Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 244 (2009) 125–137
www.elsevier.com/locate/entcs

Mobile Identity Management Revisited

Emin Islam Tatli[1] Stefan Lucks[2]

Faculty of Media
Bauhaus-University of Weimar
Germany

Abstract

Identity management provides PET (privacy enhancing technology) tools for users to control privacy of their personal data. With the support of mobile location determination techniques based on GPS, WLAN, Bluetooth, etc., context-aware and location-aware mobile applications (e.g. restaurant finder, friend finder, indoor and outdoor navigation, etc.) have gained quite big interest in the business and IT world. Considering sensitive static personal information (e.g. name, address, phone number, etc.) and also dynamic personal information (e.g. current location, velocity in car, current status, etc.), mobile identity management is required to help mobile users to safeguard their personal data. In this paper, we evaluate certain required aspects and features (e.g. context-to-context dependence and relation, blurring in levels, trust management with p3p integration, extended privacy preferences, etc.) of mobile identity management systems from the perspective of a *push context-aware application*, i.e. the Friend Finder application.

Keywords: privacy, mobile identity management, location-based applications, p3p

1 Introduction

Social, ethical and legal aspects require privacy of users in the digital Internet platform. With the introduction of new web technologies, users give away many of their personal data to other service providers and Internet users. But the risk of misusing the collected personal data threatens privacy of users. Service providers can profile users, send spam emails based on their profiling results, apply dynamic pricing which means different people pay different amount for the same service, forward and even sell data collected to third parties.

On the other hand, the legacy laws based on EU directives [3,4] regulate that personal data of an individual should not be retrieved without his consent, not be used for other purposes rather than the stated purpose, not be shared with others if it is not stated before and be deleted if the user cancels his or her consent

[1] Email:emin-islam.tatli@medien.uni-weimar.de
[2] Email:stefan.lucks@medien.uni-weimar.de

doi:10.1016/j.entcs.2009.07.044

later. Technical system developers should take into consideration of privacy regulations and integrate privacy-enhancing tools within their systems in order to help individuals to guarantee their privacy.

Identity is described as "one or more attributes which are applicable to this particular subject or object" [3]. A user can hold many identities and each identity can be assigned to many of his attributes. Identity management helps individuals to control their personal data when they need to be shared with other third parties and thus supports their privacy.

With the new trend towards high-level mobile devices like Personal Digital Assistants (PDAs) and mobile phones, context-aware mobile applications have started becoming a part of our daily lives. More context-aware applications will be experienced in the near future. Finding nearby pizza shops and restaurants, friend finder applications [7,2], tracking kids [17], locating people in emergency [10], location-based chats and games [11] are the typical examples of the context-aware applications that exist today. Mobile users of context-aware applications have also identities that are in interaction with other principals. Besides, the *location* attribute of mobile users is a very sensitive context attribute and must be protected against unauthorized access. Considering this, mobile identity management has become an important requirement for context-aware applications.

Mobile identity management can be considered as a subgroup of identity management. This statement is partially true. The new context data especially location data has its own characteristics and therefore not all identity management solutions can be applied to mobile identity management. In this paper, we focus on a specific push context-aware application (i.e. the Friend Finder) and evaluate the important privacy aspects from the perspective of mobile identity management. The aspects we mention are not only specific to mobile identity management, but their evaluation is more mobile-centric.

The paper is structured as follows: Section 2 introduces context-aware applications and motivates on the Friend Finder application. Section 3 explains the existing privacy risks and the requirement for a mobile identity management. Section 4 explains the related works. Section 5 discusses the required aspects related to mobile identity management. Section 6 gives the details of the integration of the required aspects within the Friend Finder application. Finally, the paper is concluded in Section 7.

2 Friend Finder Application

Context-aware applications facilitate the context data (e.g. location, time, velocity, etc.) of mobile users for enabling services. Service providers and telecommunication providers already focus on extending their infrastructures and developing applications in order to support mobile users getting benefit of context-aware especially location-aware applications. In context-aware applications, mobile user's context data such as current location, time, weather, profile, etc. are considered by service

[3] from Wikipedia: http://en.wikipedia.org/wiki/Identity_management

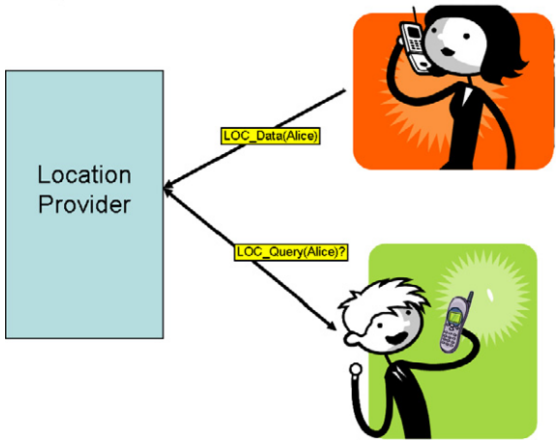

Fig. 1. Friend Finder Service

providers while the mobile users holding their PDAs are interested in getting the service that best fits their current context.

Context-aware applications can be grouped as *pull* and *push* services based on how service is retrieved. In pull services, mobile users ask for a particular service, get the requested service and finish the interaction with the service provider. Restaurant finder is a typical example for pull services. In push services, mobile users are interested in a particular service and register to the service provider in order to retrieve the service which is triggered if a certain event occurs or a certain time period passes.

Friend Finder is a typical example of *push* service for location-based applications, i.e. locating relatives and friends within certain area [7]. There are mainly two types of principals in the Friend Finder. These are mobile users and the location provider as illustrated in Figure 1. Additionally, other providers like map provider can also take part in the Friend Finder (see Figure 5).

The business logic of the Friend Finder works as follows: The mobile users participating in the Friend Finder application send periodically their location data computed by their mobile devices to the central location provider. They can then query locations of their particular friends and relatives through the location provider. Normally, the location provider presents the location information as simple text to mobile users. The map provider can enhance this functionality by showing the location information of mobile users on a visual map with navigation instructions.

3 Mobile Identity Management

Mobile users have security considerations and are anxious about the privacy of their context, especially their location [18]. In many cases, they require guaranteed context privacy, otherwise, they would refuse to use the service. Some particular questions regarding context privacy are:

- What happens if service providers collect my location information regularly and

use this collected information to track me or to make user profiles?

- What if service providers record at what times during the day I frequently use the services and send me advertisements at these times?
- What happens if the service providers share my location information with other third parties?
- Do service providers really need my location for this particular service?
- Is it enough if I give away my location information with a low resolution?

Mobile identity management helps users interacting with mobile applications to safeguard their personal data in the digital world as they do in the physical life. You have many relations with other people and organizations in the society. You are a computer scientist, a husband, a child, a friend or a stranger for somebody at the same time. That means, you have many *partial* identities [24]. Each partial identity is mapped to a group of attributes. You can intuitively decide which partial identity is used for communicating with whom. You also switch from one partial identity to another very easily and quickly. You can control to whom you trust and do not trust. This scenario needs to be also possible in the digital world. You should be able to create different partial identities, map a group of attributes to this identity and decide which partial identity to use based on your partner.

Mobile identity management should be beyond the formulation of "*which attributes belong to which identity and which identity is used with whom*". If you consider the social life, you do not give any information about you to someone which might tell this information to other people. You build automatically your trust relations with others. You do not talk about your secrets with your friends if others are around and this is something like *secure* communication. Considering *location* attribute, you do not tell your exact location everybody every time. You tell your exact location in weekdays to your boss but at the weekend your boss does not need to know your location. On the other hand, your wife can get to know your location at anytime and wherever you are. You generally remember which information was given to which person (i.e. history management). If required, you prefer staying anonymous while you are in interaction. When you buy something from supermarket, you do not need to identity yourself. All these aspects are part of identity management and must be supported by mobile identity management solutions in the digital world as well.

4 Related Work

The PRIME (*Privacy and Identity Management for Europe*) project [14] is supported by the European Union's Sixth Framework Program and the Swiss Federal Office for Education and Science. The aim of the PRIME is the development of privacy-enhancing tools for identity management.

idemix [8] has been developed within the PRIME project and aims achieving anonymous *authentication* in applications. The LBS [12] prototype of the PRIME implements a demo of location-based applications for pharmacy search. The demo

application shows how privacy of personal data and pseudonymity are protected against mobile operators and service providers. Unlike our focus on push services, the demo application considers only pull services. Besides, certain aspects like context relations and dependencies, blurring in levels are not within the concern of the PRIME LBS.

The FIDIS (*Future of Identity in the Information Society*) [5] project is a Network of Excellence project and supported by the European Union under the 6th Framework Programme for Research and Technological Development. FIDIS focuses on the topics like future identity management, identity thefts, privacy with legal-social content, mobility and identity, etc. They have surveyed a detailed database of identity management solutions in academia and industry [6].

The NEXUS project at the University of Stuttgart-Germany focuses also on context-aware applications and "*envisions the World Wide Space to be the common basis for future context- aware applications*". In their sub-project regarding security and privacy, they propose [21] providing location privacy by applying coordinate transformations. They show that how location can be rendered illegible and it is still possible to perform processing operations required by location-based services.

Jendricke et al. present an identity manager to control personal data sent from mobile devices through networks [22]. An identity manager provides an interface with which one creates different virtual identifications (IDs), i.e. pseudonyms, and binds a subset of his personal data to each ID. When communicating with a service provider, the user chooses an ID that is suitable for this particular type of communication. Before any personal data is sent to a service provider, the user is explicitly asked to confirm the transmission. On the other hand, the identity manager does cover only limited aspects of mobile identity management for context-aware applications. As examples, blurring in levels, history management, trust management and context relations are not explicitly supported.

P3P (Platform for Privacy Preferences) [16] and Appel (A P3P Preference Exchange Language) [1] are W3C recommendations and help the individuals to build a trust relation with servers and service providers. Servers and service providers specify their data collection policies as P3P policies and publish them. The users specify their privacy preferences in Appel. The P3P-capable user agents (e.g. browsers) retrieve the server's P3P policy, compare with the user's Appel preferences and in case of any confliction the communication is canceled.

For communication anonymity, Anonymizer [15] and mix-network based solutions JAP [9] and Tor [19] exist. Anonymizer simply retrieves the user's http request, forwards it to the server, receives the reply from the server and sends it back to the user. Providing this, the server does not know anything about the user. But, the Anonymizer knows about the user and therefore the users have to trust the Anonymizer. In mix-network based solutions the messages are encryptedly exchanged between different nodes staying between the sender and the receiver. Each node knows about the sender and the next node. Therefore, the first node knows about the user but not the server and similarly the last node knows about the server but not the user. Recently, a study on Tor network has been published [13].

Tor designers assume that the traffic between the user and the server is already encrypted. Otherwise, the exit node in the Tor mix-network can sniff the message networks. Based on this restriction, Swede Dan Egerstad was equipped with 5 Tor exit nodes and could sniff around 100 log-in credentials belonging to different consulates in different countries. This example shows us that any security architecture and tool should be designed in a very dynamic way. The tools for mobile identity management should also be able to enforce different security mechanisms only with small configuration changes.

5 The Aspects

Based on their experiences and analysis of existing systems, Lederer et al. [23] explain 5 pitfalls against the design of technical systems related to personal privacy. The first pitfall is *obscuring potential information flow*. The technical systems should let users know what kind of information are collected about them, its purpose, duration and the receivers. The second pitfall is *obscuring actual information flow*. Users should exactly know what actions are executed and nothing should be hidden. For example, if a cookie is set on users' device, they should be informed. The third pitfall is *emphasizing configuration over action*. The systems should not require so many configurations and expect users simply to live by them. The forth pitfall is *lacking coarse-grained control*. Users should be in the position of canceling any data transfer or blurring of personal data. The last pitfall is *inhibiting established practices*. Designs of technical systems should employ effectively the privacy patterns (e.g. blurring, anonymization, data limitation, etc.).

Considering all these pitfalls, we explain in this section the required aspects for identity management and evaluate them from the perspective of the Friend Finder, i.e. a pull context-aware application. The aspects are not directly specific only to mobile identity management. But their evaluation is specific to context-aware mobile applications.

5.1 Context-to-Context Dependence

A user can have both *static* context data like name, surname, address or *dynamic* context data like current location, local weather conditions, velocity in his car, etc. There is a very tight dependence between different context data in terms of privacy. For example, name-surname pair is dependent on address data and vice versa. If someone knows your name and surname, it is not so difficult to find out your address. That means if you give away your name-surname, you also give away your address. Similarly in location-aware applications, if you know one's current location with the velocity and direction, it is not difficult to reveal his future location within a one hour. Considering the Friend Finder application, it is not difficult to find out the identity of a particular person if you get to know his friends list. Mobile identity management systems should allow users to specify their privacy preferences. You can explicitly specify which of your personal data is released or not released.

The *context2context dependence* aspect should be integrated within mobile iden-

tity management system of the Friend Finder application. In case there exist any logical conflictions during data release, mobile users should be warned and asked how to proceed by the mobile identity management system. Providing this, the pitfalls "obscuring potential and actual information flow" can be avoided.

5.2 Context-to-Context Relation

During the management of privacy preferences, your choices are affected by the relations between different context data. As a simple example, there is a relation between the *location* and *time*. You can specify a preference like "*I do not want to release my* location *at the* weekends". Similarly, *location:(time,person)* relation can also exist."*I want my boss to get to know my location only at weekdays*" is an example for such a relation. *location:own_location* relation can be explained with the example "*I do not want to reveal my location if I am in Stuttgart*". The relation *location:remote_location* can be given as "*I do not want to reveal my location if the other party is not in the same building as me*". Static data can also have this kind of relation. *interest:interest* relation for location-based chat means that "*I release my interests only to people who hold the same interests*".

The *context2context relation* aspect should be also a part of the mobile identity management system of the Friend Finder application. Its privacy preference language should support specifying context2context relations in terms of privacy. This aspect, as a privacy pattern, avoids the pitfall "inhibiting established practices".

5.3 Blurring in Levels

Blurring of a personal data means that giving the personal data not in an exact form but rather in ranges or in a more abstract form. Blurring can help to protect privacy and identity. You can give out your exact salary. But this data can give hints about your job status, life standard, etc. If possible, the salary can be given in ranges which makes such conclusions more difficult. Location blurring can also be applied. Location tracking can be prevented by applying blurring. For certain applications, it should be enough to give only the city name or zip code instead of exact GPS coordinates. For indoor applications, location blurring can be also very helpful. Giving exact room number you are in is not something you would prefer to release easily. Instead, you can blur it and reveal only the building name if it does not hurt the functionality of the application.

Blurring can be applied in levels. For example, for outdoor locations; GPS coordinates, street name, zip code, city, country and continent can compose such location levels. For indoor locations; room number, floor number and building name can compose the levels. Blurring in levels can also be used to improve the quality of service. Assume you hold your PDA and are in the city center of Stuttgart. You are interested in finding restaurants around you. You can either give your exact GPS coordinates or you can release your zip code or city name. If you release your GPS coordinates, the service provider presents a visual map which directs you to different restaurants around. If you give only the zip code, than you get the restaurants as

a simple text list with addresses.

Blurring can improve the privacy and also the quality of service. The pitfall "lacking coarse-grained control" can be avoided by the integration of blurring in levels aspect. Hence, the mobile identity management system of the Friend Finder application should support blurring mechanisms for any context data possible.

5.4 Extensible Preference Language

The specification language for privacy preferences is very important for mobile identity management. Appel [1] as privacy preference language has limitations for identity management [20]. It is not straightforward to extend Appel for the integration of the aspects explained in this paper. The preference language for the Friend Finder application should take into consideration different static and dynamic context data, their dependencies and relations and also blurring in levels.

Our proposal for such a preference language is illustrated in Figure 2. User privacy preferences are encoded in xml format. The mobile identity management system of the Friend Finder rejects any data release unless any exception has been defined by the mobile users for a particular role (i.e. group of persons) or a person. The context data to be protected is defined with the tag *protected* and its attribute *property*. Each protected element contains one or more *exception* tags which consist of the attributes *role* and *id* and *if* tags for the validation of the exceptions. The exception can be defined for a certain group with the attribute role or a certain person with the attribute id. An exception is also evaluated as true, if only all *if* conditions are validated as true. Each if tag contains a *context* attribute (i.e. the context data for validation), a *condition* attribute (i.e. the comparison structure) and a *value* attribute.

```
<protected property="location|name|interests|velocity">
   <exception role="family|work|private|..." id="wife|boss|..">
    <if context="location" condition="is|is-not" value=" " />
    <if context="time" condition="is|is-not|before|after" value=" " />
    <if context="interest" condition="similar|not-similar" value=" " />
  </exception>
    .....
 </protected>
```

Fig. 2. The Structure of Exceptions for Privacy Preferences

As a concrete example, you want your boss to access your location information only at week days from 9.00 to 18.00 and your wife to access it anytime unless you are not outside Germany. The relevant preferences can be expressed as in Figure 3.

```
<protected property="location">
  <exception role="family" id="wife">
    <if context="location" condition="is-not" value="Germany" />
  </exception>
  <exception role="work" id="boss">
    <if context="time" condition="is-not" value="weekend" />
    <if context="time" condition="between" value="09.00-18.00" />
    <if context="location" condition="is-not" value="Germany" />
  </exception>
</protected>
```

Fig. 3. A Sample of Privacy Preferences for Location

Similarly, if you want to reveal your interests only to persons whose interests are similar as yours, the relevant privacy preferences can be defined as in Figure 4.

```
<protected property="interest">
   <exception role="*">
     <if context="partner_interest" condition="similar" value=$own_interest />
   </exception>
</protected>
```

Fig. 4. A Sample of Privacy Preferences for Interests

5.5 Trust Management with P3P

After releasing your personal data to a service provider, you can not control whether your data is misused or not. It can then be used for profiling, forwarded to other parties, used for spamming, etc. You need some trust relation with your partners before you release your data. With P3P [16], you can build this trust relation with your partners. By publishing its P3P policy, a service provider exactly explains what kind of personal data it collects, its purpose and duration of the collection, the other receivers of the personal data, whether the user can be identified from the collected data, etc. You check this policy automatically with Appel preference language and decide whether or not to communicate with the provider. P3P does not guarantee the enforcement of the policies, but it can be evaluated as a promise of providers.

The mobile identity management systems should be equipped with P3P support and a suitable preference language as explained in Section 5.4. Integration of P3P avoids the pitfalls "obscuring actual and potential information flow" and "lacking coarse-grained control". Moreover, before any data is released to service providers, this is asked to mobile users to allow or not for the transmission. This is an extra mechanism for avoiding the relevant pitfalls.

5.6 Status as Soft Shut-Down Button

The privacy of users are directly concerned with the status and mood of users. If a user is busy or away, he would not want to interact with any application. Similarly, if he is very angry or upset, he would refuse to take part in any mobile service. Therefore, a *status* option is inevitable for the mobile identity management system of context-aware applications. If a mobile user switches his status from online to offline, any data release should be automatically stopped.

The avoid of the pitfall "lacking coarse-grained control" requires a simple mechanism to cut off the transfer of data and with a simple status option, this can be achieved in the mobile identity managemet system for the Friend Finder application.

5.7 History Management

History management in mobile identity management systems allow mobile users to follow their past activies (i.e. the released context data, date, time, the corresponding partner, etc.). Besides, the history management allows users to interact

directly with the receivers of their personal data, inform about the cancellation of their consent and make them delete their personal data from their media.

Integrating history management within the Friend Finder's identity management system, mobile users would be able check at any time to whom they have given away their location information. Therefore, the pitfalls "obscuring potential and actual information flows" and "inhibiting established practice" are avoided.

5.8 Confidential Data Management

With the increasing popularity of mobile devices, confidentiality of mobile data has become more serious. Many mobile devices (e.g. laptops, PDAs, mobile phones) are either forgotten in taxis or public transport or they get stolen. If the mobile data stored on devices are not encrypted, the confidentiality of personal data is left in danger.

Mobile identity management systems deal with personal data that are normally very sensitive data. Therefore, the mobile identity management system should apply encryption techniques on the fly and prevent illegal access of unauthorized people to confidential information. This aspect is related to privacy patterns and thus avoids the pitfall "inhibiting established practice".

5.9 Content and Communication Anonymity

Content anonymity requires staying anonymous at application level. Pseudonyms can be used for enforcing content anonymity. Communication anonymity is related to network level anonymity. If a user communicates directly with a service provider, he leaves many signs that can be used for revealing the real identity of the user [4]. Communication anonymity networks and the relevant tools [15,9,19] today exist for preventing service providers from identifying of users.

The mobile identity management systems should be equipped with such tools and pseudonym-support and enable users to communicate anonymously both at application and network level. Providing this, the pitfall "inhibiting established practice" is avoided. Besides, the mobile identity management hides the complexity of enforcing anonymity from users and therefore avoids the pitfall "emphasizing configuration over action".

6 The Aspects in Action

In this section, we integrate the aspects explained in the previous section within the Friend Finder application as illustrated in Figure 5. In our example, the location provider as a trusted party exists and collects location information from mobile users. Mr. Fischer, as a mobile user, allows his wife and his boss to query his location and track his movements on a visual map displayed on their mobile devices. The map provider receives the location information of mobile users from the location provider and presents them on a visual map for the mobile users.

[4] For a complete list of data revealed in case of direct communication, refer to http://gemal.dk/browserspy/

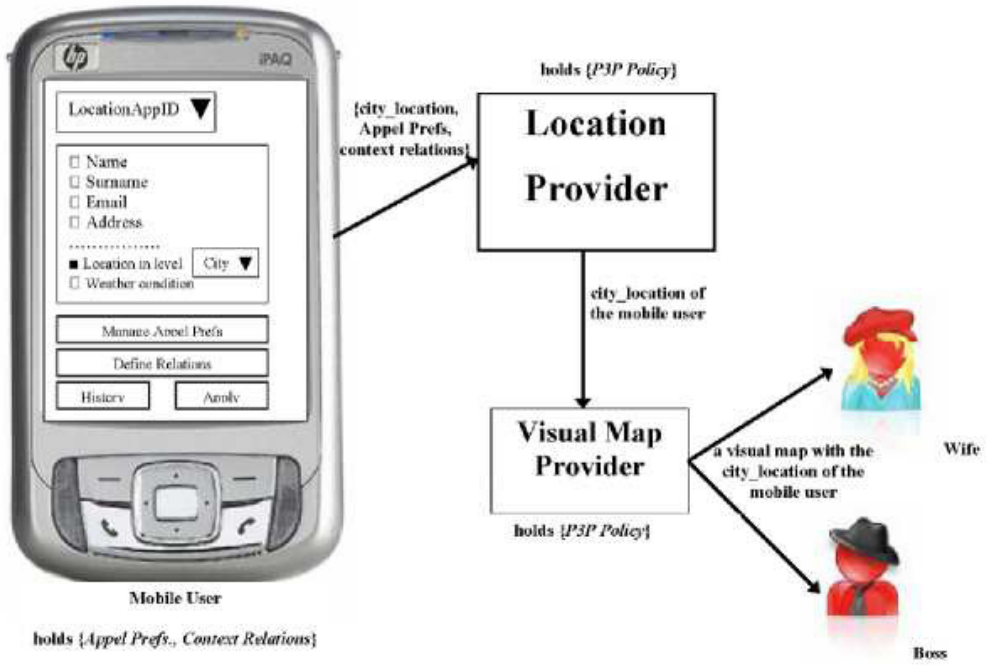

Fig. 5. The Aspects integrated in the Friend Finder Application

We emphasize the aspects explicitly in this application scenario as follows: Before communicating with the location provider, mobile users specify which static and dynamic data are sent to the location provider. As shown in the Figure 5, Mr. Fischer releases his location information in *city level*. This is the integration of the aspect "*blurring in levels*". Additionally, he can push the button "Manage Appel Prefs." and specify his Appel privacy preferences for the trust management with the location provider and map provider. He can also specify some exceptions related to the aspect *context-to-context relations* like "my location information should be sent to my boss only in the weekdays from 09.00 to 18.00" or "my location information should be sent to my wife any day if I am in Germany". In order to express such relations, we need an extensible preference language. These are the integration of the aspects *context-to-context relation* and *extensible preference language*. Mr. Fischer can also access his history data summarizing what kind of information was released, at what time and to whom by pressing the "History" button. This is the aspect *history management*.

Afterwards, Mr. Fischer presses the "Apply" button and the communication with the location provider starts. Initially, the P3P policy of the location provider is retrieved and compared with his Appel preferences (i.e. the aspect *trust management with P3P*). If there is not any confliction, he is asked to confirm that his location data will be sent periodically. At this point, the aspect "context-to-context dependence" comes into the play. Mr. Fischer did not choose the attribute "weather condition" to be released. But since the current location as the city name

is released, it is also clear that the receiver can easily find out this attribute. He is warned against this confliction. If he confirms, his location is sent within a periodical time to the location provider. For the first time, he sends also his Appel preferences and context relation rules. The location provider takes his preferences and the exceptions into consideration and evaluates them before his location data is forwarded to other principals.

When the visual map provider asks for his location information, the location provider compares his Appel preferences and the P3P policy of the visual map provider. It also checks the exceptions for the context relations and then releases the relevant data to the visual map provider. In addition, if Mr. Fischer communicates directly with the map provider, the communication is built upon an anonymous network automatically (i.e. the aspect *anonymity*).

7 Conclusion

Identity management is a requirement for the Internet users which share their personal data with service providers to protect their privacy. Considering context-aware and especially location-aware applications in which users current location data is distributed between different parties, mobile identity management has become inevitable. Today, we need privacy-enhancing tools to support mobile identity management. Additionally, for context-aware applications, the relevant aspects for identity management need to reevaluated and enhanced. In this paper, we focused on a certain push context-aware application (i.e. the Friend Finder application) and evaluated the required aspects (i.e. context-to-context relations and dependence, extensible preference language, blurring in levels, trust management with P3P, status as soft shut-down button, history management, confidential data management and content/communication anonymity) from the perspective of mobile identity management in the Friend Finder application.

References

[1] *A P3P Preference Exchange Language (Appel)*, http://www.w3.org/TR/P3P-preferences/.

[2] *Checkmate-Mobile Friend Tracking*, http://mysql3.inf.dcn.yahoo.com/checkmates/.

[3] *EU Directives 2002/58/EC*, http://www.dataprotection.ie/documents/legal/directive2002_58.pdf.

[4] *EU Directives 95/46/EC*, http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

[5] *FIDIS (Future of Identity in the Information Society*, http://www.fidis.net.

[6] *FIDIS Project - Database on Identity Management Systems*, http://www.fidis.net/interactive/ims-db/.

[7] *Friend Finder Application*, www.herecast.com.

[8] *idemix-a tool for pseudonymity for e-transactions*, http://www.zurich.ibm.com/security/idemix.

[9] *JAP: Anonymity and Privacy Tool for Internet*, http://anon.inf.tu-dresden.de.

[10] *Locating people in emergency*, http://www.sintrade.ch.

[11] *Location-based chat and games*, http://www.vodafone.de.

[12] *Location Based Services Application Prototype*, https://www.prime-project.eu/prototypes/lbs/.

[13] *Phishing attacks on Tor anonymisation network*, http://www.heise-security.co.uk/news/95778.

[14] *PRIME - Privacy and Identity Management for Europe*, https://www.prime-project.eu.

[15] *The Anonymizer*, http://anonymizer.com.

[16] *The Platform for Privacy Preferences*, http://www.w3.org/2006/07/privacy-ws/.

[17] *Tracking of kids*, http://www.trackyourkid.de.

[18] Ackerman, M., T. Darrell and D. Weitzner, *Privacy in context*, The journal of Human-Computer Interaction **16** (2001), special Issue on Context-Aware Computing.

[19] Dingledine, R., N. Mathewson and P. Syverson, *Tor: The second-generation onion router*, in: *Proceedings of the 13th USENIX Security Symposium*, 2004.

[20] Giles Hogben - Suggestions for long term changes to P3P, *W3C Workshop on the long term Future of P3P and Enterprise Privacy Languages* (2003).

[21] Gutscher, A., *Coordinate transformation - a solution for the privacy problem of location based services*, in: *IPDPS*, 2006.

[22] Jendricke, U. and D. G. tom Markotten, *Usability meets Security - The Identity-Manager as your Personal Security Assistant for the Internet*, in: *Proceedings of the 16th Annual Computer Security Applications Conference*, 2000, pp. 344–353. http://www.acsac.org/2000/papers/90.pdf

[23] Lederer, S., I. Hong, K. Dey and A. Landay, *Personal privacy through understanding and action: five pitfalls for designers*, Personal Ubiquitous Computing **8** (2004), pp. 440–454.

[24] Pfitzmann, A. and M. Hansen, *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - Consolidated Proposal for Terminolog* (2007).