Journal of Information Processing Vol.22 No.2 334–343 (Apr. 2014)

[DOI: 10.2197/ipsjjip.22.334]

Regular Paper

Ensuring Privacy during Pervasive Logging by a Passerby

Mohsin Ali Memon[1,a)]   Jiro Tanaka[1,b)]

Received: June 21, 2013, Accepted: January 8, 2014

Abstract: Pervasive logging devices capture everything along with the public nearby without their consent, thus, possibly troubling people who prefer their privacy. This has issues for privacy and, furthermore, the widespread use of such logging devices may affect people's behavior, as they may feel uncomfortable that they are constantly being monitored. People may wish to have some control over the lifelogging devices of others and, in this article, we describe a framework to restrict anonymous logging, unless explicitly permitted. Our privacy framework allows the user of a logging device to define privacy policies controlling when, where and who to restrict from logging them. Moreover, it is possible to select which type of logging sensors to apply these restrictions. Evaluation results show that this approach is a practical method of configuring privacy settings and restricting pervasive devices from logging.

Keywords: pervasive logging, privacy, geo-temporal, human proximity

1. Introduction

Lifelogging is a method to monitor and store information indiscriminately so that an individual may record their daily activities [1]. Gemmell et al. initiated life logging with a project named as MyLifeBits [2], where they attempted to record the life of a person in a digital format for easy retrieval. Lifelogging may change how we use and share personal data [3], allowing us to look back over our lives or search through and organize past experiences. Much research has been carried out in this field in order to create lifelogging devices, which enable people to efficiently monitor locations they have visited [4], maintain health records [5], [6] and log numerous other aspects of their lives [7], [8], [9]. However, lifelogging raises a number of questions, such as what, where, when and who we can monitor, and who can monitor us. Furthermore, we expect that the social acceptance and importance of personal lifelogging will increase in the near future, and that the privacy issues associated with it will become increasingly important.

Privacy requires people to be free from being observed or monitored by other people. The latest lifelogging gadgets, including SenseCam [10] and Narrative [11], are able to capture data on third parties without their consent. Since these devices are directed towards people other than the owner, in an environment where many people have these devices, some of them may be expected to alter their behavior to prevent unwanted logging by others [12], [13], and it has recently been shown [14] that, if a person is continuously observed, this impacts his behavior. Therefore, we need a mechanism that encourages pervasive logging given that an individual has already approved to be recorded by the people wearing the life log device. It is believed that the vital data including one's location traces, activity details, and health records are personal information and very helpful to recall the past but capturing these logs is beyond the scope of this article. The reason is that these logs cause no privacy risk to the neighboring people. Hence, in this research we focused only on those life log sensors (at present camera and microphone) that efficiently record the people in the surrounding and developed a mechanism by which a passerby's consent is considered before capturing them by our proposed life log device.

We propose a privacy framework through which the wearer of a lifelogging device may inform others of times and places that they would not like to be logged. One or both of the camera and microphone sensors that are employed in lifelogging devices can be prohibited from monitoring people who do not wish to be logged. The lifelogging device identifies nearby people, and then records data only if expressly permitted. In this manner, we attempt to instill privacy before capturing rather than using post capture distortion [15] (in case of images) in the log, which is incompetent if the algorithm fails due to poor light conditions [16]. The work described in this article employs infrared data transmission to overcome this limitation.

There are a number of situations where privacy cannot be guaranteed with existing lifelogging systems. For example, a person who regularly visits a public park for exercise may feel uncomfortable if nearby people photograph him. With lifelogging systems, the person may employ a privacy framework to define a policy to prohibit others from unwanted logging in that park. The main purpose of lifelogging is to aid users in recalling their personal experiences, and to achieve this they must record a considerable amount of data. However, taking the example of photographs taken by a lifelogging device, depending on the way they are used and shared, this may infringe the rights of the subjects of those photographs, who may potentially take legal action.

We focused on two challenges to ensure privacy:

Challenge 1: The privacy preferences of third parties should be

[1] University of Tsukuba, Tsukuba, Ibaraki 305–8573, Japan

[a)] mohsin@iplab.cs.tsukuba.ac.jp

[b)] jiro@cs.tsukuba.ac.jp

well described in terms of the restricted locations and time intervals.

Challenge 2: The mechanism to suspend logging should effectively avoid logging a person with active privacy settings.

To address these challenges, we describe a privacy framework and design a prototype device to implement it. Users declare their privacy settings in the form of policies, which are stored on their lifelogging devices. These privacy policies suspend the pervasive devices of others from logging when they are in close proximity. The work reported here is an extension of that described in Ref. [17].

2. Privacy Framework

Pervasive logging includes data on health logs, location traces, and body actions, which we term personal logs. However, logging may also include data on the user's surroundings, either in the form of pictures or audio recordings, termed neighbor logs. It is these logs that give rise to privacy issues for third parties. Our framework concerns the logs produced by neighboring devices, and can constrain the logging of neighboring devices using Geo-temporal privacy. An overview of the framework is shown in **Fig. 1**.

The Geo-temporal privacy settings should be defined by people who do not wish to be monitored. A user of a system may declare their privacy settings in three different ways. When privacy is desired at specific locations, the user may select that location by imposing geo constraints, and if a user desires privacy at specific times, temporal constraints should be created. However, there may be some circumstances whereby both location and time parameters are required to determine the privacy settings, and in our framework a geo-temporal constraint is created in such situations. These constraints are triggered automatically based on the location and time of the lifelogging device wearer. The user of the proposed privacy framework may employ privacy policies to prevent neighboring devices from monitoring them.

2.1 Geo-temporal Privacy

A user who desires the suspension of neighboring lifelogging sensors may set values for *sensor type*, *policy validity*, *accessibility* and *provision*, which collectively define a privacy policy, as shown in **Fig. 2**. Each privacy policy is stored on the owner's lifelogging device in the form of a tuple, so as to keep the user from being recorded by pervasive logging devices in the neighborhood. A privacy tuple has the following form: ⟨*sensor type, policy validity, accessibility, provision*⟩

Here, *sensor type*, may be a camera or microphone worn by people in the user's vicinity, and the user can restrict one or both of *camera* and *microphone* from logging. *Policy validity* declares the lifetime of a constraint, and the user can choose to apply it for one day, or apply it as a daily schedule. A policy declared as *Everyday* remains in the system as long as the user requires such a privacy plan. Unlike an *Everyday* policy, a *24 hour* policy is automatically removed from the system at the end of the day. Therefore, the user should be careful while determining the validity of a policy. *Accessibility* reveals the restriction level of the privacy policy.

We define two levels of restriction: *strict* and *standard*. *Strict* does not allow anyone to capture the constraint creator, whereas in *standard* restriction, the user is provided with a personalized friends list from their social network to select friends and authorize them to capture data on their respective devices, which may apply at times when privacy has been requested from others. Social networks have become the most convenient way to determine relationships between people, and we employ social network services to allow the user to choose other users whom they wish to permit to record them. The rest of the people are automatically denied from logging with that privacy settings. *Standard* restriction may be useful in situations where, for instance, an individual invites friends and family to a party. If a user's lifelogging device can distinguish family members from friends, the person may apply different privacy settings to different groups.

The user should declare settings for specific locations, times, or both location and time to prevent the sensors worn by others from logging. These settings can be applied using the constraint that best suits the user's requirements. A Geo constraint is created when a user selects a restricted location. For example, a user may be at a private clinic for a health check-up, and may desire privacy here. The user may be uncertain of the time of the visit, and so may select this place as a private location at all times. Alternatively, selecting a time interval to ensure privacy is considered a Temporal constraint. These constraints may help in situations, for example, where the user does not wish bystanders to take pictures of him eating in public, so the user can select lunch and dinner time as private times, regardless of their location. In addition, combined times and locations may be specified.

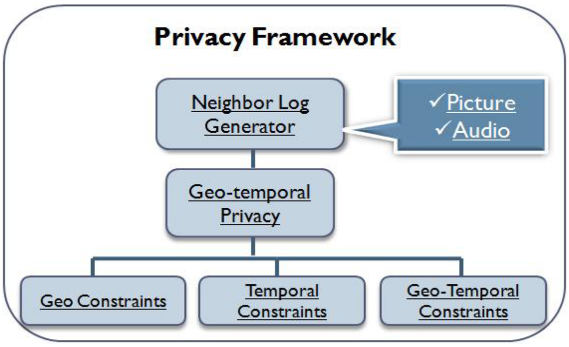


Fig. 1 Proposed privacy framework to ensure privacy from pervasive logging devices.

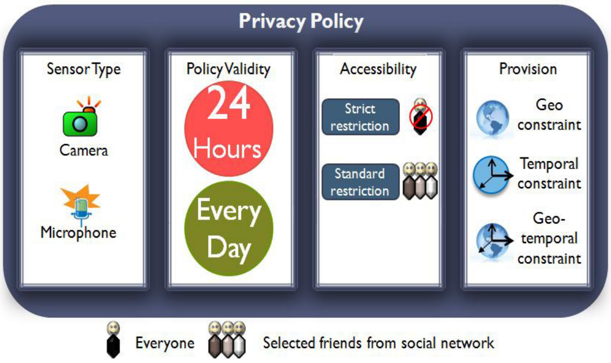
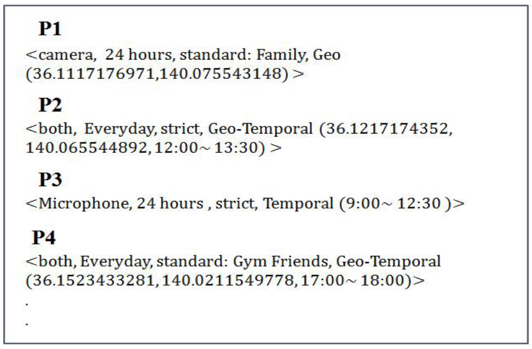


Fig. 2 Parameters to inscribe a privacy policy on the life log device.



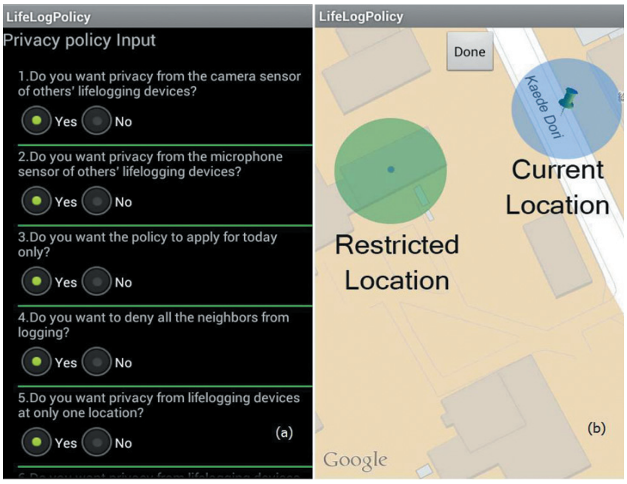
P1
<camera, 24 hours, standard: Family, Geo (36.1117176971,140.075543148) >

P2
<both, Everyday, strict, Geo-Temporal (36.1217174352, 140.065544892, 12:00~ 13:30) >

P3
<Microphone, 24 hours , strict, Temporal (9:00~ 12:30)>

P4
<both, Everyday, standard: Gym Friends, Geo-Temporal (36.1523433281, 140.0211549778, 17:00~ 18:00)>
.
.

Fig. 3 Example privacy policies stored on the life log device.



LifeLogPolicy

Privacy policy Input

1.Do you want privacy from the camera sensor of others' lifelogging devices?
● Yes ○ No

2.Do you want privacy from the microphone sensor of others' lifelogging devices?
● Yes ○ No

3.Do you want the policy to apply for today only?
● Yes ○ No

4.Do you want to deny all the neighbors from logging?
● Yes ○ No

5.Do you want privacy from lifelogging devices at only one location?
● Yes ○ No

Fig. 4 Policy input interface (a). Location selection for privacy (b).

This is termed a Geo-temporal constraint. A user may, for example, wish to avoid logging by friends in the office during working hours, but is happy for these people to log data on them when outside the office during leisure time. A geo-temporal constraint behaves as follows:

- The geo-temporal constraint will come into effect when the user checks into the specified location during a restricted interval.
- If the user checks into the restricted place before the restricted time interval, the privacy policy remains inactive.
- The policy expires once the restricted time interval is over, regardless of the user's location.
- The policy becomes void if the user departs from the restricted location before the duration of the policy lapses.

Figure 3 shows some of the privacy policies defined by a user, which are stored on their lifelogging device as tuples. Policy P1 is based on a geo constraint, which consists of a location selected by the user as a restricted place, and is specified in the form of coordinates for latitude and longitude. This policy prevents logging by people other than family members and is activated when the user's location is within a 100-meter radius of these coordinates. Policy P2 is a geo-temporal constraint, which consists of a restricted location and time interval. This policy is active when the user is at the specified restaurant during lunchtime. For the policy P2 to remain active, the user must satisfy the conditions described above. Policy P3 prevents neighboring microphones from logging during a meeting in the morning of the current day. Policy P4 applies at a gym and in the evenings, and permits only specific friends to log that user.

A policy may be overruled by a stronger policy if the specified geographical and temporal parameters conflict. Consider a situation whereby a user has created two policies, where the locations coincide. In such a case, the accessibility and validity parameters are checked, and if the accessibility of one of the policies is *strict*, we consider it the stronger policy, and these privacy settings are chosen over those of the weaker policy. If the validity of one of the policies is *24 hours*, it is regarded as the stronger policy. In the following subsection, we describe the method of ascribing privacy policies to the lifelogging devices.

2.1.1 Specifying a Privacy Policy

We programmed a smartphone to function as a lifelogging device and store privacy policies defined by the user. We designed a user-friendly interface to define the privacy policies. Here we refer to the condition/action rule based on the approach described by Kelley et al. [18] , whereby they allow the user to maintain control of their privacy policy. Our privacy input interface is shown in **Fig. 4** (a), and incorporates a rule-based system that determines a user's current privacy preferences by asking the following questions:

Q1. Do you want privacy from the camera sensor of others' lifelogging devices?

Q2. Do you want privacy from the microphone sensor of others' lifelogging devices?

Q3. Do you want the policy to apply for today only?

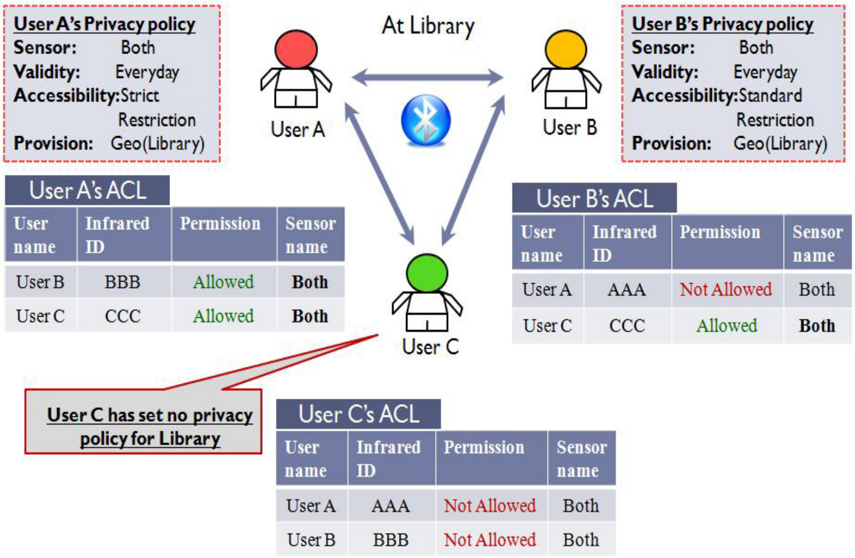
Q4. Do you want to deny all the neighbors from logging?

Q5. Do you want privacy from lifelogging devices at only one location?

Q6. Do you want privacy from lifelogging devices only during specific time intervals?

The user may define privacy policies, which are stored in an SQLite database as constraints with a user-defined name, and are constantly checked for privacy activation. All the previously defined constraints are made viewable to the user for inspection, modification or deletion. Q1 and Q2 concern the type of sensors, and replying 'yes' to both questions prevents logging with either of these sensors. The validity of the policy is determined from Q3, and accessibility is determined by the answer to Q4. If the user replies 'yes' to Q4, the accessibility level will be set to *strict*. A complementary approach appears when the user answers 'no' to Q4, which sets the accessibility parameter to *standard*. The Facebook API was exploited to fetch the user's customized friends lists, and the user was permitted to choose one or more friends lists and to monitor data themselves, even during activation of this privacy policy. In this manner, anonymous lifelogging devices, as well as those not included in the permitted friends lists, are not permitted to log data when a user with an activated privacy policy is in close proximity. The answers to Q5 and Q6 determine the provision parameter of the policy. For example, if the user answers 'yes' to Q5 and 'no' to Q6, a geo constraint is created. If the user answers 'no' to Q5 and 'yes' to Q6, a temporal constraint is created. If the user also replies 'yes' to Q5 and Q6, a geo-temporal constraint is created.

After answering these questions, the user must set the geo-



User A's Privacy policy
Sensor: Both
Validity: Everyday
Accessibility: Strict Restriction
Provision: Geo(Library)

User B's Privacy policy
Sensor: Both
Validity: Everyday
Accessibility: Standard Restriction
Provision: Geo(Library)

User C has set no privacy policy for Library

User A's ACL

User name	Infrared ID	Permission	Sensor name
User B	BBB	Allowed	**Both**
User C	CCC	Allowed	**Both**

User B's ACL

User name	Infrared ID	Permission	Sensor name
User A	AAA	Not Allowed	Both
User C	CCC	Allowed	**Both**

User C's ACL

User name	Infrared ID	Permission	Sensor name
User A	AAA	Not Allowed	Both
User B	BBB	Not Allowed	Both

Fig. 5 Privacy preferences and ACL of three users at the library.

graphical and temporal parameters based on the answers to Q5 and Q6. For a geo constraint, a map is shown with the current location (see Fig. 4 (b)) and the user may select a location and declare it as restricted. To precisely calculate the distance from the user's current location to the selected private location, we use the *inverse formula* [19]. For geo-temporal constraints, the user should select the restricted location and then choose the time period for the privacy restrictions to apply using the time preference control. The user should specify a temporal privacy policy by defining only the time interval for the privacy policy to apply. When the user defines a geo-temporal privacy policy, it is activated depending on geographical and time data obtained from the device. Currently, the privacy policy of the user must be shared between lifelogging devices in the neighborhood. We discuss privacy activation and sharing of privacy policies in the following subsection.

2.1.2 Privacy Activation and Sharing of Consent

When sharing users privacy settings, we must assume that the lifelogging devices are capable of communicating with each other. In our approach, the devices employ Bluetooth, thus making the prototype suited for correspondence or sharing of privacy settings over a relatively short range. When two or more users with the prototype devices meet, the devices dynamically compile an access control list (ACL) for the current location by sending messages via Bluetooth. The contents of ACL include the name and ID of the people in the vicinity, including the name of the sensors and the privacy settings (i.e., permissions to allow logging at that time and place). The ID is a unique identification of the person with the prototype device. A fresh ACL is created for each location visited by the user, including locations that are re-visited later on the same day.

Here we describe the process of privacy activation and sharing of privacy settings based on their activated privacy policies using an example. Assume three users of the prototype system, A, B and C, are frequent visitors of a library. A and B are friends on a social networking site, but C is unrelated with either A or B. Both A and B are privacy vigilant, i.e., they have set a geo constraint by selecting the library as a restricted location and enabled this privacy policy for everyday use on their devices. C has no concerns of being logged by anyone in the library, so has not set a privacy policy at the library. **Figure 5** illustrates the privacy polices defined by these users before arriving at the library. A and B have restricted both the microphone and camera sensors of neighbors from logging them. However, their accessibility settings are different; A has selected *strict*, which means that nobody is allowed to log him in the library, whereas B has selected *standard*, and listed some friends, including A, as allowed to log him, but not unknown users.

The geo constraints on the lifelogging devices of users A and B are activated when either of them arrives at the library with the device. Once a privacy policy is turned on, the accessibility parameter is examined for that policy. If it is *strict*, a message is compiled consisting of the user's social network name, the unique ID emitted by the attached infrared transmitter, the privacy settings (i.e., permissions for logging) and name of the restricted sensor for the activated policy. These messages are sent via Bluetooth to the logging devices of the neighbors. User A's lifelogging device compiles a message that reads {User A, AAA, Not Allowed, Both}, and sends it via Bluetooth to the logging devices of B and C, which maintain an ACL and record A's preferences, which in this case, states that they are not permitted to log user A in the library. The accessibility parameter of B's policy is *standard*, and for this reason a message is compiled containing only the social network name of B, and sent to the neighboring devices. The neighboring devices (within the range of Bluetooth connectivity) also share their social network names with B; receiving the names of the nearby users, B compares this with the names of allowed users in the social network's friends list. If a name is in the allowed friends list, a message is sent from user B to the neighboring devices, which reads {User B, BBB, Allowed, Both}. However, if the name is not found in the allowed friends list, it replies with a message that reads {User B, BBB, Not Allowed, Both}. In our example case, the lifelogging device of A is allowed to log B in the library. However, C is not permitted to log via any sensor; C sends a message that reads {User CCC, Allowed, Both}, allowing everybody to log them. In this way, the privacy policies are used to compile the ACLs on the lifelogging devices, as shown in Fig. 5.

Note that, in this example, users A and B are friends on a social network. Nonetheless, A's privacy policy did not permit B to log via the microphone or camera in the library. B's privacy policy allowed A to record data in the library, whereas anonymous people, including C, were not permitted to log B. Despite their diverse perspectives in terms of privacy from pervasive logging devices, both A and B have attained the required level of privacy. In the next subsection, we describe the algorithm used for lifelogging suspension, which is based on the ACL and proximity sensing.

2.1.3 Life Logging Suspension Algorithm

Here we describe the mechanism to suspend the sensors. Logging is suspended depending on the proximity and privacy settings of other devices, which are detailed in the ACL. Each user must have an infrared transmitter as part of the lifelogging device, as well as an infrared receiver facing in the direction of the camera in order to detect and identify the people in sight. Each user's infrared transmitter emits a unique 12-bit ID encoded on a 40-kHz carrier at 5-second intervals. As soon as an infrared receiver detects a signal from another device, the ID is checked against the ACL in order to obtain the privacy settings of that user. If the ID matches one in the ACL, the permissions for that infrared ID are assessed. For *allowed* permissions, both the camera and microphone of the lifelogging device are able to log the person in sight with no disruption. For *not allowed* permissions, the restricted sensor name is checked, which can either be *camera, microphone* or *both*; depending on this result, one or both sensors are deactivated and not allowed to log for 150 seconds, becoming active again in the absence of another request for logging suspension. If the received ID has no match in the ACL, i.e., the person in sight is not recognized, the lifelogging device continues to record with no disruption.

To implement the lifelogging suspension algorithm, we refer to the same example as discussed in Section 2.1.2. Three users, A, B and C have shared their privacy settings and updated their ACL for the location of library. A's *strict* privacy policy suspends the lifelogging devices of both B and C via both camera and microphone sensors whenever they are in proximity of A. The algorithm is intended to prevent logging by devices of neighbors in the vicinity of an individual without any intervention, and in accordance with the pre-defined privacy constraints set by that user.

3. System Description

A prototype was implemented on a Nexus S smartphone running Android 4.1. We used the integrated camera, microphone, Global Positioning System (GPS) and Bluetooth functionality to create a lifelogging device, and implemented the privacy framework described above. We utilized a 5-mm-diameter infrared light-emitting diode (LED) (Toshiba TLN110), which emitted a unique ID. These transmitters are commonly used in remote controls and switches. The infrared receiver (PL-IRM2121-A538) shown in **Fig. 6** (a) was used to receive signals from neighboring devices and input this data to the smartphone. The system has a range of 8 meters, and the receiver can detect at angles of 30 degrees. We follow the approach of Choudhury et al., and create a system that is similar to Sociometer [20], which can identify people in close proximity and understand face-to-face interactions. We used the Arduino Mega ADK Board [21], shown in Fig. 6 (b), to communicate between the sensors and the smart phone. This board had a 9-V external power supply (i.e., a battery) to serve the infrared transceiver functionality.

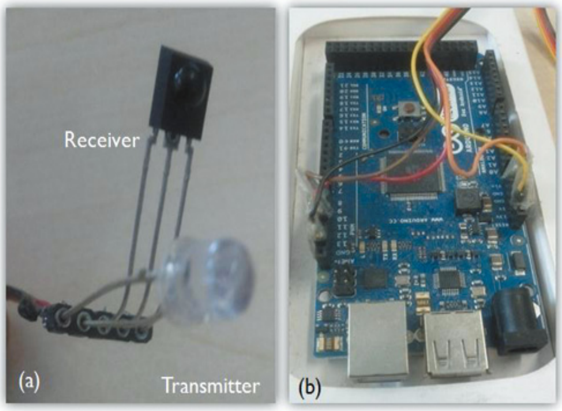


Fig. 6 Infrared Transmitter and Receiver (a). Arduino Mega ADK board (b).

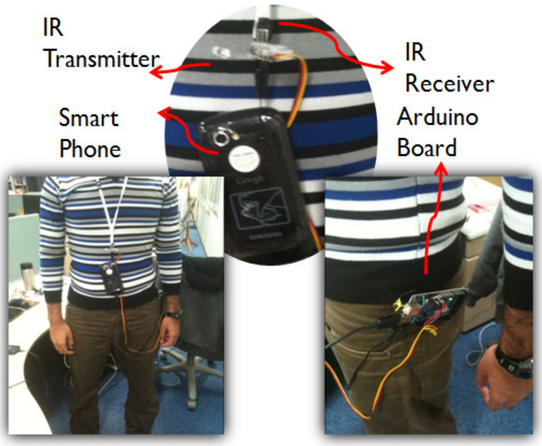


Fig. 7 The Prototype device [17].

The prototype system was wearable, using a 15-inch neck strap, with the infrared sensors fixed as shown in **Fig. 7**, and the microcontroller board attached to the waist of the user. The prototype device takes one picture and records 10 seconds of audio every minute unless interrupted by another lifelogging device with the appropriate privacy settings to cause a suspension of logging. The user may view the image or listen to the audio immediately or transfer all the data to a computer for viewing later. Because of the limitations of the hardware supplied with the smart phone, the image and audio quality is relatively poor; however, the focus here is on the privacy framework so, for the purposes of this study, we do not consider this to be a significant drawback. The Google Maps API for Android was employed to select private/restricted locations, and the Facebook API was used to create friends lists

Table 1 Sensors and APIs used by prototype system.

Sensors	Purpose
Camera	Capture logs in the form of images
Microphone	Capture logs in the form of audio records
GPS	Sense the current location
Bluetooth	Share user's name and Unique Id with bystanders
Infrared Transmitter	Emit appropriate infrared signals to neighboring devices
Infrared Receiver	Receive infrared signals from neighboring devices
APIs	Functions
Facebook API	Obtain customized friends lists
Google Maps API	Choose restricted location for Geo-temporal privacy

of users that have a given set of privacy settings. **Table 1** lists the purpose of device sensors and APIs that were employed in our prototype system.

4. Evaluation

4.1 Experiment to Assess Privacy Policy Input Interface

We carried out an experiment to analyze whether a user was able to easily set a privacy policy on the device. We created five sets of privacy settings, and asked users to create policies for each situation, which is designed to assess Research Challenge 1 (see Section 1). These situations are as follows:

Situation 1: Activate privacy when waiting for a train at the train station

Situation 2: Activate privacy at the work place during working hours

Situation 3: Activate privacy while meeting with a friend

Situation 4: Activate privacy during shopping at a mall

Situation 5: Activate privacy at a gym while exercising

At the end of the experiment, we evaluated the privacy policies set by the users to determine whether they had accomplished the task, and asked the users to comment on their privacy preferences. We mainly focused on the answers of Q5 and Q6 (see Section 2.1.1), as these determine whether the privacy policy will be geo, temporal or geo-temporal.

4.1.1 Participants

We recruited ten participants, 4 female and 6 male, aged 21–54 years with mean age of 37.1 years and a standard deviation of 8.82 years. The participants were professionals, including businessmen, doctors and engineers. Each user was briefed on the advantages and potential drawbacks of lifelogging devices, and how our system can help to improve privacy. The users were encouraged to take their time so that they could fully understand each situation prior to inputting the privacy policies into the lifelogging device.

4.1.2 Results and Summary

The privacy policies set by the users were reviewed, and we found that they opted for geo, temporal and geo-temporal policies based on to their own preferences, as shown in **Fig. 8**. In Situation 1, 50% of users created a geographical constraint, arguing that they often go shopping at the station and do not use the train at a regular time. The remaining users reported that they were sure of the time they will take the train, so chose a temporal constraint instead. For Situation 2, 50% of users commented that they commute during working hours and, therefore, preferred temporal constraints. The remaining users selected geo-temporal constraints to avoid logging in this situation, since they worked at a fixed place for a definite time period.

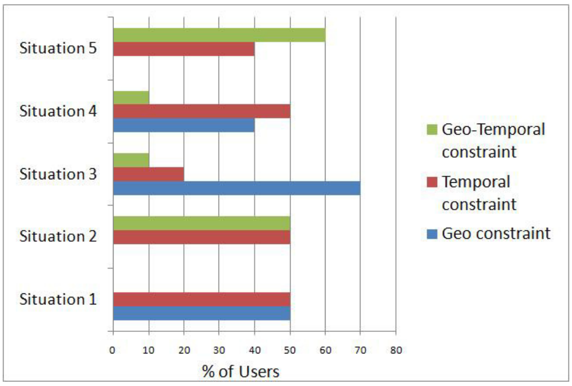


Fig. 8 Preferred privacy policies by the users for the given situations.

Geo constraints were favored by 70% of users for Situation 3, as they knew the location where they were going to meet a friend. Additionally, 20% of users reported that they often gather with friends at specific times, but not at fixed locations. One user said that he typically meets with his friend at the coffee shop during breaks from work; therefore, he selected a geo-temporal constraint for this situation. For Situation 4, 50% of users stated that they sometimes watch movies in the multiplex within the shopping mall and, hence, preferred a temporal constraint, and specified a shopping time only. Additionally, 40% of the users specified a geographical constraint, because they typically go shopping at a specific mall.

In Situation 5, 60% of users selected a geo-temporal constraint, as they desired privacy in the gym; however, 40% of users choose a temporal constraint, as they would only specify their exercise times to be restricted, and they preferred to be recorded at other times by their friends at the gym.

These results show that the users understood the situations well and built the constraints based on their own preferences. The mechanisms to achieve privacy, while being logged by specific users, were appreciated by the participants, and they were intrigued by the idea that privacy constraints on their lifelogging device can suspend the camera and microphone of neighboring devices. The simple and user-friendly interface made it easy for the participants to describe their privacy settings.

4.2 Experiment to Evaluate Logging Suspension

We carried out a second experiment to assess efficiency in achieving Research Challenge 2 (see Section 1). We configured four identical devices and provided them to users to wear during the experiment. We devised two study locations and observed the behavior of the devices at these locations for two weeks. Location 1 was a computer science laboratory where the users already had a fixed work place, and Location 2 was a cafe where they have lunch. Each user was asked to perform privacy activation tasks at the study location, as described in **Table 2**. We observed the privacy plans that each user specified and, to investigate the effect of privacy policies on the neighboring devices, we analyzed

Table 2 Tasks to be performed.

Tasks	Location	Time
Task 1: Set up a privacy setting to avoid logging from life log device of all the participants	(Location 1) Computer science laboratory	During stay
Task 2: Create a privacy policy that authorizes only one friend but denies all the rest to log	(Location 2) Cafe	During lunch time

Table 3 Privacy policies inscribed by the users.

Users	Task 1		Task 2	
	Geo-temporal	Temporal	Geo-temporal	Temporal
User A	11	14	0	10
User B	10	12	0	10
User C	13	8	0	10
User D	10	18	0	10

each subject's logs at the end of each day to trace the times and locations that the device was suspended from logging.

4.2.1 Participants

Four participants were invited to use the devices, and were given the option to suspend logging during private times, such as in the rest room. All four participants were students, with 1 female and 3 male, aged 26–31 years. They worked at the computer science laboratory, and had a good understanding of privacy issues associated with pervasive logging. Each participant was briefed for 30 minutes on how to specify geo-temporal privacy settings, and the consequences for neighboring devices. All of the participants were encouraged to accomplish the tasks at the study locations.

4.2.2 Results and Observations

To accomplish the requirements of Task 1, the users must restrict every participant from logging while they are at Location 1. Because each user's daily schedule for Location 1 was not consistent, they created more than two privacy policies for Task 1 in a single day. We observed that each user made privacy policies with the *strict* restriction to avoid logging from the remaining participants, and selected validity of *24 hours*. The users preferred temporal constraints to geo-temporal constraints in some situations, and selected the time intervals of their stay at Location 1. One of the reasons for choosing a temporal constraint for Task 1 was that, on many occasions, the users had fixed schedules while in the laboratory, and did not have plans to move to any other location during that period. **Table 3** lists the total number and type of privacy policies specified by each user during the two-week period. User D created the most policies, because he had part-time work 3 days a week, which required him to go to another location. The mean number of policies set by each user to accomplish this task was 2.4 per day.

To achieve Task 2, the location and times were not fixed, as the participants chose different places to have lunch each day. However, they all went together to complete Task 2. Therefore, each participant created a temporal privacy policy each day with a validity of *24 hours*, and selected lunchtime to accomplish Task 2. This policy was applied to the camera sensor and expired at the end of the day. Because of the *standard* restriction, each participant had to select one user to grant permission for logging. The selection of an eligible user for logging was done at random. We observed that each user created 10 privacy policies for Task 2 in total during the two-week period, and that they were all successfully activated at lunchtime, regardless of their location. The mean time required to create a privacy policy was 39.07 seconds for Task 1 and 36.37 seconds for Task 2.

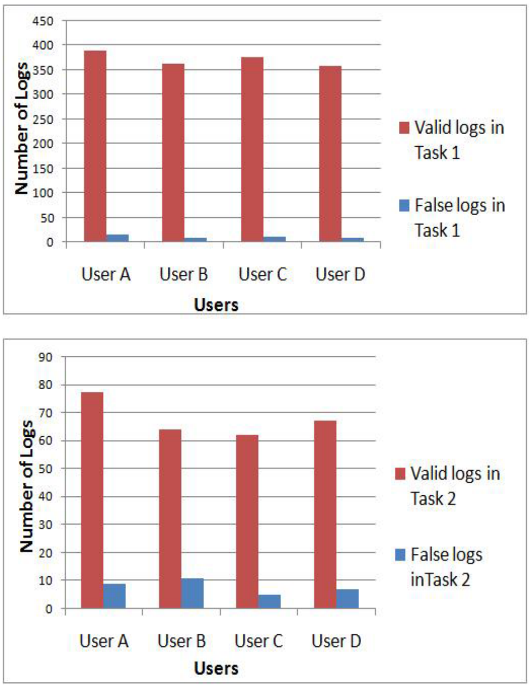


Fig. 9 Valid and false logs by each participant during the tasks.

The efficiency of our privacy control method can be assessed by considering the relatively small number of false logs. Here, a false log refers to logging a user (either via the camera or microphone) when the privacy settings of the neighbor do not permit logging. **Figure 9** shows a comparison of valid and false logs captured by each user at the study locations. The proportion of false logs by all participants was 2.8% for Task 1 and 10.5% for Task 2.

In Task 1, the *strict* restriction was specified by all users and, in principle, there was no opportunity for the neighboring devices to log anything; however, on average, 4.4 false logs were recorded per day during this task. The most common reason for false logging was because participants moved their hands while talking. The presence of an object obscuring the infrared sensors interrupted both incoming and outgoing signals.

The objective of Task 2 was to allow one friend to log during lunchtime, while denying all other users. The mean number of false logs during Task 2 was 3.2 per day. The loose-fitting of infrared sensors caused false logs during this task; on some occasions the infrared sensors were directed towards the permitted friends, whereas the camera was facing a different user, with active privacy restrictions. This limitation may easily be overcome by embedding infrared sensors with the camera, ensuring both devices are aligned in the same direction.

These results indicate that the approach is a promising method to achieve privacy from pervasive devices, even if there are more than two users at a given location with different privacy settings. At the end of the experiment, two questions were asked from the users to obtain their opinions of the privacy framework:

(1) Does wearing the device hinder your everyday work?

(2) Is the device useful for alleviating privacy concerns?

The users responded to these questions using a five-point Likert scale, where 1 corresponds to 'I do not agree' and 5 to 'I agree completely'. There was a mixed response to question (1), as some users complained that the device was heavy when worn on the neck for a prolonged period of time. However, in response to question (2), they were satisfied that the privacy framework could address their concerns.

4.3 Benefits and Limitations

The privacy framework described here is expected to be effective in a range of situations, especially when people are in close proximity to each other during a discussion, and their face may not be in the line-of-sight of the camera, but their voice can be clearly recorded. A privacy system with a face recognition tool would fail with no line of sight, and the device may continue to log the voice regardless of the privacy settings. Moreover, a computer-vision based technique may not be feasible for a lifelogging device because of the computational expense [22]. Our approach does not require complex algorithms, which is advantageous for commercial life log device because of the low power consumption.

The system was able to accurately detect other users in the range 0.15–6 meters, so long as a line-of-sight to the infrared transmitter was available. However, in some settings, the infrared transceiver system may be deliberately or accidentally obstructed and, as a result, logging of users with active privacy settings may occur. This can be overcome by embedding a light sensor in the device to prevent it from logging if there is not a significant change in optical power near the device over a given threshold time. In this manner, the person obstructing an infrared signal may not be able to log further.

5. Related Work and Discussion

Lifelogging brings to the fore a number of privacy issues, including emotional blackmail and other forms of exploitation [12]. In this section we discuss related work in three categories: sensor-based privacy, computer-vision-based privacy, and the privacy frameworks and methods employed during logging.

5.1 Sensor Based Privacy

Makino et al. developed a tactile sound-based lifelogging system employing a piezoelectric device located on the user's fingernail, which responds to touch and acoustic signals that propagate through the fingertip [23]. They attempted to enhance privacy by avoiding the use of a camera, microphone and GPS; however, this approach does not include a sufficiently rich array of lifelog data for many users requirements. If we consider that avoiding camera and microphone recording may ease privacy concerns, then several systems have been proposed using radio-frequency identification (RFID) tags [24], [25] and accelerometers [26] to recognize daily activities. Nevertheless, lifelogging entails a diverse range of information; the work described in Refs. [8], [27], [28] employed RFID approaches in conjunction with a camera and microphone to enrich lifelogs with contextual information and focused on reliving past events efficiently. However, the privacy of those nearby was not considered. Our approach ensures privacy while incorporating a camera and microphone, which are the most common sensors used in pervasive logging.

5.2 Computer-vision-based Privacy

The privacy issues associated with recording video or audio have been discussed by Chaudhari et al. [15]. Wearable lifelogging systems can attempt to protect privacy during video recordings in real-time using face detection, tracking and blocking algorithms to obscure the faces of subjects; however, this approach may fail in poor light conditions. Furthermore, the system depends upon skin color detection algorithms, which sometimes failed following a small movement of the shoulders (where the camera was mounted). Audio identification of subjects may be distorted using a time-based pitch-shifting algorithm. Furthermore, such approaches are computationally expensive, which creates problems for battery-powered devices.

Various methods have been proposed to protect privacy in video surveillance systems, including a system in which CCTV footage is encrypted, and only privileged users are given access to video data, and other users are only provided with statistical data on the objects contained in the video [16]. However, this approach may lead to errors including missed detection and false positives, and post-capture privacy techniques may reveal personal information if they fail. In our approach, we first identify other users in close proximity, and only record data if their privacy settings allow logging.

5.3 Privacy Frameworks and Methods

A privacy framework was proposed by Giang et al. [29], which employed pre-defined privacy policies based on trust values. They estimated trust via peer recommendations and previous interactions between individuals, and assigned three possible states to the requester of personal information: trusted, public or distrusted. O'Hara et al. suggested that the data recorded by lifelogging devices may be categorized as either public or private [1]. Rawassizadeh et al. [30] addressed privacy concerns after data has been logged using various sensors. They developed a sharing model in which the logged data has an expiration date. They pointed out that the use of smartphones for lifelogging can make data private via encryption [31]; however, their approach failed to consider the privacy of bystanders who may be in the range of the logging device. Petroulakis et al. [32] considered security and privacy issues in lifelogging in the smart environment and proposed a lightweight framework, with the focus on interconnectivity of devices and sharing of preferences and habits. They studied the energy consumption using a communication model and an attacker model using an experimental test-platform for secure sharing of lifelogs under different scenarios.

Thus, retaining privacy in the course of lifelogging has been of great concern with evolving technologies and prevailing gadgets. Our approach is novel as it incorporates individuals' consent before allowing the pervasive devices to log them.

5.4 Discussion

Lifelogging devices are expected to become increasingly pervasive, and are currently capable of recording indiscriminately, without regard for the privacy of those who do not wish to be part of someone's lifelogs. Privacy is a major issue for lifelogging devices. For example, the Defense Advanced Research Projects Agency (DARPA) LifeLog project was canceled in 2004 following criticism from civil liberties groups over the privacy implications of the system. For these reasons, we have developed a privacy system that provides an interface for users to declare privacy settings on their lifelogging devices. These privacy preferences affect only those sensors that are responsible for logging others.

There are some situations where lifelogging device users impose strict restrictions and deny being logged by others. For instance, in a restaurant or cafeteria, people may wish to avoid anonymous lifelogging. However, we are not always facing a stranger while eating at public places and, in our system, the camera or microphone only suspends logging for a relatively short duration when the person is facing a user with active privacy settings. Logging resumes when there are users in a line-of-sight of device when the duration of suspension of logging comes to an end. Moreover, personal logging sensors, such as GPS or accelerometers, are not affected during the suspension of logging with the camera or microphone. As a consequence, the devices will log only personal information related to the owner of the device and will not record any data on neighboring users. We place privacy concerns above maintaining a lifelog, since users should be guaranteed that they have the power to suspend logging by anyone. Using this mechanism, people may log personal life events, while ensuring the privacy of neighboring users.

6. Conclusion and Future Work

Extensive use of lifelogging devices in the future is expected to raise significant privacy issues, and effective mechanisms to protect people's privacy from continuous monitoring from pervasive devices will be extremely desirable. We employed an Android-based smartphone to function as a lifelogging device, while incorporating the privacy preferences of third parties. Our technique allows users to determine privacy settings by specifying restricted locations and times, while permitting specific friends to log them.

The evaluation results show that the approach provides a simple and effective way to specify a user's privacy preferences. The users of the proposed system felt that it was able to ensure privacy from neighboring lifelogging devices, and we believe that our work towards privacy-aware pervasive logging will influence future generations of lifelogging technology. We plan to extend our privacy framework to consider other methods of specifying privacy settings in addition to geographical and temporal constraints.

References

[1] O'Hara, K. et al.: Lifelogging: Privacy and empowerment with memories for life, *Identity in the Information Society*, Vol.1, pp.155–172 (2009).

[2] Gemmell, J. et al.: MyLifeBits:fulfilling the memex vision, *Proc. tenth ACM Intl. Conf. Multimedia*, pp.235–238 (2002).

[3] Czerwinski, M. et al.: Digital memories in an era of ubiquitous computing and abundant storage, *Comm. ACM*, Vol.49, No.1, pp.44–50 (2006).

[4] Kalnikaite, V. et al.: Now let me see where i was: understanding how lifelogs mediate memory, *Proc. SIGCHI Conf. Human Factors in Computing Systems*, pp.2045–2054 (2010).

[5] Kunze, C. et al.: Application of Ubiquitous Computing in Personal Health Monitoring Systems, *Biomedizinische Technik*, Vol.47, pp.360–362 (2002).

[6] Lee, M.L. and Dey, A.K.: Using lifelogging to support recollection for people with episodic memory impairment and their caregivers, *Proc. 2nd Intl. Workshop on Systems and Networking Support for Health Care and Assisted Living Environments*, pp.1–3 (2008).

[7] Kärkkäinen, T. et al.: I don't mind being logged, but want to remain in control: A field study of mobile activity and context logging, *Proc. SIGCHI Conf. Human Factors in Computing Systems*, pp.163–172 (2010).

[8] Kim, I.J. et al.: Personalized life log media system in ubiquitous environment, *Proc. 1st Intl. Conf. Ubiquitous Convergence Technology*, pp.20–29 (2007).

[9] Li, Y. and Landay, J.A.: Activity-based prototyping of ubicomp applications for long-lived, everyday human activities, *Proc. 26th SIGCHI Conf. Human Factors in Computing Systems*, pp.1303–1312 (2008).

[10] Microsoft Sensecam (online), available from ⟨http://research.microsoft.com/en-us/um/cambridge/projects/sensecam/⟩ (accessed 2013-12-17).

[11] Kallstrom, M.: Lifelogging camera: the narrative clip (online), available from ⟨http://getnarrative.com/⟩ (accessed 2013-12-17).

[12] Allen, A.L. and Gemmell, J.: Dredging up the past: Lifelogging, memory, and surveillance, *The University of Chicago Law Review*, Vol.75, pp.47–74 (2008).

[13] Cheng, W.C. et al.: Total recall: Are privacy changes inevitable?, *Proc. 1st ACM Workshop on Continuous Archival and Retrieval of Personal Experiences*, pp.86–92 (2004).

[14] Dubey, D.R. et al.: Reactions of children and teachers to classroom observers: a series of controlled investigations, *Behavior Therapy*, Vol.8, pp.887–897 (1977).

[15] Chaudhari, J. et al.: Privacy protection for life-log video, *Proc. IEEE Workshop on Signal Processing Applications for Public Security and Forensics*, pp.1–5 (2007).

[16] Senior, A. et al.: Enabling video privacy through computer vision, *IEEE Security & Privacy*, Vol.3, pp.50–57 (2005).

[17] Memon, M.A. et al.: Restrain from pervasive logging employing geotemporal policies, *Proc. 10th Asia Pacific Conf. Computer Human Interaction*, pp.201–208 (2012).

[18] Kelley, P.G. et al.: User-controllable learning of security and privacy policies, *Proc. 1st ACM Workshop on AISec*, pp.11–18 (2008).

[19] Vincenty, T.: Direct and inverse solutions of geodesics on the ellipsoid with application of nested equations, *Survey Review*, Vol.22, pp.88–93 (1975).

[20] Choudhury, T. and Pentland, A.: The sociometer: A wearable device for understanding human networks, *Proc. Workshop on Ad hoc Communications and Collaboration in Ubiquitous Computing Environments* (2002).

[21] Arduino mega adk board (online), available from ⟨http://www.arduino.cc/en/Main/ArduinoBoardADK/⟩ (accessed 2013-12-17).

[22] Anuar, A. et al.: Opencv based real-time video processing using android smartphone, *Intl. Journal of Computer Tech. and Electronics Engineering (IJCTEE)*, Vol.1, pp.58–63 (2011).

[23] Makino, Y. et al.: Life log system based on tactile sound, *Proc. Intl. Conf. Haptics: Generating and Perceiving Tangible Sensations*, pp.292–297 (2010).

[24] Smith, J.R. et al.: Rfid-based techniques for human-activity detection, *Comm. of ACM Special issue: RFID*, Vol.48, pp.39–44 (2005).

[25] Minamikawa, A. et al.: Rfid supplement for mobile-based life log system, *Proc. Intl. Symp. Applications and the Internet Workshops*, p.50 (2007).

[26] Kwapisz, J.R. et al.: Activity recognition using cell phone accelerometers, *ACM SIGKDD Explorations Newsletter*, Vol.12, pp.74–82 (2011).

[27] Blum, M. et al.: Insense: Interest-based life logging, *IEEE Multimedia*, Vol.13, pp.40–48 (2006).

[28] Aizawa, K. et al.: Efficient retrieval of life log based on context and content, *Proc. 1st ACM Workshop on Continuous Archival and Retrieval of Personal Experiences*, pp.22–31 (2004).

[29] Giang, P.D. et al.: A trust-based approach to control privacy exposure in ubiquitous computing environments, *Proc. IEEE Intl. Conf. Pervasive Services*, pp.149–152 (2007).

[30] Rawassizadeh, R. and Tjoa, A.M.: Securing shareable life-logs, *Proc. IEEE 2nd Intl. Conf. Social Computing*, pp.1105–1110 (2010).

[31] Rawassizadeh, R. et al.: UbiqLog: a generic mobile phone-based life-

log framework, *Personal and Ubiquitous Computing*, Vol.17, pp.621–637 (2013).

[32] Petroulakis, N.E. et al.: A lightweight framework for secure life-logging in smart environments, *Information Security Technical Report*, Vol.17, No.3, pp.58–70 (2013).

Mohsin Ali Memon is a Ph.D. candidate in the Department of Computer Science at University of Tsukuba, Japan. His research interests include interaction technologies, lifelogging, and privacy control methods. He received his B.Eng. in Software Engineering and M.Eng. in Information Technology at Mehran University of Engineering and Technology, Pakistan, in 2006 and 2009, respectively.

Jiro Tanaka is a Professor of Department of Computer Science, University of Tsukuba. His research interests include ubiquitous computing, interactive programming, and computer-human interaction. He received a B.Sc. and a M.Sc. from the University of Tokyo in 1975 and 1977. He received a Ph.D. in Computer Science from the University of Utah in 1984. He is a member of ACM, IEEE and IEICE.