

Extending P3P/Appel for Friend Finder

Emin Islam Tatli

Department of Computer Science, University of Mannheim

tatli@th.informatik.uni-mannheim.de

Abstract

FriendFinder as a location-based service collects location data from mobile users and distributes a particular user's location upon request. Privacy of users data especially location data needs to be guaranteed according to both user and legacy perspectives. W3C's privacy recommendation for internet platform P3P/Appel only considers the privacy relations between the users and the service providers. In this paper, we explain the shortcomings of P3P/Appel for providing privacy in FriendFinder and propose enhancements to the P3P/Appel policy languages.

1 Motivation

With the support of computing location in the mobile platform, location-based services like locating people, locating moving objects (e.g. fleet management), etc. have been already implemented today. *FriendFinder* is a typical example of locating people service [5]. As illustrated in Figure 1, the users participating in the *FriendFinder* service send regularly their location data computed by their mobile devices to the central *Location Provider* and can also query the location of their particular friend through the location provider. Before the users join in the service, they need to authenticate themselves to the location provider.

The users utilize mobile devices (e.g. mobile phones, PDA, laptops, etc.) for getting the service. Each mobile device has different hardware capabilities and the content provider should know the capabilities of the mobile devices for creating the most suitable content for the devices. Hence, each mobile device sends a reference link that contains the device capability features in the request's http header. With User Agent Profile (UAProf) [8] specifications, each mobile device's characteristics like screen size, model, input character set, etc. can be defined in xml format. As a specific example, the http request sent by Nokia 6230i contains "*x-wap-profile: http://nds1.nds.nokia.com/uaprof/N6230ir200.xml*" line in the http header and the content provider refers to the device

features described in this link to compose the most suitable content. For the *FriendFinder* service, it is assumed that the content provider is a part of the location provider.

On the other hand, user privacy as a non-functional security requirement becomes a big barrier against the success of location-based services. Users have privacy doubts regarding the location provider and other users which can collect and misuse their personal data. Considering the privacy risks, W3C has published a recommendation called Platform for Privacy Preferences (P3P) [7] which is a xml-based language for privacy policy encoding. Appel [2] (A P3P Preference Exchange Language) is also a specification language for user privacy preferences specific to P3P. But considering the privacy doubts of the users in *FriendFinder*, P3P does not cover all user privacy aspects.

In this paper, we discuss the possible privacy risks in *FriendFinder*, explain all privacy aspects, especially the aspects which are not considered for the user privacy and propose enhancements for the P3P/Appel policy languages.

The paper is structured as follows: Section 2 enumerates possible privacy risks in the *FriendFinder* service. The EU directives about the personal data protection are given in Section 3. A privacy policy encoded in natural language and P3P are given in Section 4 and 5 respectively. The shortcomings of P3P for privacy management are discussed in Section 6. Section 7 proposes the extensions for the policy languages and the related work is given in Section 8. Finally, Section 9 concludes the paper with a discussion and future work.

2 Privacy Risks

There exist a number of privacy risks in the *FriendFinder* service against users. The possible *attackers* are the other users, the location provider or other third party providers. The privacy risks are:

1. Location- and Action-relevant Risks:

With the aim of tracking users and their actions, the attackers can analyze collected location data. They can target a single user, store his location data and analyze it to reveal where he stays (e.g. if he is in a night

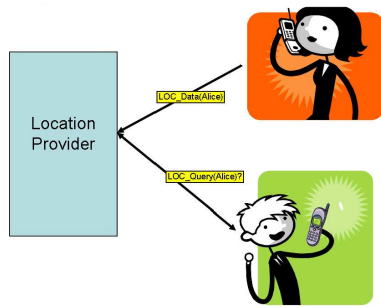


Figure 1. FriendFinder Service

club or fitness center), follow his actions or even guess the place at which he would be in the future. Besides, other users as attackers can try to reveal the location of a particular user without having any permission.

2. Relation-relevant Risks:

With the aim of revealing the relations among the users, the attackers can find out who stay in the same place or travel through the same direction at the same time. They can also collect friend-search queries, analyze which person communicates with whom and reveal the relations among the users.

3. Monetary Risks:

UAProf data can expose device capabilities (e.g. phone type showing whether it is a cheap or costly device) and user preferences (e.g. font size revealing the user's visual acuity). The location provider can collect UAProf data sent by the users and profile them according to their mobile device types. The profiles can be shared with the third party mobile device companies to send advertisements to the users. This is a spamming problem and threatens the privacy of the users. Besides, getting UAProf data the thieves can find out costly devices and target their owners.

Dynamic pricing is another monetary risk. The location provider analyzes how frequently the users retrieve the service and apply dynamic pricing which means that different users pay different amounts for the same delivered service based on their activeness. In the same way, UAProf profiles revealing costly device owners can cause dynamic pricing.

4. Medical Data Risks:

Profiling the devices with big font sizes and displays with image-disabled functionality which are revealed by UAProf data can threaten the medical privacy of the device owner with a weak visual acuity.

3 EU Directives for Privacy

Privacy has also legacy aspects. The European Parliament and the Council of the European Union have published the directive 2002/58/EC [3] that is concerned with the processing of personal data and the protection of privacy in the electronic communication sector. This directive is a complement of the EU Directive 95/46/EC [4]. Relevant to FriendFinder service, the EU Directive 2002/46/EC contains the issues like security, confidentiality, data storage and location data. Considering the legacy aspects, the privacy and security threats should be taken into consideration when software architectures are designed and PET (privacy enhancing technologies) tools should be integrated within the software architectures.

3.1 Security - Art. 4

The service providers must take appropriate measures to safeguard the security of their services. If a particular security risk exists, the users should be informed of these risks and any likely costs involved with providing the possible remedies.

3.2 Confidentiality - Art. 5,6

Member States shall ensure the confidentiality of communications and the related traffic data through national legislation. They shall ensure also that the access and process of the data is allowed only if the user concerned is clearly informed and gives his consent.

3.3 Data Storage - Art. 6

The user data can be stored and processed by service providers for the duration necessary for the services and billing purpose. Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done. But the data stored must be erased or made anonymous when it is no longer needed for the purpose of the transmission. In addition, the users should be always in the position of withdrawing their consent to store and process their data.

3.4 Location Data - Art. 2,9

Location data means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than

traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

4 Privacy Policy in Natural Language

A privacy policy for FriendFinder service which keeps in mind the legacy aspects specified in the EU directives is given informally in this section.

Regarding security and confidentiality; the location provider should inform the users for the possible security and privacy risks in this service and provide confidentiality of user data especially location data against unauthorized disclosure by applying the relevant encryption techniques.

Regarding data collection; the location provider should not collect any information that is not relevant for transmitting its service and guarantee that no data is stored longer than the duration that is necessary for the service transmission. Especially the users should be provided with the information that who is collecting data, what information is being collected and the purpose, the other data recipients, the access rights, the retention policy and the dispute policy.

Regarding data forwarding from the location provider to other parties, it should only happen if the user is informed for this transmission before and gives his consent. In addition, the user should be in the position of withdrawing their consent for sharing this data with other service providers.

Regarding UAProf profiles; no real profile should be sent to location provider unless their privacy policies and the user's preferences are negotiated. If this is a technical requirement to initiate the communication, then an *empty* profile should be transmitted at the beginning [1].

Regarding other users; the location provider should release the location data of a particular user to other users if only they get explicitly authorized by this user. Moreover, the user should be in the position of withdrawing his consent for location release to the location provider, a particular user or all users under some circumstances like at certain dates, at certain mood or busyness.

5 Privacy Policy in P3P

Platform for Privacy Preferences (P3P) is a recommendation of W3C. It aims protecting web users against internet privacy risks. P3P server policies are encoded in machine-readable XML format. Within a P3P policy, a service provider can specify its identity data, the data it collects and the reason, the retention period, the dispute policy, whether the users can be identified with the collected

data and the parties that can access the data. In addition, the users specify their privacy preferences in Appel [2] (A P3P Privacy Exchange Language). Before the user starts communication with the service provider, the user's P3P-enabled agent retrieves the server's P3P policy, compares with the privacy preferences and interacts with the user to decide how to proceed in case there is a conflict between the server's policy and the user's preferences. If there is no conflict, the agent initializes communication with the service provider.

P3P does not cover all user privacy aspects that are explained in the previous section, because the main consideration of P3P is only the service provider. On the other hand, the user's privacy issues are related to the user himself, the environment and other users as well. P3P only controls data collection and forwarding privacy aspects. In Figure 2 and 3, a part of a sample P3P policy is given to illustrate privacy policy specification.

```
<ENTITY>
<DATA-GROUP>
<DATA ref="#business.name">Location Provider Service</DATA>
<DATA ref="#business.contact-info.online.email">p3p@example.com</DATA>
<DATA ref="#business.contact-info.online.uri">http://www.example.com</DATA>
<DATA ref="#business.contact-info.postal.organization">University</DATA>
<DATA ref="#business.contact-info.postal.street">University Address</DATA>
<DATA ref="#business.contact-info.postal.country">Germany</DATA>
</DATA-GROUP>
</ENTITY>
<ACCESS><all/></ACCESS>
<DISPUTES-GROUP>
<DISPUTES resolution-type="service"
service="http://www.example.com/p3p_dispute.html"
short-description="Dispute">
<LONG-DESCRIPTION>
For any inconvenience, apply to our Customer Service (dispute@example.com)
</LONG-DESCRIPTION>
</DISPUTES>
<REMEDIES><correct/><money/><law/></REMEDIES>
</DISPUTES-GROUP>
```

Figure 2. P3P Sample Policy

The data like the name and contact information about the policy holder are specified in *ENTITY* tag. The policy specifies with the *ACCESS* tag whether the user is allowed to view or update his/her collected data. In this policy, the users are given access to all identified data. The privacy holder defines the possible solutions for any disputes under *DISPUTES-GROUP* tag. For example, this policy specifies that in case of any dispute the customers can contact to the customer service. For remedies the error can be corrected, governing law can specify the remedies or monetary damages can be paid to the users.

Each *STATEMENT* tag specifies a group of personal data, the purpose of data collection, the consequence, the identifiability, who can access the data, and the retention time. *PURPOSE* tag specifies that the collected data can be used for both the main purpose which is for the distribution in the FriendFinder service (implied by *<current/>* tag) or individual analysis for determining individual characteristics (implied by *<individual-analysis/>* tag). *RECIPIENT*

```

<STATEMENT>
  <EXTENSION optional="yes">
    <GROUP-INFO name="Location"/>
  </EXTENSION>
  <CONSEQUENCE>
    Location data will be collected with the aim of enabling the service.
  </CONSEQUENCE>
  <PURPOSE>
    <current/><individual-analysis/>
  </PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
    <DATA ref="#dynamic.miscdata"><CATEGORIES><location/></CATEGORIES></DATA>
  </DATA-GROUP>
</STATEMENT>

```

Figure 3. P3P Sample Policy (cont.)

tag has the value `<ours/>` which means only the service provider and its agents can access the personal data. RETENTION tag has the value `<stated-purpose/>` which requires information to be deleted at the earliest time possible.

6 Shortcomings of P3P/Appel

A user's privacy preferences can be related to the service provider, the user himself, other users and the environment as depicted in Figure 4. But P3P considers the privacy concerns of a user with the relation of *only* service providers. Therefore, FriendFinder needs more comprehensive privacy policies for user-centric privacy management.

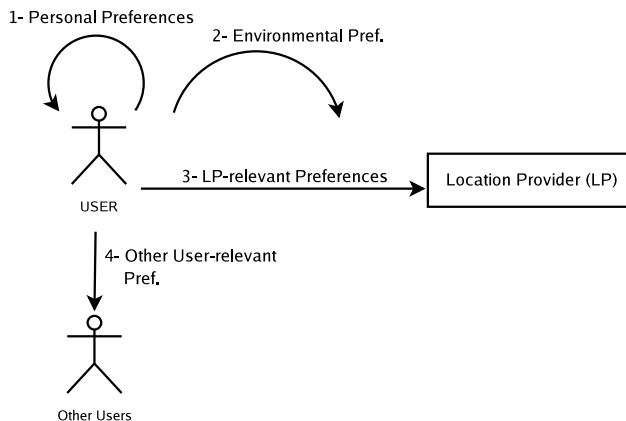


Figure 4. Privacy Concerns of Users

P3P policies and Appel preferences should be extended to cover all user privacy aspects. The shortcomings of P3P/Appel according to the all privacy factors are explained in the following subsections:

6.1 Factors relevant to Location Provider

By comparing the provider's P3P policy with the user preferences, the user privacy related to the provider can be enforced. But there are still some shortcomings of P3P

and Appel to express the user privacy preferences related to server side. These include:

- a) Policy negotiation is not possible with P3P. But the privacy sensitivity of users can be different and therefore the service providers should be in the position of presenting different privacy policies that enable policy negotiation with different user preferences.
- b) P3P policies are static and do not support dynamic evaluation. For example, quality of service based on the blurring level of the location can not be expressed in P3P. As a dynamic privacy aspect, the user may want to be navigated to a certain restaurant if he gives his exact location. If he blurs his location and gives only the zip code for example, then he could get a list of the restaurants in that area as plain text. Such dynamic behaviors are not concerned in the P3P specification.
- c) The EU privacy directives require that for the confidentiality of user data, encryption techniques should be enforced, but you can not express this privacy requirement in Appel preferences and check whether the service provider support encrypted secure channel for client communications.

6.2 Factors relevant to the User

At certain conditions, the user may not want to participate in the FriendFinder service and reveal his location to others. As examples:

- a) at certain dates and times, e.g. on holiday, in the evenings, at the weekends, etc.
- b) based on the mood or status of the user, i.e. if the user is very unhappy or away.
- c) based on location (if his location is a certain place, e.g. X street, only then he reveals his location).

6.3 Factors relevant to Other Users

Based on the identity and conditions of other users, the user may not want to reveal his location to a particular user. As examples:

- a) only the users with certain identities can access the location of the user
- b) only the users that are at a certain location can access the location of the user, e.g. the users that are in the same building as the user is in

6.4 Environmental Factors

The user's privacy concerns can also be affected from the environment like application type (i.e. indoor/outdoor application), physical conditions (e.g. light, pressure, etc.), network infrastructure, etc. As examples:

- a) if only the service is an outdoor application, the user participates in the service.
- b) if the service is an outdoor application, the user releases his exact location (e.g. GPS coordinates). Otherwise he wants to blur his location and gives away only building name instead of the floor name and/or room name.

7 Extensions to P3P/Appel

P3P and Appel need to be extended for integrating them within a complete privacy architecture for FriendFinder or generally speaking for location-based applications. They should be extended in such a way that they support negotiation, encryption and dynamic evaluation. Moreover, the policy and preferences languages should be extended for supporting context-based features stemming from the user, the environment and other users as explained in the previous section. The context-based features of the user can be the user identity (e.g. name, address, phone number, etc), the user profile (e.g. user interests, schedule, etc.), his morale, his busyness, location and time. The features of the environment can be physical conditions (e.g. light, pressure, etc.) and the network infrastructure (e.g. indoor application, outdoor application, etc.). The features of the other users are similar to the user's features.

There exist a tight relation between all these features in terms of privacy. One feature affects the user over another features in terms of privacy level. For example, the feature identity is affected by the feature morale status. The user may not want to share his location with another user if he is angry with him. Or similarly, if the user is very unhappy, he would stop sending his location data to the location provider in order not to let others know his location. As an example for the relation between location and the network infrastructure, the user would blur his location for indoor application, whereas he gives his exact location for outdoor applications. It is clear from these examples that any feature can be a privacy evaluation factor for another feature and P3P/Appel should be extended in such a way that all these feature-to-feature relations can be expressed in policies for user privacy management.

In Figure 5 depicting the feature relations, it is shown that to protect the features of the user and the environment, it should be possible to evaluate all other features within privacy policies and preferences. After the evaluation, the

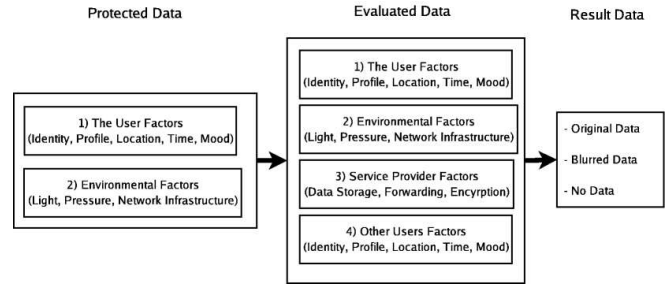


Figure 5. Feature Relations for Privacy

original private data can be released to others, or blurred version is released or the data is not given away.

8 Related Work

Myles et al. designed an architecture for preserving privacy in environments with location-based applications [10]. They extend the P3P policy language in order to cover also location-based applications. Mobile users initially send their privacy preferences called *validators* to the central location server. To make a location request for a particular user, the service providers should send their privacy policies to the location server. Afterwards, the validators are evaluated with the request and the relevant privacy policy. If this process is successful, the location is sent to the service provider.

pawS [12] is a privacy awareness system for ubiquitous computing environments. It uses P3P policies to specify privacy concerns for collected data and the Appel language to specify the user privacy preferences. The mobile device runs a mobile privacy assistant that communicates with the ubiquitous devices, receives their privacy policies, compares with the user preferences and finally accepts or rejects the communication with the ubiquitous device.

In the Wasp project [11], the Appel language is extended to support context-based applications. They add the support for date, time, day of the week and location entities in the preference language. This is a good approach to show that P3P can be extended to support context-based applications. But the work supports only basic context data. As shown in Figure 5, more context data and the rules considering context-to-context relations should also be integrated within the preference language. This provides, if some context values do not satisfy the privacy conditions, refuse to send this context data instead of not using the service at all.

The EU project Prime [9] aims at developing user-centric identity management solutions for privacy. *idemix* [6], a prototype tool of Prime, provides anonymous authentication over the internet services.

Considering the existing works, we believe our enhanced privacy policies and preferences complements two main lacks in the privacy area for context-based applications. Firstly, the set of context data we evaluate is very broad and not restricted with a small set of context. Secondly, we support dynamic policies, i.e. restrictions on context data can be formulated based on the values of other context data.

9 Discussion and Future Work

P3P is a good privacy approach for web users, but user privacy management for location-based services requires more than P3P. Other privacy aspects of users stemming from personal, environmental and other users-relevant factors should be also taken into consideration for an enhanced privacy management. P3P policy and Appel preferences languages should be extended by covering all privacy aspects of users. Moreover, P3P and Appel need to support dynamic behaviors of services like checking if encryption is enforced. As a future work plan, we focus on implementing a complete architecture for user-centric privacy in location-based business applications, extend P3P/Appel data languages according to context-to-context relations, integrate the new enhanced policies and preferences within the privacy architecture and do usability experiments with end users.

References

- [1] Nilsson, M. et al. Privacy Enhancements in the Mobile Internet. Proceedings of the IFIP WG 9.6/11.7 conference on Security and Control of IT in Society, June 2001.
- [2] A P3P Preference Exchange Language (Appel). <http://www.w3.org/TR/P3P-preferences/>.
- [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] Friend Finder Demo Application. www.herecast.com.
- [6] idemix-a tool for pseudonymity for e-transactions. <http://www.zurich.ibm.com/security/idemix>.
- [7] P3P. www.w3.org/2006/07/privacy-ws/.
- [8] UAProf (User Agent Profile) Specification. <http://www.openmobilealliance.org/tech/affiliates/wap/wap-248-uaprof-20011020-a.pdf>.
- [9] PRIME - Privacy and Identity Management for Europe. <https://www.prime-project.eu>, 2006.
- [10] Ginger Myles et al. Preserving privacy in environments with location-based applications. *IEEE Pervasive Computing*, 2(1):56–64, 2003.
- [11] M. Zuidweg et al. Using p3p in a web services-based context-aware application platform. <http://www.w3.org/2003/p3p-ws/pp/utwente.pdf>.
- [12] Marc Langheinrich. A privacy awareness system for ubiquitous computing environments. In *Proceedings of the 4th international conference on Ubiquitous Computing*, pages 237–245, London, UK, 2002. Springer-Verlag.