Mobile Positioning vs. Privacy

Mikko Heikkinen
undergraduate student
Networking Laboratory
Helsinki University of Technology
mikko.heikkinen(at)hut.fi

Abstract

Mobile positioning enables finding of the current location of a specific mobile phone or other suitable mobile device. Mobile positioning can be used to implement various safety, billing, information, and tracking services. The EU introduced a formal directive concerning location data; the USA is trusting mostly on entrepreneurial self-regulation. Finland has recently established clear positioning legislation. The privacy risks of mobile positioning are substantial but one can try to minimize them in several ways. The user is the owner of his or her position, but is easily mislead by the complexity involved in handling location information.

1 Introduction

Mobile positioning is a new rapidly advancing mobile technology application which brings a myriad of privacy issues into consideration when being implemented. Essentially, mobile positioning enables finding of the current location of a specific mobile phone or other suitable mobile device. Mobile positioning can be used to implement various safety, billing, information, and tracking services [1]. Some examples are presented in table 1. The use of these applications can result in difficult privacy issues concerning the use of the location information: is an employer entitled to know the exact location of employees, are parents required to know their child's location all the time and how widely authorities can take advantage of the positioning information of possible suspects of crime, among others.

1.1 Technical Background

There are many competing technologies available for implementing mobile positioning. The European and American standardization organisations ANSI and ETSI have committed to the standardization of the following mobile positioning technologies: Cell of Origin (COO), Enhanced Observed Time Difference (E-OTD), Time of Arrival (TOA), and Assisted GPS (A-GPS) [1, 4]. Ericsson's Mobile Positioning Protocol (MPP) [1, 2], Nokia's mPosition [5], and Open Mobile Alliance's Mobile Location Protocol (MLP) [12] integrate these various technologies. Considering IP networks, MobileIP [3] is worth mentioning.

COO is the easiest to implement. When it is used, the location of a mobile device is the location of the base station the device is currently using. In urban areas an accuracy of 150 metres can be reached within pico cell sites. The accuracy decreases rapidly when larger cell sizes are in use. COO has a response time of three seconds and can be deployed without modifications to mobile devices. COO is the only technology that is widely deployed in wireless networks today.

E-OTD is based on calculating time differences in signal arrival between at least three base stations and a location measurement unit. The calculation is done by mobile devices enabled with E-OTD software. E-OTD provides accuracy between 50 and 125 metres and a response time of five seconds, but requires software modifications on existing mobile phones.

TOA requires the time synchronization of base stations with GPS or atomic clocks. Thus, it is quite expensive to implement, but does not require modifications to mobile devices. TOA offers slightly better accuracy than COO, but has a slow response time around ten seconds making it unusable for many applications.

A-GPS uses the Global Positioning System (GPS) to derive the location information. GPS is a precise positioning system using several satellites orbiting around Earth. A-GPS provides an accuracy of around

Table 1: Examples of Mobile Positioning Services

Application	Mass acceptance accuracy requirements	Objective	Location frequency
Location Sensitive Billing	250m	Competitive Pricing	Originated calls, received calls, mid-call
Roadside Assistance	125m	Send help	Originated calls
Mobile Yellow Pages	250m	What's near me?	Originated calls
Traffic information	Cell/Sector	What's traffic like?	Originated calls or every 5 min
Location based messages	125m	Advertise, alert, inform	Originated calls or every 5 min
Fleet tracking	30 - 125m	Resource management	Every 5 min or on demand
Track packages	Cell/Sector	Locate and direct	On demand
Driving directions	30m	Guidance	Every 5 secs

20 metres with a response time of a few seconds. The best results are achieved when the mobile network is equipped with specific assisting capabilities to share the calculations required with the mobile device. Unfortunately, this along with the requirement of A-GPS enabled mobile devices drives the implementation costs of A-GPS pretty high.

MPP is an example of an intelligent network (IN) solution. MPP is lying above the COO, E-OTD, TOA, and A-GPS protocols in the protocol stack. It consists of a mobile location center which relays the location information from lower level protocols to the application requesting the information. MPP works only with Ericsson network architecture. Nokia has a similar IN solution called mPosition. Open Mobile Alliance's MLP tries to establish vendor independent location messaging. MLP requires that both the location center providing the location information and the location based service requesting it comply with MLP's XML based messaging. The relations of the technologies mentioned above are summarized in figure 1.

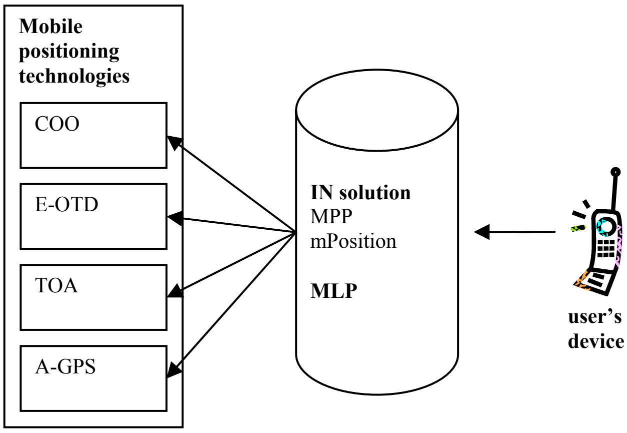

Figure 1: Technological relations

MobileIP enables an IP node to roam freely in different IP based networks while maintaining its home IP address. When a mobile IP node (for instance an IP based mobile phone in the future) goes away from its home IP address, it tells a home agent to route its traffic to the new address called the care-of-address. This process is transparent to higher level application protocols. IPv6 provides route optimization capabilities to MobileIP by enabling the mobile node to tell its current care-of-address to selected correspondent nodes. The traffic from these nodes doesn't have to be tunnelled through the home agent.

2 Legislation

The European Union and the United States of America have chosen different approaches concerning mobile positioning. The EU introduced a formal directive concerning location data; the USA is trusting mostly on entrepreneurial self-regulation.

2.1 Legislation in the EU

The new European Union directive 2002/58/EC has introduced specific regulation concerning mobile positioning. The directive was officially adopted on July 12, 2002. It establishes a common framework for data protection in telecommunication services and networks regardless of the technology in use. Its predecessor 97/66/EC only referred to calls in circuit-switched networks, whereas the new directive addresses all traffic data in a technology neutral way [3]. Traffic data is defined in the directive as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof" [11]. However, the new directive differentiates between location data *within* traffic data giving less precise positioning information and location data *other than* traffic data allowing the exact positioning of user's device.

Whereas for location data within traffic data informed consent is required when location information is used for value added services, i.e. services beyond "transmission of a communication or billing" (Art. 6 par. 3); for location data other than traffic data either anonymisation or informed consent is required (Art. 9 par. 1) *and* users that have given their consent have the possibility to temporarily refuse the processing of location information for each connection or transmission of a communication (Art. 9 par. 2). In both cases, users have the right to withdraw their consent entirely at any time. Before giving his or her consent, a user must be notified what type of location data is going to be used, how long it is going to be used, why it is going to be used, and whether third parties are allowed to access it.

2.1.1 Case Finland

Finland has been always eager to implement new EU directives among the first ones. The directive 2002/58/EC was implemented in the privacy law concerning electronic messaging (SVTSL 516/2004) on September 1, 2004 [7, 8]. The law replaced an old one, and the issue of mobile positioning was taken into special consideration. The Finnish Communications Regulatory Authority (Ficora) is responsible for monitoring the obeying of the law and the rulings based on it, whereas the Office of the Data Protection Ombudsman is responsible for monitoring the use of mobile positioning information and some other applications derived from the law. According to the law, a telecom operator is entitled to use location information if its customer has not prohibited it to do so. Location information is defined as geographical information used for other purposes than delivering a message. The operator must get a consent from its customer before it is allowed to give away location information to a third-party service provider. This consent must be got for each service separately. The law allows the use of location information for telecom operators in order to provide value added services, but each customer has the right to deny the use of his or her location information for these purposes.

2.2 Legislation in the USA

Compared to the European Union, the legislation concerning mobile positioning is much looser in the United States of America [6]. There is no established general data protection. Instead, the industry has developed privacy regulation in a self-regulated way. There are, however, certain governmental parties interested in privacy regulation. The Federal Trade Commission (FTC) has been rigorous to ensure that companies abide to the privacy policies they have published. The Federal Communications Commission (FCC) has ruled that the section 222 of the Telecommunications Act of 1996 requires that telecommunication companies have to obtain an oral, written, or electronic consent from their customers to use customer proprietary network information (CPNI) to market services other than the customer's current service relationship with the company. Besides this opt-in policy, recently an opt-out policy was developed, which allows telecommunication companies to share "communications-related" CPNI to its affiliates. The definition of affiliates is rather broad, covering agents, affiliates, joint venture partners and independent contractors. There is, however, little experience of this opt-out policy in practice. The definition of "communications-related services" is rather vague, and leaves room for debate.

Concerning positioning, FCC ruled on July 24, 2002 as a response to an initiative from an independent association, that "wireless carriers must receive a customer's explicit approval before using their location information". The situation seems clear but the liberal nature of American legislation always paves way for trials. There are a few specific issues to mention concerning positioning legislation in the USA. The first is the Children's Online Privacy Protection Act, which generally speaking prohibits the collection of private data online from children without prior consent from their parents. The law could have implications also to mobile positioning, and developers should be extremely careful when implementing online services taking advantage of mobile positioning which could have children users. The second issue is the E911 legislation which requires mobile operators to deliver information concerning caller's position to authorities when a call is made to the national emergency number 911. The advanced phase of the law requires a positioning precision of 50-100 meters which will implicate major technical changes in American mobile networks causing the nation-wide emergence of positioning capabilities.

3 Privacy Enhancing Technologies

There are certainly many risks involved when mobile positioning is being used [9]:

- Financial risks are caused by e.g. court cases following the misuse of location information during work relations.
- Location based spam might be sent to positioning users.
- Harm to reputation might arise in certain situations, e.g. when a spouse finds out his or her partner's suspicious whereabouts.

At least five major privacy enhancing technologies are available for protecting sensitive mobile location information and thus reducing the risks mentioned: Mix Networks, P3P, intermittent connectivity, user interface solutions, and trusted location cloaking proxy. The first two can be used only in IP networks.

3.1 Mix Networks

Mix Networks is a part of the Freedom System, which is a pseudonymous IP network providing privacy protection by hiding user's actual IP address and other personally identifying information [3]. Anonymous Internet Proxies (AIPs) are the core network privacy daemons responsible for passing encapsulated packets between themselves until packets reach an exit node or an AIP wormhole. When a certain AIP runs as an exit node, it works like a regular network address translator. The traffic between AIPs is symmetrically encrypted. When client sends traffic to the service provider, the service provider sees the IP address of the AIP wormhole responsible for passing the packet to it, not the actual IP address of the client.

3.2 P3P

The Platform for Privacy Preferences (P3P) was originally established as a standard to control privacy preferences in web services but it can be modified for protecting positioning privacy [3]. P3P is based on the XML language. It is used in conjunction with the MobileIP technology discussed in the Introduction section of this paper. The home agent needs to have a web server interface and a privacy policy set up for location data in order to take advantage of P3P. It sets up a web site for mobile users to grant or revoke their consent to use location based information for value added services. The mobile node has to have a P3P-compatible user agent including P3P privacy preferences defined by its user for processing location data. The mobile node accesses the home agent's web site in order to receive the current privacy policy set by the user. There are two main problems with P3P: when the mobile node negotiates with the home agent about the privacy policy, it actually sends information about its current location. Thus, the home agent must be inside a safe zone or anonymous connections have to be allowed. The more profound problem is that user cannot be sure whether third-party value added services actually obey his or her privacy policy. Thus, P3P must be backed up with binding legislation such as the new EU directive 2002/58/EC. The extension tags of the upcoming MobileIP implementation of the IPv6 protocol will provide a more powerful solution, but P3P can be implemented today.

3.3 Intermittent Connectivity

With intermittent connectivity, the mobile device avoids to reveal its precise position by requesting geographically coded requests one set at a time rather than individually through separate queries [9]. For example, a user wants to know what kind of service is available on a specific address. User's device positions itself and requests from a third-party service provider what services are available on all addresses on the street, not just the specific address it is interested in. As it can be easily noted, intermittent connectivity is only suitable to a restricted group of applications due to the unnecessary additional data transfer.

3.4 User Interface Solutions

Privacy protection can be also established by innovative user interface design [9]. For instance, the interface of a mobile device could provide information at what extend user is giving away his location at the moment and who are requesting information about user's location. Of course, a certain balance has to be maintained in order not to overload the user with unnecessary information.

3.5 Trusted Location Cloaking Proxy

A trusted location cloaking proxy provides anonymity by adjusting the resolution of the location information reported to services based on the density of users in a region [9]. For example, when a distrusted service requests information about the cars in its neighborhood, it receives a location of a user with k-anonymity within a region that includes k-1 other users (or cars in this case). The proxy runs a cloaking algorithm that selects the smallest of a set of regions that includes the user and at least k-1 other users and reports it to the service. In consequence, the distrusted service cannot easily map the reported location back to an individual user.

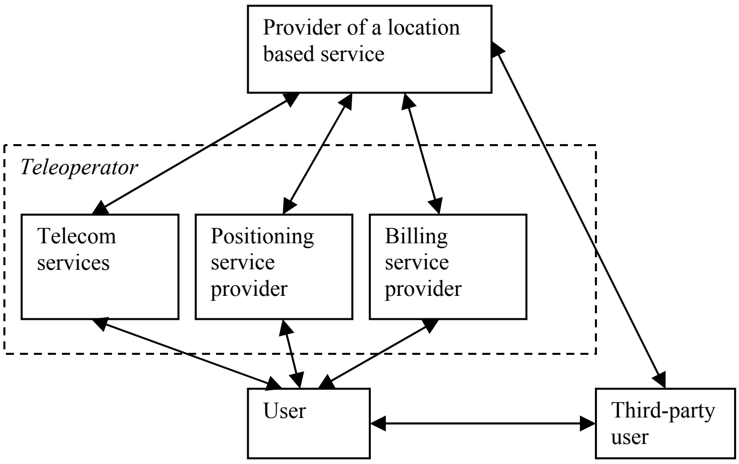

Figure 2: The parties of mobile positioning

4 Discussion and Conclusions

There are many parties to be taken into account when considering the privacy issues of mobile positioning [10]; they are summarized in figure 2. The third party service user means a person who receives location information from a find-a-friend service, for instance. All these parties must comply with the privacy policies set by the law and by them themselves. One must also note that they must implement necessary security measures to prevent the abuse of location information. Usually teleoperators have sufficient security arrangements already implemented, but the situation might not be so with independent service providers. The unnecessary use of location information should be avoided to prevent possible abuse. In addition, all users of the positioning service should be aware that their location information is being processed and they should be always able to disallow such usage. Furthermore, users should know precisely the extent and the purpose of location information processing.

One question raises up when one examines privacy issues involved in mobile positioning: who is the owner of user's position? The current legislation provides no clear single answer. It seems that location information is somewhat analogical to portable mobile numbers: the teleoperator maintains the number or position, but the decision of its usage remains to the user. However, position is a much more abstract concept than number resulting in increased flexibility and options in its usage causing greater risks of abuse.

After consent for usage of location information has been given, teleoperators and individual service providers may have multiple possibilities for processing it in many contexts in order to gain financial advantage. A normal end-user will have substantial difficulties in trying to piece together all the different contexts and applications in which his or her location information might be used. He or she probably has difficulties understanding the terminology involved and the real consequences of his or her consent.

Therefore, though the user has a right to choose, he or she might not be able to gather sufficient amount of information to make an informative decision.

Legislation cannot do miracles; the real hope lies in the goodwill of teleoperators and service providers. The adaptation of positioning-based services will be severely hindered if there are substantial privacy scandals reaching critical amount of publicity. A mutual respect of privacy will most likely guarantee a successful future for the promising positioning-based applications.

References

[1] Buckingham, Simon. An Introduction to Mobile Positioning. http://www.mobilewap.com/wp/positioning.htm, referenced on 7.10.2004.

[2] Ríos, Sergio. Location Based Services: Interfacing to a Mobile Positioning Center. http://www.wirelessdevnet.com/channels/lbs/features/lbsinterfacing.html, referenced on 7.10.2004.

[3] Escudero-Pascual, A., Holleboom, T., and Fischer-Huebner, S. Privacy for Location Data in Mobile Networks. http://www.it.kth.se/~aep/PhD/docs/paper8-nordsec2002.pdf, referenced on 7.10.2004.

[4] LaMance, Jimmy, DeSalas, Javier, and Järvinen, Jani. Assisted GPS: A Low-Infrastructure Approach. http://www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=12287, referenced on 11.10.2004.

[5] Nokia White Paper. Location Aware Applications Take Off. http://www.nokia.com/nokia/0,8764,56867,00.html, referenced on 11.10.2004.

[6] Tervo-Pellikka, Raija and Simojoki, Samuli, Positioning technology. Report of the NAVI Regulatory Framework –project. Helsinki Institute for Information Technology. http://www.vtt.fi/virtual/navi/cd/International_Regulations.pdf, referenced on 7.10.2004.

[7] Ficora. Sähköisen viestinnän tietosuojalaki (in Finnish). http://www.ficora.fi/suomi/tietoturva/svt.htm, referenced on 14.10.2004.

[8] Tietosuojavaltuutetun toimisto. Sähköisen viestinnän tietosuojalaki (in Finnish). http://www.tietosuoja.fi/2001.htm, referenced on 14.10.2004.

[9] Schilit, Bill, Hong, Jason, and Gruteser, Marco. Wireless Location Privacy Protection. Invisible Computing, December 2003, 135-137. http://www.computer.org/computer/homepage/1203/invisible/rz135.pdf, referenced on 7.10.2004.

[10] Simojoki, Samuli. Location-based Services and General Privacy and Data Protection Principles. Report of the NAVI Regulatory Framework –project. Helsinki Institute for Information Technology. http://www.vtt.fi/virtual/navi/cd/Privacy_Principles.pdf, referenced on 7.10.2004.

[11] Regulatory framework for electronic communications in the European Union, Situation in September 2003. http://europa.eu.int/comm/competition/liberalization/legislation/regulatory_framework.pdf, referenced on 28.10.2004.

[12] Open Mobile Alliance. OMA-LIF-MLP-V3_1-20040316-C. http://www.openmobilealliance.org/release_program/docs/CopyrightClick.asp?pck=MLP&file=OMA-LIF-MLP-V3_1-20040316-C.pdf, referenced on 28.10.2004.