Privacy-Concern for Context-Aware Environments

Tomoko Shoji, Tatsuo Nakajima
Department of Computer Science
Waseda University
tomo@dcl.info.waseda.ac.jp

Abstract

Context-aware computing offers attractive services by collecting information from various sensors, and the services will be adapted according to the current condition of the real world. However, the danger of overflowing personal information is also getting high because the data retrieved by the sensors usually contain privacy information. In this paper, we study on the tradeoff between privacy and the quality of services, and we present the design of our system that we are currently developing. Our proposed system controls the tradeoff according to a user's requirement, and guarantees the trustworthy of the management of privacy information.

1 Introduction

The research of sensor-used applications is now developing. As sensor-used application techniques are getting developed, many new applications will be born. These new applications stand by the information which is gathered by sensors or is stored in personal servers or something like that. As gathering information by sensors or giving personal information, a service becomes suitable for its user, because the information which is gathered is about the user's personal information and with which the application can match the service to the user. Such an application is called a *context-aware application.*

If all information transfer is done seamlessly, it will be useful for users, but to use such applications, the user must care about own privacy. By using personal information, the application becomes suitable for a user, but on the other hand, without concerning about privacy protection, this application can be just a surveillance system[1, 2].

The protection of the personal information is concerned to be guaranteed by a law. However, the protection of the personal information by a law is quite complicated. Only the law itself, it is impossible to cover all the possibility of being surveillance. The problem of the protection of the personal information is just started to be worried. So, now is the time when we should think about the personal-privacy problem in context-aware environments.

In this paper, we suggest some techniques of protecting privacy in context-aware environments. What we think as an important aspect to protect privacy in context-aware environments, is to let users control their personal information by themselves. Therefore, how a user manages to know about how one's information will be treated will be the most important aspect to concern. In Section 2, we state the definition of some terminologies. Section 3 explains two examples of the use of context-information. In Section 4, we explain our recent research, and Section 5 explains about the concept of trustworthy which becomes the main point of this system. Finally, Section 6 states the conclusion.

2 Background

Now, we will explain the basic background of our research, about how we think of privacy, what is privacy, and what is privacy protection?

2.1 Privacy

When we look at a dictionary, there are a lot of meaning of privacy, for example, the power of control for personal information not being known by the third person. Then what is the personal information? We state the word personal information as the information with which the third person can define a specific person. Now the main aspect of what we should concern about is what is the meaning of *privacy-protection* in context-aware environments.

Recently, the Japanese government is trying to keep all the resident's cards in a database, so that office work will be done efficiently. However, this trial caused the resident's worry. They worry about their residential information be opened to the third person by keeping them on the net. Because of this concern, they start to realize the danger of the internet business, so the nation requests the government to set the law for the protection of personal information, and so the law became in operation now.

However, the law is not perfect enough to protect personal information from context-aware environments. The definition of the privacy is also difficult to set, and the meaning of the protection is also difficult to define, so now, we described our meanings of privacy protection, and depends on that, we introduce the technique which we think is important to be considered to create context-aware environments.

2.2 Context-Awareness

Now, what context-awareness means. Recently, by using sensor information, an application can gather a lot of information about users to give them a personalized

Proceedings of the Second IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems (WSTFEUS'04)
0-7695-2123-1/04 $ 20.00 © 2004 IEEE

service. Many services depend on the situation of a user. These services are called context-aware services. Context-aware applications use the current situation and it helps the applications to give a user a suitable service. For example, a car navigation system uses the current location of a user to navigate a user to go to the destination. At these situations, a lot of information will be taken, and so, it will be important to manage the information.

2.3 The concept of the Tradeoff in a context-aware Environment

In context-aware environments, a user's personal information has to be given. A user can choose whether they give their information seamlessly or not. However, if they decide not to give any information without being asked, then, they can't take services seamlessly, or the service will not be suitable for the user. They have to give their information each time they decide to take a service. On the other hand, if a user chooses to give their information seamlessly, then they can take the service without doing anything and the service will be personalized for them. The point is that unless users decide to give their information, the service will not be suitable for the user.

Each time when some new techniques of using sensors to gather information are developed, the privacy-protection problem is considered. However, the normal thinking way of privacy-protection is to prevent from the personal information being known by the third person, but what we have to think about is how should we keep out the information, which applications collected, from being exposed by wicked persons. Usually, once the information is transfered, the use of the information is not able to be known to the user, but this point is exactly what we should concern. Therefore, the keyword for this privacy-concern in context-aware environments is "The Tradeoff" between privacy and the quality of services.

3 The examples of the context-aware application

Here, we give some examples of the use of personal information in context-aware environments. The main point of this example is that the application requests some context-information to use, and the service gives the tradeoff between privacy information and the quality of services. Much information the user gives, more suitable the services will be given.

3.1 Informing the shopping information

There is an application which informs a user about shopping information. This application requests the position of a user, and informs the user about the information of the shop which is around the position of the user. The information will be the sales information, the trend, etc. If a user allows to give the positioning information only, the offered information will be general information only. However, if a user allows services to give the distinction of sex, the information will be suitable for the sex. Adding that, with the age, the information will be suitable for the age. It is not necessary to identify a user, but if the user gives the personal information also, then the offered information will be suitable for the user.

3.1.1 Discussion

What will be the necessary to use this application is to give positioning information. To make this service suitable for a user, the application requests much information. If a user just wants to have a general information, the information may not contain information which identify a user, like age, sex. However, the tradeoff should be taken into account. More private information the user give, more suitable service will be given to the user. If a user allows services to save one's shopping record, then the application may be able to give more suitable information to the user, which is something like that from the user's trend's point of view, the arrival of some new items.

If a user wants to protect one's personal information from being misused, the user can deny to give personal information, but then the service will not be personalized.

3.2 Making a customer card service

Now, most of the shops have some kinds of members card. To join this, customers always write and give personal information to the shops. By constructing context-aware environments, it will be easier to join this. This means that if a user allows to give their information to make members cards, the information will be given to the shops without the user taking any bothersome steps.

3.2.1 Discussion

The context-information which is required for this application in most of the time will be name, age, sex, address, phone number, and sometimes an occupation. By using these information, the shop side sometimes gives a point from the purchase record, or keeps the record, and from that, the shop may give the user some special sale information.

Now a day, a customer feels quite few risk to make this, but when it becomes digital information which has a risk to be misused or be surveillance, the user may hesitate that the own personal information be handled without being noticed, and kept as digital information. However, if the user trusts the system, the user may use this technique and may want to make the card seamlessly.

3.3 Requirement

Thinking over the examples, what we should consider about is how to operate these application systems, and how to make the user trust the systems and make them use the systems? The point is how much the user gives personal information, and how much the service is suitable for the user. More a user gives personal information, much a service becomes suitable for the user. Then,

whether the user gives personal information or not depends on how much the service is interested and the main point is whether the system is trustable or not.

If a user has to give one's personal information to make the service suitable for the user, then the user may want the guarantee about that one's personal information not being misused. If it is guaranteed, then many users may want to make the service suitable for them, and if many users trust the system and give much information for market development, then the system may become more suitable for the user. Now, our research point is this trustworthy. What we need to do to make the system trustworthy, and to let the user use the system. Next section explains our system for privacy protection.

4 Privacy Negotiation

Based on these applications, we are researching on the technique of using policy-preference documents matching. To think about this, we are making some situations in which context will be needed. Now we present our recent research.

4.1 Policy-Preference matching system

Our system which we call "Privacy-Negotiation System" is built because we thought that the most important issue to think about privacy-protection is to let users to control their own personal information by themselves. By this system, we are trying to give users the right of choice about whether they permit to give their information seamlessly for a certain purpose or not.

To do this, we prepare two kinds of documents called preference and policy documents. Our system adopts the extension of the P3P specification[4]. The preference document is created by a user. This document states whether a user permits to give its information seamlessly for a certain purpose or reject it. On the other hand, the policy document is created by a service provider and it states that which kind of information is requested to get the services, and how it will be handled, etc.

By creating these two documents and using them, we want to make it possible that users control their personal information's use by themselves. Before giving a service, the preference document and the policy document are compared, and if each statement is agreed, the information transfer will take place without noticing it to a user, but if a user does not permit to give the information which is needed to use an application, the application does not work. If a user wishes to use the application, the service provider asks the user to give the personal information which is needed to give the service, then the user changes the rule to give, so he/she can take the service.

The main part of this research is to create a policy document and a preference document, and to compare them before the information transfer takes place. Each document's role is as stated before, here, we explain how to create them actually.

We are creating these documents using XML. For the XML schema, we are constructing a hierarchical data structure. To make the matching system easier, we are thinking of creating the database which will be the set of context information, hierarchical. This is because we think that the information which will be collected, will be very large amount, so it will be good if we make a hierarchical data structure to arrange them.

4.2 Gathering information by sensor

This time, we are trying to use some kinds of sensors to collect information. The kinds of the sensors will be accelerometers, light sensors, force sensors, thermometer and so on. Because of the characteristic of the sensors, once the sensors are set to collect information, the data which can be detected according to the characteristic of the sensor, will be collected whether or not the user wants to. The point is that what a user can do about sensing information, is only after the information is collected by the sensors. If a user can understand how the information which he/she gave, is handled after giving, then it will be useful.

What we are thinking is the situation where context information is taken to use an application, will be common. To build such an environment, what we need to do is to make a normal user(ordinary person) to accept such an environment. That means that we build the situation where the normal user gives their personal information without any doubt. For this purpose, the most important thing is to make sure that the system is secure enough and the personal information will not be used in a wrong way, so what we need to do is to let the normal user know about the sensors and the situation of context-aware environments more in detail.

4.3 A Sample Scenario

Here is the situation which we think. The sample application is something like this. We think about the situation at which all garbages are recycled and so, if a person throws a garbage to the proper position, the person will get refund. On the assumption that the price of a bottle of beverage includes the price of the bottle. If the person returns the bottle later, then the price of the bottle will be refunded.

At a present state, the person must bring the bottle to where the person bought the bottle. However, at the context-aware environments, the person does not have to bring it to the shop, but just need to throw it to the proper garbage box which realizes the type of the garbage and the person who throws it.

This auto-realize garbage box has a tag reader, and a user has an RFID tag. All users have respective tags, and when the user comes to throw a garbage, the tag reader reads the user's tag and realizes who the person is. According to circumstances, the garbage box may realize where the person lives and if the person who throws the garbage, lives in the area where the box stated, then the

user may get more refund because the user pays a tax to that area. This will be the merit of the user when he/she gives their information to the system.

4.3.1 Policy-Preference Documents

Based on this scenario, we need to create a preference and policy documents. At the policy document, we set that the personal information which the application needs is the place where the user lives, and whether or not the user pays taxes. These information are used only for this application. By using these information, the application can realize who the person is and be able to check whether the application should pay the refund or not. Except the personal information, the application reads the tag which is put onto the bottles also, so that the garbage box realizes which types of the garbage is thrown. All garbages must be sorted, so the garbage boxes are different from each category, and the category is inflammable, noninflammable, recyclable, and so on.

On the other hand, we imagine a user whose preference is that all information which are needed to use the garbage refund application, are allowed to give seamlessly, and other users whose preferences are that the user does not want to give the information about where to live. When these two types of the user come in the territory of the application, the document matching will take place in such a way which is described in the next section.

Except that, what other types of the information will be used is something like this. As a purpose of the information's use, there is a choice among current application use, marketing, inventory control, user's preference check, and so on. As collected information types, as a personal information, a user's general information, which is like, name, gender, age, address, etc, and the user's action will also be personal information, which is like, what the user buys, where the user goes, who the user with, how the user acts, and so on. Finally, as the use of information, except the application use, it can be the third person who has the same purpose, and the third person who uses the information for different purposes. By combining these items in many ways, policy-preference documents will be made.

4.3.2 Document-matching Implementation

Based on the scenario, here is the result of document matching. We defined two types of users for this scenario. Respective users have different preferences, so the result of the matching will be quite different.

For the first type of users, the user allows the application to use the information which will be needed to use the application. In addition to that, the application sets the policy as it uses the information only for current services. Therefore, the information which will be transfered seamlessly will be the place where the user lives, whether the user pays taxes, and what the type of the garbage is. This time there is no information that the user denies to give. This user can get a refund when he/she throws the recyclable garbage, and will get a special refund for paying taxes and cooperating the recycle at the area where he/she pays tax.

For the second type of users, the user denies to give the information about the living. This means that the application can realize the types of garbage, but not user. Therefore, a user may be able to get refund somehow, but because the living information is not defined, so the special refund will not be paid. This decision will be informed to the user, that without giving the living information, the user can't get the special refund.

4.4 Discussions

This example shows two different cases showing the tradeoff between privacy and the quality of service, one can get a service seamlessly, and the other can't. If a user trusts the system, and gives the information, then the user can have merit, but if not, then the user has to give each time when he/she wants to get a service. This is the tradeoff among this environments, more information the user gives, more personalized services will be given.

This example uses the tags, but we are also concerning to use a variety of sensors. The use of the sensors will be something like gathering temperature data from a thermometer to control the temperature of the closed area. Then, if a user who is in that area, allows the application to use the information of the user's physical condition, the temperature of that area may be suitable for the user.

The main problem of this system will be the trustworthy. If the users do not trust that the system treats their personal information as stated, or if they can't realize the merit of this system, the system won't prosper. Therefore, in the next section, we suggest some solutions to give trustworthy on this system.

5 Trust Management

The main point of this system is this concept of the trustworthy. If a user does not trust the system, he/she may not use it, and if user does not use the system, the application cannot collect sample information, it will be difficult to set recent trend. This will be a vicious circle. Therefore, we think about the concept of trustworthy in this system. Our system use policy-preference matching technique, to make this system work well, policy-preference matching system has to be trustworthy. Even though a service provider side makes policy document and set the policy, if the service provider does not follow it's policy and use the private information in a wrong way, this matching system will be useless. Therefore, to guarantee that the service provider treats the user's personal information as they set in policy document, will be one of the important aspect to construct this system.

We concern this problem in two ways. The first one is systematic and the other one is legal. The systematic one starts from understanding what kind of trustworthy relationship is needed between a user and a system. What makes a user trust the matching system? On the other

hand, the legal solution is to protect personal privacy from a legal point of view. If personal information is misused, it is punished legally.

5.1 Systematic Solution

At first, we explain about the systematic solution. We need two ways to make a trustworthy system systematically. The system contains certification system and reputation system. The certification system gives the application a certification which guarantees that the application handles the personal information as it is stated at policy document. Then, after the application starts to work, the reputation system let the user examine the application, and give the reputation to the application. By using these two system, if the application handle the personal information correctly will be guaranteed.

5.1.1 Certification System

At first, we describe about certification system. When context-aware applications become more common, a new organization where gives a certification to an application may be born. Hopefully, this organization falls under the jurisdiction of government, so that we do not have to worry about the trustworthy of this new organization. This new organization examines how the system handles the information which they collected, and the policy document, and if the system works well, the organization gives the certification to that system. Then this certification becomes good sign to users.

Actually, a certification system for internet systems exists already. We are also thinking of using this existing system by extending it for the context-aware environment use.

However, this organization may not be able to guarantee that the application does not work wrong after getting the certification, so the reputation system is needed.

5.1.2 Reputation System

The reputation system is that a system gets reputation from third party, and much reputation makes the system more trustworthy. This third party can be a user. When a user uses the system, and feels good to use the system, the user can set the reputation to that system. If many users or other third party put the reputation to a system, that reputation will be a good sign to decide if the system is trustworthy or not.

5.2 Legal Solution

Finally, we explain about a legal solution. Even though many engineers try to protect personal information from being misused, not all of them can be protected. Some of them is needed to be protect legally. A privacy problem is difficult to limit by law because there is a freedom of speech. However, we think like this. When matching system works and a user starts to use an application, it will be considered that a contract which states the use of personal information, is exchanged between the user and the service provider side. Then when the service provider side misuses a user's personal information, it will be considered as the service provider breaks the contract.

6 Conclusion

What we are doing so far is one step of constructing context-aware environments. To make such an environment, we have to make a lot of people know about context-aware applications. Therefore, we are considering some applications and picking up the problems. What we think the most important problem to construct the context-aware environment is to protect the personal privacy. Even though we make some convenient applications, if a user does not trust the system and refuses to give personal information, the applications will be useless, so we need to make some systems which guarantee to protect personal privacy. To solve this problem, we suggest to use document matching system, and to guarantee this matching system, we are considering systematic solution and legal solution.

There is one more point to concern before constructing context-aware environments. The problem is that it will be difficult for users to make preference documents, and it also will be annoying for system engineers to consider about privacy problem each time when they make application. To solve this problem, we are considering to make some template for the users. Though the template is made as the user can use it soon, if the user wants to customize the preference document afterwards, we prepare for such users to customize it easily and also by using the document, each time when the user uses an application, and customizes the preference, the record of the change will be kept, and the change will be reflected next time when the user use the same application.

Finally, future work will be the researches of trustworthy system. As described before, it is important to make an application trustworthy. The main point of this system is to let the users trust the system, which means that the trustworthy of the policy document should be highly enough. Once the digital data is created, it is thought to be difficult to control it, but we want to find the solution, and so we have suggested both systematic and legal solutions.

References

[1] Marc Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environment", In proceedings of Ubicomp 2002

[2] Asim Smailagic, Daniel P.Siewiorek, Joshua Anhalt, David Kogan, Yang Wang, "Location Sensing and Privacy in a Context Aware Computing Environment", In proceedings of Ubicomp 2001

[3] Lawrence Lessig, "CODE and other laws of Cyberspace", published by Basic Book, 2000

[4] Lorrie Faith Cranor, "Web Privacy with P3P", published by O'Reilly & Associates, 2002