A Dynamic Approach for User Privacy Management in Location-based Mobile Services

Amr Ali-Eldin
Ordina ICT B.V.
Management & Consultancy
Ringwade 1, 3439 LM, Nieuwegein, the Netherlands
Tel.: (+31)30 663 7315
Fax: (+31)30 663 7496
e-mail: amr.ali-eldin@ordina.nl

***Abstract*— Recently, we have noticed the wide spread of GPS enabled mobile phones, which enable mobile applications to track users locations and start pushing customized advertisements to them. For a small benefit a user might get from these Ads, a user might be willing to share his or her location without even knowing the impact this might have on his or her privacy. In this paper, we propose a dynamic approach for evaluating those coming requests for users' locations based on users pre-described privacy preferences by providing users with what we call a *Privacy Threat Level* (*PTL*) indicator. We have developed a simulation console and presented a scenario showing how this approach can work in practice.**

Keywords-Privacy; User preferences; Information Collectors; Smart Phones; Service Providers; Pervasive Computing; Location-based services (LBS)

I. INTRODUCTION

Recent development in pervasive computing have paved the way for the deployment of pervasive and ubiquitous services [1]. We have also seen how the introduction of the latest technology of smart phones like iPhone 4, Blackberry, Android, iPads etc. has led to a complete set of location-based services (LBS) capabilities like road navigators for example. LBS collect and use users location to provide new or improved services [2]. Despite the benefits these services can bring to users and stakeholders, they pose a threat to user privacy. We have also noticed that most smart phones now come with a built-in GPS capability, which makes it possible for mobile applications to get users location and start pushing advertisements and services. According to a recent survey by the Mobile Marketing Association (MMA) [3], about two thirds of iPhone owners now use location-based services at least once a week mostly to locate nearby points of interests, shops and services. Location information may be collected rather unobtrusively or passively and used by service providers without users' notice or informed consent and that represents a real threat to user privacy.

Consider the case, a system engineer Jo works for a system developing international company, which supports different oil refining sites located in the sea. Jo has a smart phone with an application installed that is called BeThere. BeThere provides Jo with the logistic services to help him with his work activities and guarantee his safety. If Jo wants to leave one site to go to another, he plans his trip via BeThere. A helicopter comes to pick him up from the place where he is. BeThere also has business partners near each location: tourist guides, hotels and restaurants. BeThere keeps a profile of Jo, which got Jo's personal information such as name, identity etc., payment information, location information, and calendar information.

BeThere business partners or simply third parties will also like to have some of Jo's private information for their services provisioning or promotions even though they are unknown to Jo. This can mean that Jo will not know that they collect private information. Furthermore, Jo will not be able to know, which party collects what information from BeThere even when he is triggered by their push services or Ads. Tourist guides will like to gather Jo's personal, and location information to provide customized guiding. They will collect payment information as well. Hotels will like to gather Jo's identity information and payment information to recommend accommodation in each location. Restaurants will like to gather context information: location, eating preference, and schedules to provide suitable meals (see Fig. 1).

Although Jo's first privacy preferences will be that no third parties can have access to his information, Jo will be interested to use specific services depending on his situation. It is not that he gets push services that he will not be interested in. Sometimes there might be an interesting pop-up with a nice offer, which one cannot refuse. For example, when Jo enters a restaurant, he wouldn't mind it if the restaurant sends him an offer of what they can offer of drinks with a special price. Most of the times we see that LBS services are based on opt-in subscription from the customer. But what we also can see is that these types of services are pushed to customers in a dynamic way. Jo is not against that but would like the process used to get these services to be reliable, simple, flexible and safe. Jo, as many others, is very concerned about having control of his privacy at anytime and everywhere specially with the spread of such push services.

Accordingly Jo, as a customer of BeThere, will like to be able to express his privacy preferences when using BeThere's services. Jo will initially allow travel agencies and tourist guides to have access to his information while entertainment providers will be blocked. Additionally Jo would like to be informed when there is a privacy breach and

 ISBN: 978-1-61208-164-9

to intervene. Last and not least, he wants to be able to change his preferences at any time, which makes the process of managing his privacy preferences complex.

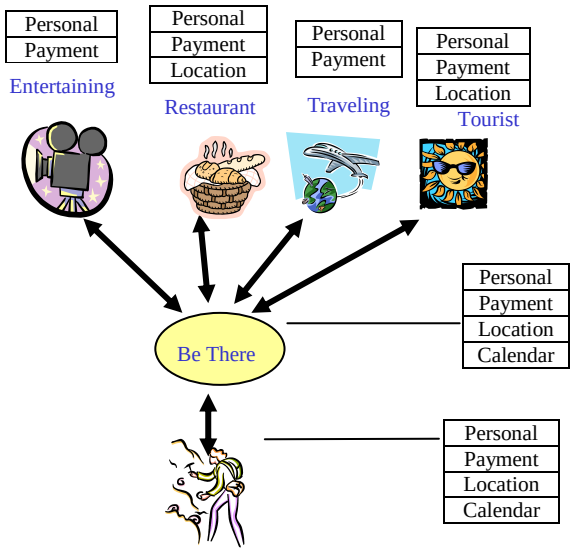

Figure 1. Jo and *BeThere*

The rest of this paper is organized as follows. In Section II, we discuss existing approaches and related work. Then in Section III, we discuss the most relevant principles of the P3P platform. Next, we introduce our proposed Privacy Threat Level *(PTL)* approach in Section IV. Thereupon in Section V, we present a prototype example based on what the concepts where prototyped. We finalize by presenting our conclusions in Section VI.

II. EXISTING APPROACHES AND THEIR LIMITATIONS

Privacy threats emerge as a result of the linkage between user identifying information and his or her context-related data. Therefore, most literature has focused on the separation between both types of information when dealing with privacy issues: whether to control users identities, by controlling identity capturing through the use of anonymity solutions as in [4-8], or by access control mechanisms like [9-12], distributing and encrypting of data packets in [13] and physical security through limiting data access within a specified area in [14].

Most of these approaches presented so far focus on conventional data management techniques, which are static [5, 9-11, 13, 15-17]. In other words, they are not aware of user context. Knowing user's context, it may be possible to recover his or her identity even if his or her real identity itself is not communicated. For example, if an anonymous user (on a chat site) tells someone that he was working for a company X from year 2000 till year 2006. Then, his identity is now limited to employees of company X till year 2006. Knowing employees who left company X in year 2006 and knowing the user's current location and or personal interests can help reveal that person's real identity. Therefore, we like to argue that not only user identity information but other information with different degrees of confidentiality should be protected as well, which in turns represent the context of that user.

Controlling the full collection of user contexts may represent the most realistic approach in pervasive environments towards user privacy protection as we have seen in Jo's case. This can be achieved by either reducing the accuracy of the collected data as in [18] or by enforcing user decisions of whether to allow user context to be collected by a certain party. In order to do so, information collectors' ways of dealing with the user contextual information need to be communicated to the user to be able to make a decision. Besides that users should be able to describe their preferences when it comes to their private information. In Jo's example, when he receives a pop-up pushing some nice meal or drink asking for his location, Jo would like to control who else can get this information. One of the leading efforts in this approach, the platform of privacy preferences (P3P) [19] has defined a way of describing information collectors / service providers data practices that constitute a P3P privacy policy. Each practice possesses a descriptive value that is defined by APPEL, the P3P Preference Exchange Language 1.0 [20], which was proposed as the language for expressing user preferences. We think that a P3P based description of user preferences is considered insufficient for describing a dynamic data enriched environment such as the pervasive and mobile environment because it is focused on Internet applications and may not have support to dynamic situations as we will see later in this paper.

One of the well-known P3P based privacy preferences description approaches is 'AT&T privacy bird' [21]. AT&T privacy birds help Internet users to stay informed about how information they provide to Web sites can be used. An AT&T Privacy Bird automatically searches for privacy policies at every website a users visits and asks users for their privacy strictness levels. They can also customize their preferences themselves by importing an XML pre-defined preferences list. To the best of the author's knowledge, the AT&T privacy bird is not designed to deal with mobile and pervasive environments.

Based on the above-given review of previous research results, we argue that there is a need for the development of a flexible approach for privacy that can deal with the dynamics as present in pervasive and mobile computing environments. By preference, such models should be consonant with existing successful, de facto standard platforms for privacy preferences. In this paper, we adopt the P3P as reference model and add some enhancements to suit with dynamic environments.

III. THE PLATFORM OF PRIVACY PREFERENCES (P3P)

P3P [19] has defined a number of data practices that together constitute a P3P privacy policy. A Privacy Policy is a collection of both vocabulary and data elements that describe the data practices of particular website (or section of a web site). A Privacy Policy includes a sequence of statement elements that may have the following sub elements:

 ISBN: 978-1-61208-164-9

- *Purpose:* A purpose is represented in the P3P syntax as a *PURPOSE* element. Each *PURPOSE* element can contain one or more sub elements that describe a site's reasons for collecting the information. The P3P vocabulary defines twelve kinds of purposes.
- *Recipient:* The recipient defines the party with, which the collected data will be shared. *Recipient* is represented in the P3P syntax as a *RECIPIENT* element, which can contain one or more sub elements that describe kinds of recipients. The P3P vocabulary defines six types of recipients.
- *Retention:* Retention defines the duration for, which the collected information will be kept. Retention is represented in the P3P syntax as a *RETENTION* element, which can contain one or more sub elements that describe kinds of retentions. The P3P vocabulary defines five types of retentions.
- *Consent Behaviour:* The consent is defined in P3P to be of three kinds; *request, limited* and *block*. A request consent means complete agreement from the user, and a block consent means no agreement at all. A limited consent, however, assumes consent with blocking identification information from transmission.

Given these data elements, a typical P3P model for users' privacy preferences (in terms of consent decisions to be made) is based on the following rule description:

{<*purpose*>, <*recipient*>, <*retention*>} ➔ *user consent behaviour*

A. P3P Limitations

As we have discussed above, privacy preferences are used to describe users' allowed data practices, i.e., they define what users allow the service providers or information collectors to do with their information. A user may specify privacy preferences written in APPEL [20]. The process of writing users preferences using APPEL rules that function properly is cumbersome due to some limitations and shortcomings in the APPEL language design principles [22]. One of these shortcomings is that people cannot specify what is acceptable rather than specifying what is unacceptable. It is not easy to write an APPEL statement that defines request consent for a specific behaviour of a service provider. Agrawal, Kieren et al. [22] argue that even exact connectives (or-exact, and-exact) will result in incorrect behaviour when being used to avoid this problem. Therefore, they proposed Xpref based on Xpath [23] to replace APPEL specifications. Though the approach of correcting APPEL seems a fundamental one [22], we assume that replacing APPEL is a process that will take a long time and needs a lot of effort as well. In this paper we will adopt another approach here by making use of the so-termed PTL Approach.

IV. THE PTL APPROACH

In this section, we present a way of dealing with dynamics through asserting a PTL value to data practices combinations. At each moment in time, we get an updated user consent decision that corresponds to the dynamics caused by the change of user situation or location.

A. Calculating aggregated PTL Values

Information collectors such as service providers usually present one single list of practices, expecting users to either accept it or reject it as a whole. However in practice, different combinations of data practices as offered in a service provider's privacy policy can have different impacts on user privacy concerns. This impact may vary from one user to another and from one context to another. In our approach, the difference in impact on privacy is expressed in the form of a numeric value, which is a weighting value reflecting the threat a particular request for information poses to a person's privacy. The PTL is calculated by dynamically evaluating the service provider data practices.

The PTL always has a value between 0 and 1: the higher the value, the higher the underlying threat to privacy. For example, if the threat value of requests with telemarketing purpose is set to 0.8 and that of contact to 0.5, this means that collecting user data for telemarketing is considered more invasive than for contact. What the user specifies in his or her preferences using the PTL approach is how he or she thinks a telemarketing purpose is threatening to his privacy concern. Average users are unlikely to understanding P3P vocabularies, and as a result there is a possibility that the values they define do not accurately reflect what they want. This means that a way has to be found to carry out the weighting process in a user-friendly way, taking into account the changing domain specifications.

As argued above, each request may pose a threat to privacy depending on how the requested information will be dealt with. In other words, depending on what we call allowed data practices compared to asked ones. However, combinations of practices can have different impacts on privacy. For example, the purpose of 'individual analysis' can have a lower PTL value if combined with a recipient of 'ours' rather than that of 'unrelated third parties'. Here, 'ours' may represent the set of family people or group of close friends and 'unrelated third parties' may denote the set of non-business partners. Fig. 2 shows an example of how practices' combinations can affect the various PTLs: the tailoring purpose PTL equals 0.6 and if combined with other data practices, the overall combination has different aggregated PTL values. For example, a "tailoring, ours" combination has the lowest combined PTL in violating privacy compared to the "tailoring, third parties" combination.

For the sake of simplicity, in this paper we assign PTL values per combination of practices rather than per single practice. The final aggregated PTL of a certain engagement of a service provider is thus composed based on the aggregation of all PTLs per practices' combinations.

 ISBN: 978-1-61208-164-9

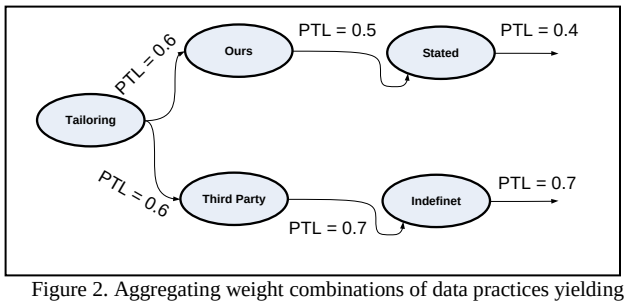

Figure 2. Aggregating weight combinations of data practices yielding different PTL values.

B. Privacy Rules Design

In the previous subsection, we argued that combinations of data practices influence PTL values of given services providers' data practices. In this section, we elaborate further on this issue. Preferences description refers to the way preferences will be presented to the end users. In this paper, our proposed model is based on the P3P specifications' one. Service providers' data practices are also expressed using P3P vocabularies [19]. Our proposed model uses PTL values as a representation of how users think their privacy can be violated. We can define the PTL model in the following way:

{*<purpose>*, *<recipient>*, *<retention>*, *<situation>*} ➔ *PTL*

The underlying rationale for choosing this rule description is to make it more user-friendly. This way one user can indicate a PTL value instead of having to worry about making a consent decision herself. Before a user decides whether to give consent or not, he or she has first to think whether this rule is threatening his or her privacy by assigning a PTL value. He or She can afterwards decide based on the aggregated PTL values whether to give consent or not. If we look again at the previous example adding the situation to the model has impacted the overall PTL (see Fig. 3).

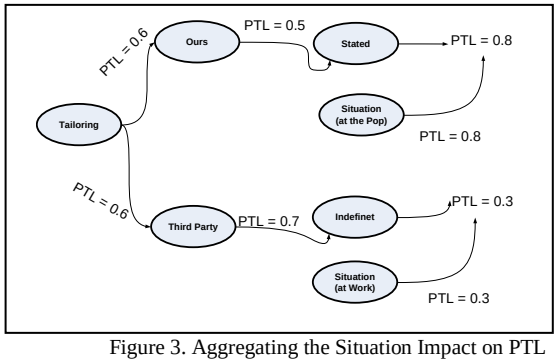

Figure 3. Aggregating the Situation Impact on PTL

We assume that a privacy preference consists of one or more privacy preferences rules (statements). Each rule consists of a specific data practices combination, associated consent behaviour, and a PTL value. The statements are connected via connectives as described below. Our proposed privacy preference rule, or just referred to as privacy rule in the rest of the paper, can be described as follows:

{<Purpose (n)>, <Recipient (n)>, <Retention (n)>, <consent behaviour>, <PTL (n)>}, <Rule Connective>

C. Rule Connectives

Rule connectives are logical operators that define the influence of each privacy statement on the others in order to evaluate the overall behaviour. We adopt the P3P defined connectives; AND, OR, NON-AND, NON-OR, AND-EXACT and OR-EXACT. The connectives govern the way preferences statements are compared to those in the privacy policy as follows:

1) AND

A rule will fire only and only if all contained statements are found in a privacy policy and matched.

2) OR

Any match of the contained statements is enough for firing**.**

3) NON-AND

Any of the contained statements should not match (logical complement of AND).

4) NON-OR

None of the contained statements should match (logical complement of OR).

5) AND-EXACT

All contained statements should match in the privacy policy of the collector for acceptance and no other statements (not matched) should exist in the privacy policy.

6) OR-EXACT

A match of any of the contained statements is enough to fire both and no other statements should exist in the privacy policy.

D. Privacy evaluation mechanism

As mentioned above, a privacy rule is a statement specifying a PTL value associated with a certain data practices combinations and associated situation. Furthermore, situation also influences PTL values. The next step is to specify the evaluation mechanism needed to automate the process of assessing PTL values. A weighting analyzer will be needed to develop an output that consists of {consent, PTL} for example, {request, Low}, which means a consent type of request with a PTL value of Low. The consent here refers to the output coming from APPEL evaluation. The weighting analyzer will look for practices combinations in the policy and accumulate the overall PTL value. Within the weighting analyzer, evaluation takes on the following pattern: first find available combination matches and then accumulate weights according to matching combinations.

 ISBN: 978-1-61208-164-9

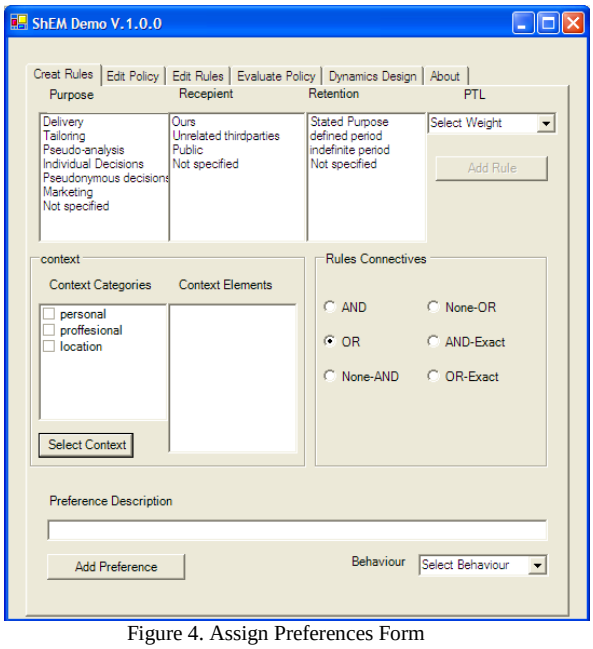

Figure 4. Assign Preferences Form

V. A PROTOTYPE EXAMPLE

We have built a prototype console using visual basic.Net in order to simulate the evaluation process of the proposed privacy rules using the PTL approach. Fig. 4 shows how users would have to assign preferences. In this prototype, we provide two ways of expressing user preferences; a static and a dynamic way. In the static way, preferences consist of allowed practices combinations associated with a PTL value. While in the dynamic way, we associated PTL values with the user situation. In this console, and for the sake of simplicity, we used a PTL range from 1 to 10. The user could assign data practices values per context group as well. We defined three context groups; personal, professional and location. Each preference could have multiple data practices combinations. Each preference is assigned a behaviour value. The user can define the rule connective among the six defined connectives in the P3P specifications. Fig. 5 shows how the form of assigning dynamic preferences can look like.

Let us get back to Jo's case as was shown in Fig. 1. For the sake of simplicity, we assume the following:

- We take an example of only location type of requests.
- *PTL* values are accumulated using an OR logic meaning that we take the highest value among the matching rules connected with the OR connector.
- Low *PTL* values means $PTL <= 4$, Medium *PTL* values means $4 < PTL <= 7$, High *PTL* means $PTL > 7$.
- Jo's situation is classified to three situations: {"in my Room"; "in the Hotel's Bar / restaurant"; "at the client"}. Associated PTL values are {8,4,2}.

Jo classifies his allowed data practices combinations (privacy preferences / rules) as shown in Table I while Information collectors asked data practices for location information are shown in Table II.

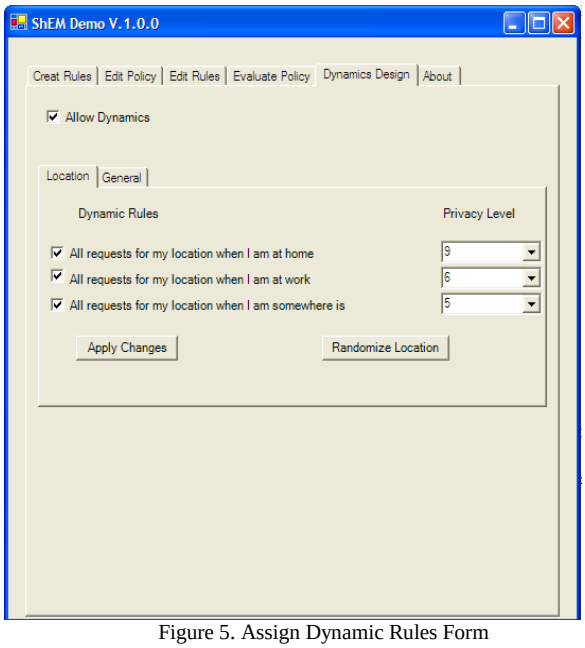

Figure 5. Assign Dynamic Rules Form

TABLE I. JO'S PRIVACY PREFERENCES

Purpose	Recipient	Retention	Consent	PTL
Not specified	Not specified	Stated Purpose	Request	3
Not specified	Not specified	indefinite period	Block	9

TABLE II. INFORMATION COLLECTORS ASKED DATA PRACTICES

Information Collector	Purpose	Recipient	Retention
Entertaining	Marketing	Not specified	indefinite period
	Delivery	Ours	Stated Purpose
Traveling	Not specified	Not specified	indefinite period
Restaurent	Marketing	Not specified	Stated Purpose
Tourist	Marketing	Not specified	Stated Purpose
BeThere	Not Specified	Ours	Stated Purpose

In case *BeThere* requests location of Jo, then this is what happens:

- The weighting analyzer collects BeThere asked data practices. These are: {Not Specified, Ours and Stated Purpose}
- The weighting analyzer checks Jo's allowed data practices and associated *PTL*s. According to APPEL evaluation, the output consent behaviour becomes "Request" while the accumulated *PTL* value is "3". Then the weighting analyzer checks for Jo's current location that is asked by BeThere, let's assume that Jo is at the the restaurant, this has

 ISBN: 978-1-61208-164-9

a *PTL* value of "4". This leads to a final *PTL* of "4". The recommended output becomes then {"Request", "Low"}.

- In case Jo location changes, for example to "in my room", *PTL* becomes "8", having said that, then the final *PTL* becomes "High". Though APPEL output doesn not change and remains "Request", Jo should reject this transaction at that time because his situation being at his room is considered highly private by him.

The rest of the information collector's evaluation takes place similarly. The evaluation output is displayed in Tables III & IV. Table III shows the output behaviour without taking Jo's situation into account while Table IV shows the evaluation taking Jo's situation into consideration. For example, collection of Jo's location is rejected for indefinite retentions although the other allowed data practice of Entertaining has an output of {"Request" & "3"}, the final static evaluation for Entertaining would be: {"Block", "9"}. When taking dynamics into account, Jo's evaluation does not change much because the static evaluation scored already privacy threat when dealing with Entertaining service provider.

TABLE III. STATIC EVALUATION OF JO'S PRIVACY

Inf. Collectors	Purpose	Recipient	Retention	Fired Conse-nt	*PTL*
Entertaining	Marketing	Not specified	indefinite period	Block	9
	Delivery	Ours	Stated Purpose	Reques t	3
Traveling	Not specified	Not specified	indefinite period	Block	9
Restaurent	Marketing	Not specified	Stated Purpose	Reques t	3
Tourist	Marketing	Not specified	Stated Purpose	Reques t	3
BeThere	Not Specified	Ours	Stated Purpose	Reques t	3

TABLE IV. DYNAMIC EVALUATION OF JO'S PRIVACY

	In my room		In the hotel's bar / restaurant		At the client	
	APPEL Output	*PTL*	*APPEL Output*	*PTL*	*APPEL output*	*PTL*
Entertaining	Block	9	Block	9	Block	9
Traveling	Block	9	Block	9	Block	9
Restaurent	Request	8	Request	4	Request	3
Tourist	Request	8	Request	4	Request	3
BeThere	Request	8	Request	4	Request	3

From the above tables we notice that for some cases the static evaluation scored already a threat when the service provider is intending to keep Jo's details for indefinite period of time as in case of *Entertaining* and *Travelling* ones (see Table III). Therefore the dynamic evaluation will not be expected to differ. In other cases, the static evaluation can allow the transaction while the dynamic one detects the threat. For example in the case of "BeThere" and when the situation changes to "in my room" as shown in Table IV the final evaluation has shown a high *PTL*, which means we should update the static *PTL* value. In this case, Jo should get a message warning him from continuing this operation.

VI. CONCLUSIONS AND DIRECTIONS

In this paper, we proposed a privacy control approach for location-based services (LBS), which takes into account the dynamics of such environment into the design of users' privacy rules. To do so we proposed a privacy threat level indicator (PTL) to be inserted in rules description. PTL refers to the amount of threat expected to user privacy when using a data practices combination. We also porposed the way to evaluate privacy rules using both APPEL and PTL approach. We have developed a simulation console that shows how dynamic preferences are described and evaluated in practice. We also presented a scenario showing how this approach can work in practice.

Average users are unlikely to understanding P3P vocabularies, and as a result there is a possibility that the values they define do not accurately reflect what they want. This means that a way has to be found to carry out the weighting process in a user-friendly way, taking into account the changing domain specifications. To do so, some empirical studies should be carried out to understand how to come up with sensible PTL values. Another possible next step is to implement and integrate the console with an LBS pilot or with an operational LBS on any of the new devices platforms such as iPhone or iPads and let real users try it and record their experience with our approach.

ACKNOWLEDGMENT

The author would like to thank Dr. Jan van den Berg very much for his help with reviewing parts of this paper. Furthermore, the author aknowledges the support he got from Ordina to publish and present this work in the press.

REFERENCES

1. S. Kalasapur, M. Kumar, and B. Shirazi, "Evaluating Service Oriented Architectures (SOA) in Pervasive Computing," Fourth IEEE International Conference on Pervasive Computing and Communications (PerCom'06), 2006, pp. 275-285.
2. M. Ackerman, T. Darrell, and D.J. Weitzner, "Privacy in context," HCI, 2001, vol. 16, issue 2, pp. 167-179.
3. F. Lardinois, "Two-Thirds of iPhone Users Now Use Location-Based Services at Least Once a Week," http://www.readwriteweb.com/archives/location_services_used_by_two_thirds_of_iphone_users.php, April 22, 2010, Last Access Date: July 15th, 2011.
4. D. Riboni, L. Pareschi, and C. Bettini, "Shadow attacks on users' anonymity in pervasive computing environments," Pervasive and Mobile Computing, 2008, vol. 4, issue 6, pp. 819-835.

 ISBN: 978-1-61208-164-9

5. D. Chaum, "Security without Identification Card Computers to make Big Brother Obsolete," Communications of ACM, 1985, vol. 28, issue 10, pp. 1034-1044.
6. J. Camenisch, and E.V. Herreweghen, "Design and Implementation of Idemix Anonymous Credential System," Proc. the 9th ACM conference on Computer and communications security, New York, USA, 2002, pp. 21-30.
7. A. Lysyanskayal, R.L. Rivest, A. Sahai, and S. Wolf, "Pseudonym Systems," Sixth Annual Workshop on Selected Areas in Cryptography (SAC '99), 1999, Springer-Verlag LNCS, pp. 184-199.
8. A. Coen-Porisini, P. Colombo, and S. Sicari, "Dealing with anonymity in wireless sensor networks," the ACM Symposium on Applied Computing (SAC10), 2010, Sierre, Switzerland, pp. 2216-2223.
9. R.S. Sandhu, and P. Samarati, "Access control: principle and practice," Communications Magazine, IEEE, 1994, vol. 32, issue 9, pp. 40 - 48.
10. B. Schneier, "Cryptographic design vulnerabilities," Computer, 1998, vol.31, issue 9, pp. 29 - 33.
11. R. Agrawal and J. Kiernan, "Watermarking relational databases," the 28th VLDB Conference, 2002, Hong Kong, China, pp. 155-166.
12. B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in Web-based social networks," ACM Transactions on Information and System Security (TISSEC), 2009, vol. 13, issue 1, article no.6.
13. C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu, "Tools for Privacy Preserving Distributed Data Mining," ACM SIGKDD Explorations, 2002, vol. 4, issue 2, pp. 28 - 34.
14. M. Langheinrich, "Privacy by Design- Principles of Privacy-Aware Ubiquitous Systems," Third International Conference on Ubiquitous Computing (Ubicomp2001), 2001, Springer-Verlag LNCS, pp. 273-291.
15. J.R. Rao and P. Rohatgi, "Can Pseudonymity Really Guarantee Privacy," the 9th USENIX Security Symposium, 2000, Colorado, USA, pp. 85-96.
16. M. Reiter and S. Stubblebine, "Authentication metric analysis and design," ACM Transactions on Information and System Security, 1999, vol. 2, issue 2, pp. 138-158.
17. P. Zimmermann, "PGP User's Guide," 1994, Cambridge, USA, MIT Press, Volume I and II, Distributed with the PGP software.
18. L. Pareschi, D. Riboni, A. Agostini, and C. Bettini, "Composition and Generalization of Context Data for Privacy Preservation," the Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM '08), 2008, Washington DC, USA, IEEE Computer Society, pp. 429-433.
19. L. Cranor, B. Dobbs, S. Egelman, G. Hogben, J. Humphrey, M. Langheinrich, M. Marchiori, M. Presler-Marshall, J. Reagle, M. Schunter, David A., and R. Wenning, "The Platform for Privacy Preferences 1.1 (P3P1.1)," Specification W3C Working Group Note, http://www.w3.org/TR/P3P11/, 13 Nov. 2006, Last Access Date: July 27th, 2011.
20. L. Cranor, M. Langheinrich, and M. Marchiori, "A P3P Preference Exchange Language 1.0 (APPEL1.0)," W3C Working Draft, http://www.w3.org/TR/P3P-preferences/, 15 April 2002, Last Access Date: July 27th, 2011.
21. L.F. Cranor, P. Guduru, and M. Arjula, "User Interfaces for Privacy Agents," ACM Transactions on Human Computer Interactions, 2006, vol. 13, issue 2, pp. 135-178.
22. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "XPref: a Preference Language for P3P," Computer Networks, 2005, vol. 48, issue 5, pp. 809-827.
23. J. Clark and S. DeRose, "XML Path Language (XPath) Version 1.0," W3C Recommendation, http://www.w3.org/TR/xpath/, 16 November 1999, Last Access Date: July 15th, 2011.

 ISBN: 978-1-61208-164-9