacy protocol for a GSM network. Again Pseudo IDs are used in intermediate routers, in an attempt to hide a user’s location while she is using a mobile device.

4.4 Advantages and Problems of Anonymizers

The advantages of anonmyizer solutions over privacy policies are twofold [7]. First, LBS providers can process data with less overhead. They can collect information data, distribute them to third parties without seeking consent from the user. Secondly, users are released from the burden of evaluating service providers’ tedious policy statements.

There are a number of problems though. First, how does a user know the best value of k_{min}? If k_{min} is too large, the cloaked location information may be too ambiguous for a LBS to yield an accurate result; if it is too small, the privacy of a user is exposed. The LBS may be able to give a guideline to the user, but it can suggest a value of k_{min} smaller than necessary. Secondly, the k_{min}-anonymity requirement may be impossible to achieve if less than k_{min} users are using the same service at the same time [7]. Thirdly, the solutions may not survive the attack of malicious entities who spoof location data. If the middleware uses these bad location data, its output may not meet the anonymity requirements [7]. Finally, a centralized anonymizer is assumed in these solutions, which collects information from different users. This may not be scalable in a pervasive environment [1].

5 Organizations Working for Location Privacy

The issue of location privacy has already raised concerns in the software industry. A number of organizations have been working on standard processes and guidelines for developing privacy-aware applications. One of the most notable efforts is from the Internet Engineering Task Force (IETF)'s Geopriv working group. Its primary objective is to access the privacy requirements, and develop protocols and APIs that allow devices to communicate in a confidential, integrity-preserving, and private manner. It is also interested in the issues of adjusting the resolution of location data for anonymous and pseudonymous transfer [6].

The Open Mobile Alliance (OMA) is an industry forum, formed in June 2002 by about 200 companies, most of which are major mobile operators and service providers. Its goal is to develop market-driven and interoperable mobile services across different geographical areas [17]. It emphasizes on “openness”, and attempts to provide standards for developers in mobile computing. It has integrated several related technical forums, one of which is the Location Interoperability Forum (LIF). A task of this forum is to develop a set of location privacy guidelines for system designers to follow [15].

6 Conclusions and Future Work

The advance of positioning technologies allows location-based services to emerge as a new generation of applications. They promise to provide us safety and convenience, but also raise a new concern – intrusion of personal privacy. Without proper countermeasures, we can lose our privacy and constantly monitored by “Big Brothers” in a total surveillance society.

We studied different efforts in protecting location privacy. While privacy legislations provide some protection, they have to be properly supported by technologies. One such technology is to require both users and service providers to specify their privacy policies, and implement a middleware to automatically evaluate them, in order to lessen the effort of both parties. This class of solutions generally assumes that service providers respect legal and social norms. On the other hand, anonymizers place less trust on service providers; they evaluate location information with reduced temporal and spatial resolutions to make it difficult for service providers to intrude users’ privacy.

An interesting question is: can we have an integrated solution that captures both the advantages of privacy control policies and location anonymizers? While laws and privacy policies provide a cheap and simple solution to protect privacy, anonymizers equip users with better degree of “self-protection”. There are also various interesting issues about location anonymizers that are worth further study. First, the solutions and anonymity metrics proposed in this survey assume either anonymous or pseudonymous applications. Whether these techniques work for non-anonymous applications are questionable. Secondly, the k-anonymity constraint does not work if fewer than k users are using a particular application. We may thus need another metric to measure privacy in such situations. Thirdly, anonymizers generate location information of lower resolution, but this can lower the quality provided by service providers. It will be interesting to study the relationships between privacy, location uncertainty, and quality of service.

Location privacy, like security, is a multifaceted problem. It is an emerging and important issue. Governments, industry, researchers and users should work together to understand how it can be protected, while unleashing the full power of location-based services.

References

[1] Jalal Al-Muhtadi, Roy Campbell, Apu Kapadia, M. Dennis Mickunas, and Seung Yi. Routing through the mist: Privacy preserving communication in ubiquitous computing environments. In *International Conference of Distributed Computing Systems*, 2002.

[2] Anonymizer. Anoymizer website. http://www.anonymizer.com.

[3] Alastair R. Beresford and Frank Stajano. Location Privacy in Pervasive Computing. *IEEE Pervasive Computing*, 2(1):46–55, 2003.

[4] World Wide Web Consortium. The Platform for Privacy Preferences 1.0 (P3P 1.0) Specification. http://www.w3.org/TR/2001/WD-P3P-20010928, Sept. 2001.

[5] Sen. John Edwards. Location Privacy Protection Act. http://www.techlawjournal.com/cong107/privacy /location/s1164is.asp, 2001.

[6] Internet Engineering Task Force. Geographic location/privacy (geopriv) charter. http://www.ietf.org/html.charters/geopriv-charter.html.

[7] Marco Gruteser and Dirk Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *Proceedings of the First International Conference on Mobile Systems, Applications, and Services*, May 2003.

[8] Marco Gruteser, Graham Schelle, Ashish Jain, and Dirk Grunwald. Privacy-aware location sensor networks. In *Proceedings 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS)*, 2003.

[9] Urs Hengartner and Peter Steenkiste. Access control to information in pervasive computing environments. In *Proceedings 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS)*, 2003.

[10] Urs Hengartner and Peter Steenkiste. Protecting Access to People Location Information. In *Proceedings of First International Conference on Security in Pervasive Computing*, LNCS. Springer, Mar 2003.

[11] IBM. Pervasive Computing: IBM Wireless, Voice and Mobile Software Products. http://www-306.ibm.com/software/pervasive/index.shtml.

[12] Ari Juels, Ronald L. Rivest, and Michael Szydlo. The blocker tag: selective blocking of RFID tags for consumer privacy. In *Proceedings of the 10th ACM conference on Computer and communication security*, pages 103–111. ACM Press, 2003.

[13] Marc Langheinrich. A privacy awareness system for ubiquitous computing environments. In *4th International Conference on Ubiquitous Computing*, 2002.

[14] Chii-Hwa Lee, Min-Shiang Hwang, and Wei-Pang Yang. Enhanced privacy and authentication for the global system for mobile communications. *Wirel. Netw.*, 5(4):231–243, 1999.

[15] Location Inter-operability Forum (LIF). Location Inter-operability Forum (LIF) Privacy Guidelines (LIF TR 101 Report Version 2.0.0). http://www.openmobilealliance.org/tech/affiliates/LicenseAgreement.asp?DocName=/lif/lif-tr-101-v2.0.0.zip, 2002.

[16] Ginger Myles, Adrian Friday, and Nigel Davies. Preserving Privacy in Environments with Location-Based Applications. *IEEE Pervasive Computing*, 2(1):56–64, 2003.

[17] Open Mobile Aliance (OMA). About OMA. http://www.openmobilealliance.org/about_OMA/index.html.

[18] T. Robinson. Location is everything. *Internet week online*, September 12, 2000.

[19] Einar Snekkenes. Concepts for personal location privacy policies. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, pages 48–57. ACM Press, 2001.

[20] Mike Spreitzer and Marvin Theimer. Providing location information in a ubiquitous computing environment (panel session). In *Proceedings of the fourteenth ACM symposium on Operating systems principles*, pages 270–283. ACM Press, 1993.

[21] J. Warrior, E. McHenry, and K. McGee. They know where you are. *Spectrum*, 40(7):20– 25, July 2003.