Restrain from Pervasive Logging Employing Geo-Temporal Policies

Mohsin Ali Memon
University of Tsukuba
1-1-1, Tenno-dai, Tsukuba,
Ibaraki, 305-8573 Japan
mohsin@iplab.cs.tsukuba.ac.jp

Jiro Tanaka
University of Tsukuba
1-1-1, Tenno-dai, Tsukuba,
Ibaraki, 305-8573 Japan
jiro@cs.tsukuba.ac.jp

Tomonari Kamba
NEC BIGLOBE, Ltd.
1-11-1, Osaki, Shinagawa,
Tokyo, 141-0032 Japan
kamba@biglobe.co.jp

ABSTRACT
Life logging has been a prominent research concern in recent years with the invention of wearable life capture gadgets and it has played a significant role in some situations such as helping Alzheimer disease patients. However, at the same time, it has raised privacy concerns among ordinary people. At present, life log devices are pervasively capturing information, including people in the vicinity without their consent. This will produce a great concern in the future if the majority of people come to have life log devices that record continuously what is happening around. In this paper, we propose a mechanism to restrict people from capturing a person in their personal digital diaries in real time by introducing Geo-temporal privacy framework. Furthermore, the system ensures that the unwilling party is not revealed to the life logging system users and privacy is sustained when the Geo-temporal framework discontinues the log activity after an encounter with the reluctant party. The prototype is developed on an Android-based smart phone that works as a life log device with a policy controller. The phone is connected to an Infrared Transmitter/Receiver with an interface board, for identifying human proximity.

Author Keywords
Life log; geographical; temporal; pervasive; neighbor; privacy.

ACM Classification Keywords
H.5 INFORMATION INTERFACES AND PRESENTATION: H.5.1 Multimedia Information Systems---*Evaluation/methodology*.

General Terms
Human Factors; Security; Privacy.

INTRODUCTION
Life logging is a strenuous activity where our day to day activities such as dining, travelling, congregating, etc. are recorded. The invention of compact and portable capture devices have driven people towards saving and maintaining their personal life experiences. Several attempts have been made by various researchers to digitize day to day activities, thus, increasing the social acceptance of personal life logging. Among them, "My life bits" [1] project by Gemmell et al. used Microsoft SenseCam to capture everything beyond legacy content, like papers, photos, and videos, into a second level that included real time capture of conversations, meetings, sensor readings, health monitors and computer activity, collecting around 1-2 thousand photos every day. In [2], Kim et al. used body worn sensors including audiovisual device, GPS, 3D-accelerometer and processed logged information to create metadata to be retrieved easily afterwards.

Without denying the benefits of the above mentioned research, we naturally pose the following question: what if people do not want to be captured by someone's life log device? This is where the Geo-temporal privacy framework comes into play. The proposed idea redefines the meaning of privacy in terms of life logging, because while detaining these personal experiences and activities, we inadvertently capture numerous people without their consent, thus negating the idea that life logging is a solipsistic activity, since the captured crowd may include friends, family members or strangers. Because these life log devices are consistently retaining everything in our life from watching TV to waiting for the train and so on, the problems arise when our personal life log device is obtaining pictorial and auditory information of our neighbors in the course of maintaining the record of our life. Such situations may be unsettling for those who love their privacy and do not like to be captured or recorded by someone they are unaware of, at a particular location and time.

In order to avoid circumstances where users are always concerned that their movements are captured by someone, the proposed system permits them to employ privacy policies on various life log sensors and hence decide by themselves whether anonymous people can capture them at a certain place and time. These policies facilitate the people to select specific locations and time slots when their neighbors will not be able to confine their activities. The exploitation of such systems can be practical in various situations. For

APCHI '12, August 28–31, 2012, Matsue-city, Shimane, Japan.

example, a person might restrain anonymous people from taking pictures of them in informal company gatherings or they may feel uncomfortable when their colleagues try to capture them when they fail in an assessment.

In general, the purpose of life log is to recall previous events including the people we came across or what others said when we were in a gathering in a natural setting. At the same time, it may compel us to be vigilant when we come to know that our daily lives are being captured, resulting in unnatural behavior. Furthermore, the use of such logs in lawsuits is also a matter of concern, which still needs to be addressed.

VARIOUS CONCERNS IN NEIGHBOR'S LOGGING

Let us assume we are using a messenger service on the internet, where we have various status options to choose from, such as, *away*, *busy* or *offline* mode, and we select one depending on our mood or availability of time to interact with others. The activity of capturing neighbors via life log devices is not much different because the neighbor's consent to be a part of one's life log is indispensable. Life log devices are capturing the events and objects without any intervention. When it comes to taking a picture or recording a person's voice, many people dislike to be recorded by an anonymous person and like to have the control of their privacy, depending on the place and people they are surrounded by. A survey conducted by Karkkainen et al. in [3] supported the idea that people were content with life logging when they had the authority to share the photos and videos taken by the life log device, but showed utmost care in case of neighbor's pictures as no proper privacy mechanism was available to deal with such situations. Allen et al. in [4] also showed concerns over legal and ethical problems of life logging and named the work of [1] as an act of sousveillance or surveillance when the SenseCam takes snapshots of people around the owner of life log device. They also wondered whether this data can be used in lawsuits to prove criminal acts. The purpose of research by Cheng et al. in [5] was to emphasize legal and social questions while pervasively logging everything in life. They proposed an authenticity mechanism ensuring the originality of the data being logged. According to them, the life logging systems will be commonly used by people in future just like cell phones and credit cards, exposing where we were and when. The survey conducted in [6] to gain feedback about the use of SenseCam revealed that most of the people preferred to be informed and asked before any recorded data was to be shared.

Hence, there are various privacy concerns pertaining to what a person does with our pictures, videos or recorded conversations and poses a clear threat if shared on social networking sites without our knowledge, thus placing us in an uneasy situation. Therefore, the need to cope with such situations is clearly arising in the course of logging neighboring information. The next section explains our approach to halt logging others unless given permission to do so.

OUR APPROACH

Life log sensors can be categorized as Personal log generator and Neighbor log generator. Personal log generators are obligated to log user's daily activities and trace visited locations, where as neighbor log generators are capable of capturing the people around. The research presented in [7,8,9] shows the most suitable examples of personal logs generation, because the sensors used by the authors help to recall events related to a particular location and assist in diagnosing a disease through previous health records.

Here, we have no concern over personal logging, but we are interested in developing a Neighbor log generator which may capture the neighbors only with their agreement. This happens because if we make our neighbors aware that we are observing them with our life log device, it may induce spuriousness in their conduct. Therefore, we present Geo-temporal privacy framework which empowers people to defend themselves from unauthorized logging. The following subsection illustrates this framework in detail.

Geo-Temporal Privacy Framework

Geo-temporal privacy framework helps a user to inscribe privacy in the context of location, time, or both, over the explicit sensors worn by neighbors posing a threat to his day to day dealings. The constraints or privacy policies are classified as geographical (location based) and temporal (time based), which are to be applied on the neighbor log generator as shown in Figure 1. We call these constraints "geo-temporal."

Neighbor log generator is capable of observing people around, by recording their conversations and capturing videos and pictures. The competence of such sensors is best explained in [1,2,10,11] and these sensors work without the owner's intervention, as they are fairly sensitive. Although, the neighbor log may contain geo tags adhering to the captured data; in this case, audio and pictorial information of people around is of immense privacy concern.

The users of the proposed system are allowed to apply either geo, temporal or both constraints on each neighbor log

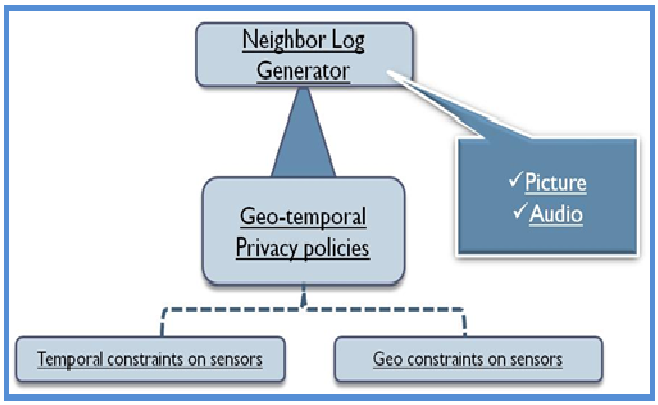


Figure 1. Geo-Temporal Privacy Framework

generator carried by the people in their vicinity. These privacy constraints or policies facilitate a user to hide from unidentified people, depending on specified location and time, thus imposing a selection criterion over anonymously produced content by life log devices of the people in a close proximity.

The above mentioned framework, when applied in a life log device, grants the authority to hide from unnecessary sensing. This framework is effective even if extended to more than two neighboring log generators. In the broad perspective, it encourages people to continue their routine activities as they please, without being secretive or restrained in any way.

Privacy Policies

Every privacy policy resides in the owner's life log device. The policy is a tuple of:

<sensor, accessibility, validity, provision>,

determining how the restriction should behave on the neighbor's life log sensors when triggered. These policies are inscribed by the life log device possessor and values for the type of sensor, accessibility level, validity period and provision of policy are to be selected. Figure 2 depicts the way each privacy policy is infixed in the life log device so as to keep a user from being recorded by pervasive logging devices in his/her neighborhood.

The Sensor can be a camera, microphone or any other device capable of logging passerby's information. Accessibility determines the restriction level of the policy, where, *strictly restricted* means no one is allowed to capture, *moderate restricted* means family members are allowed, whereas, *standard restricted* means family, friends as well as neighbors are allowed to log the person. In figure 2, neighbor refers to the person who lives in the neighborhood. The user may select certain levels of reservation from people in his/her vicinity depending upon his/her frame of mind. Validity specifies the lifetime of a policy after which the policy dies and this parameter is frequently monitored to keep checks on policies that have expired and to delete them as well. Here, *present day* policy expires after the day comes to an end but *everyday* policy never expires. Provision is allowed either by restricting a particular location, a certain time span or both. It depends upon circumstances where preferring the location is more significant because of indefinite time duration, or selecting a time slot regardless of location.

The attributes of each policy such as sensor type, accessibility level, validity period and provision are to be decided by the user for appropriate situations. For example, people may inscribe an everyday policy for restricting a stranger to picture them at a fitness center/dance club. In this example, the restriction is applied on the camera of people around who are unknown. The validity of that policy is every day because visits to that place are frequent with no time restrictions. The privacy policies are activated automatically

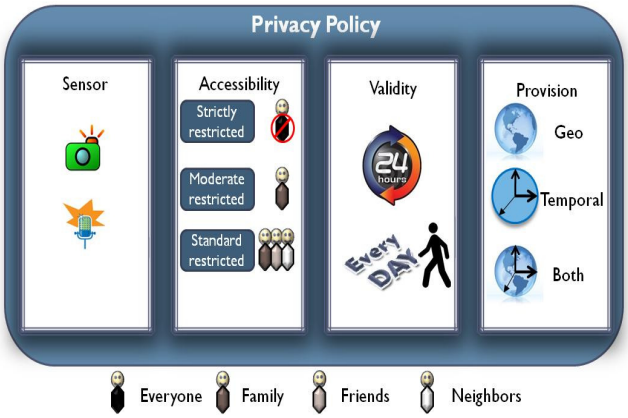


Figure 2. Privacy Policy attributes

when a person enters the location inscribed on their devices or when the time specified for a particular policy commences, thus, enabling the restrictions to be applied on the passerby's life log devices.

Policy overlapping

A policy is assumed to be weak and may be triumphed over by a strong policy only if changes occur in policy accessibility and temporal values but the rest of the parameters remain the same. This phenomenon is named as 'Policy overlapping'. The overlapped policy is always a one day policy, which means that the lifetime of overlapped policy is for the current day, after which that policy is no longer effective.

Policy overlapping may be suitable in situations where an everyday policy may be overlapped by an occasional one day policy due to some changes in the schedule. For example, a person who wishes to spend more time at work simply changes the temporal value of his/her privacy policy, leaving the other parameters untouched, hence s/he achieves policy overlapping. Similarly, a standard restricted policy is overlapped by strictly restricted policy in situations such as when a person is at a party and s/he is revealing hard facts about something/someone which s/he does not want logged by anybody.

SYSTEM DESIGN

The proposed system presumes that everyone wears identical life log devices which are capable of communicating with each other. A life log device in this approach is composed of a GPS enabled smart phone connected to an infrared Transmitter/Receiver pair. The smart phones have built in Bluetooth, thus making them compatible to communicate or share information within a certain range. Each user wears the smart phone with the help of a 15 inch long neck strap and plants an infrared LED on it with a receiver facing others. Here, infrared Transmitter/Receiver is used to detect and identify people in sight or face to face interaction. Choudhury et al. first used this technique to measure face to face interaction between people in [12].

Policy Implementation

The privacy concerns of a user employing the life logging device are advocated in the form of privacy policies, which are stored on the user's life log device. Once these policies are set, the user's location and time is being monitored for the privacy policy to be activated. To apply privacy restrictions, users share their privacy concerns relating to current location and time, along with contact and infrared ID to the people nearby via Bluetooth. The infrared LED worn by the users emits distinctive signals within regular intervals, while the infrared receiver detects the beam of infrared light. Once the human proximity is perceived, the passerby's life log device is directed to act according to the privacy concerns of the person in sight. Figure 3. shows the steps being followed in the course of logging bystander's activities, in this case, taking pictures, while considering the individual's privacy policies delineated by him/her for that location/time or both.

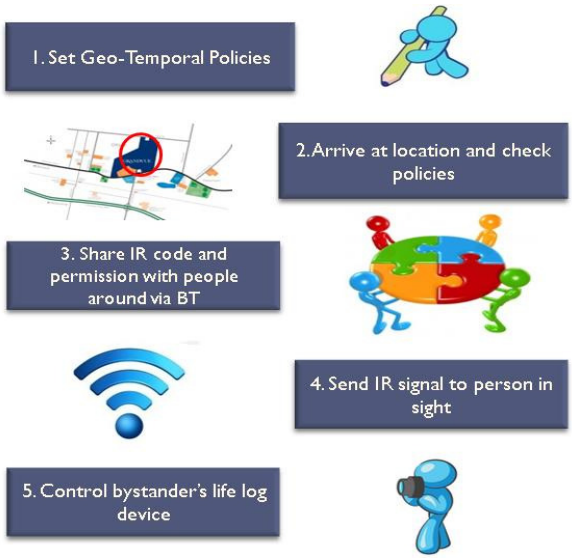


Figure 3. Steps followed to prevent oneself from pervasive logging

Potential Scenario

The system mentioned above fits best in situations where we are visiting a crowded place such as a social gathering with our family members, but it also saves us from scrutiny of others in the confines of our own home. Let us envision that we have invited our relatives, friends and neighbors to a gathering at our home. Here, we may not mind our family members to log us, but hesitate to permit friends or neighbors capturing us or other family members in their pervasive life log devices. Therefore, we make a moderate restricted privacy policy to discontinue the camera operation being performed by life log devices on our friends and neighbors. We broadcast our infrared ID and logging permissions to the people in our home. Figure 4 explains a situation where the privacy concerns are being shared among four users of the system within Bluetooth range and the Access control list (ACL) is maintained by all four users. Here, user A

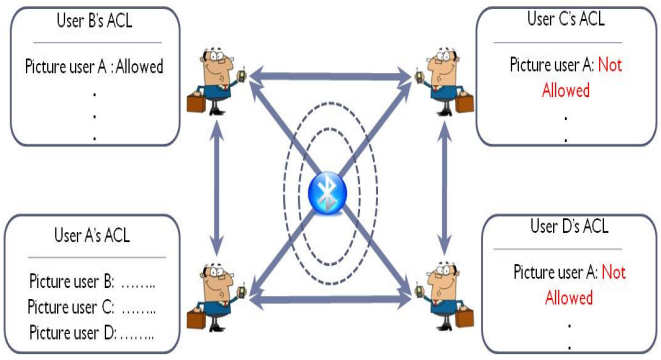


Figure 4. Policy sharing among Bluetooth enabled devices

represents the host, user B is a family member, whereas user C and user D represent a friend and a neighbor respectively. The ACL contains information of who can capture user A with their life log devices. Thus, in this example, user B is permitted to take user A's picture but when there is a face to face contact with user C or user D, their life log device is unable to capture User A. The privacy policy inscribed by the host, who is represented as user A, and its influence on people arrived at a gathering is shown in Figure 5.

The proposed approach protects an individual from being logged by others' life capture devices, depending on the policies prescribed by him/her for a particular place, time or both. It also ensures that the unwilling participants in life logging are not disclosed to the person monitoring the life log device content at that time, but instead, it only records the identification and contextual details to help maintain the owner's life log.

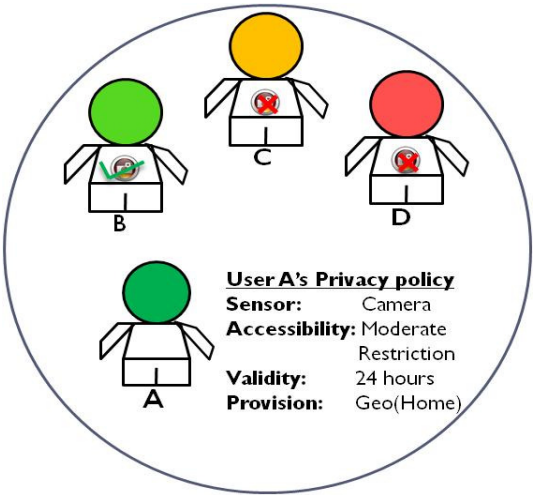


Figure 5. Scenario explaining the proposed approach

SYSTEM FUNCTIONALITY

Device prototype

Our life log device used as a prototype for the proposed approach consists of a Nexus S smart phone employing Android 2.3.6. The infrared Transmitter/Receiver communicates with the smart phone through an Arduino Mega ADK board [13]. The transmitter used for the

prototype is a 5mm round infrared LED and the infrared remote control receiver module helps in detecting the signals arriving from a distance of 9 meters at an angle of ±30°.

The current prototype is wearable, as shown in Figure 6, but it is limited to only control the built-in smart phone camera of the life log device wearer. The camera captures the surroundings with a regular interval of 60 seconds unless interrupted by the reluctant party. Figure 7 shows some pictures stored in the gallery of the smart phone and taken while wearing the proposed life log device on a certain day. The pictures stored on the life log device can be viewed date wise as well as location wise. Being a smart phone, the capabilities of the prototype life logging device are quite restricted since it is not meant to be literally used in logging everything. Thus, a discussion about the efficiency of the life log device and the way it helps to remember the past events is outside the scope of this paper.

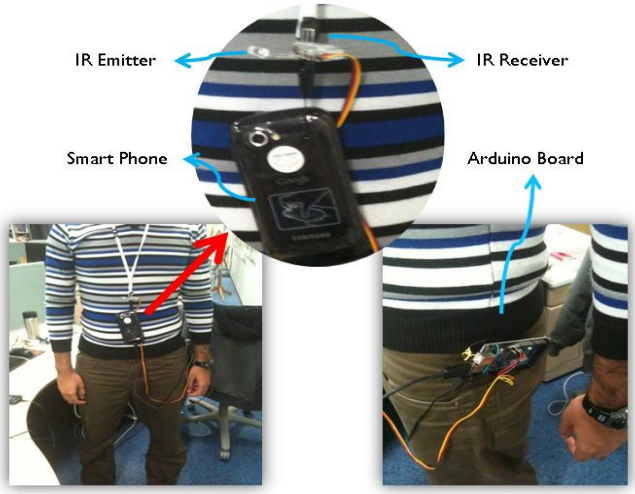


Figure 6. Life log device prototype

Policy Inscription

The privacy policies are inscribed using an android application and stored in the SQLite database. These policies are continuously being monitored so as to apply specified restrictions on passerby's life log devices. Each user is entailed to explicitly determine the privacy policy by picking the sensor type, accessibility, validity and provision values as shown in Figure 8(a). By default, a policy is 'standard restricted', which means that the family, friends and neighbors, determined by the contact list on the user's cell phone or social network, are allowed to capture. A policy is being checked for an overlap if the validity of newly created policy is set for *present day*. If a user selects 'Geo' provision, then a map is shown to mark locations to activate the privacy, as shown in Figure 8(b). Here, the user`s current location is marked by a green pin and the restricted location is marked by a blue circle. The restricted location is where the privacy policy is activated. The user can select multiple locations for a single policy, but can only deselect the last selected location by pressing the 'Remove' button. Each selected

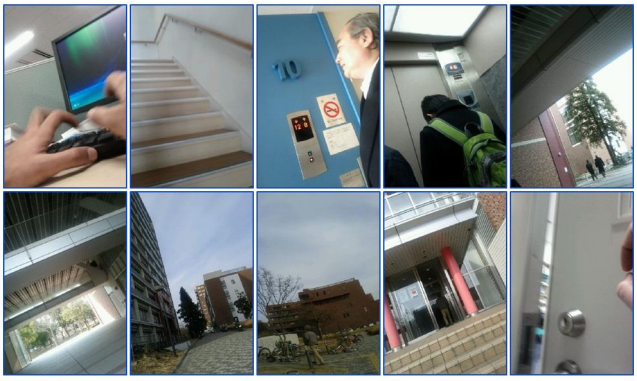
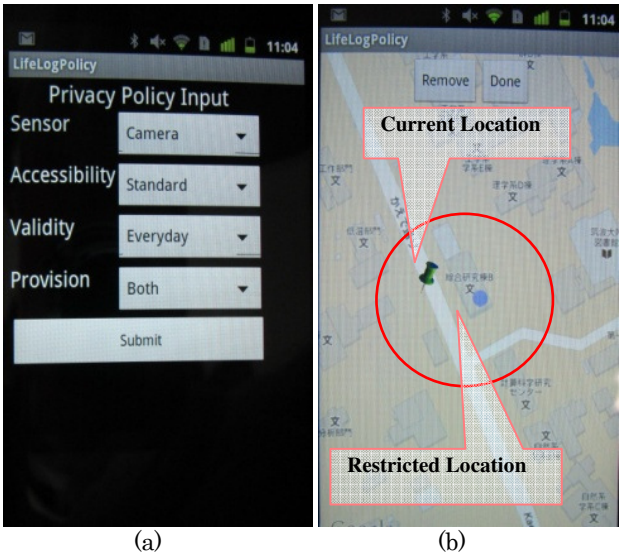


Figure 7. Proposed Life log device capturing neighborhood

location on the map means that the policy applies around a 100 meter radius of that location. If the user selects 'Temporal' provision, then a timer box appears to determine the time slot for maintaining the user's privacy during the prescribed timing. By selecting 'Both' provision, the user is requested to determine both location and time parameters to restrict bystanders from logging when s/he is in their vicinity. This is decided by the user or owner of life log device to either guard his/her privacy at a particular location for a specific time duration or for the whole day.

The provision of selecting either location or time may be useful in various circumstances. For example, if we are doubtful about the duration of staying at a particular location and desire no unidentified person to capture our activities, then we may choose geo provision for that privacy policy. On the other hand, when we are uncertain about our prospected location, but we do not want anyone to bother us during a particular period of time, then we make a temporal constraint. The owner of the privacy policies is given the liberty to edit everything, including accessibility, sensor type, validity, etc, except for the main values of location and time. This is because doing so would result in an entirely new



(a) (b)

Figure 8. Life Log Privacy Policy Android App

policy. Hence the best option would be of constructing a new policy instead of editing the old one.

System Execution

On arrival at a particular location, user's privacy policies are examined for a possible policy overlap for that location or time and then the user's consent about that location and time along with infrared ID is shared among other life log devices within the Bluetooth range in order to maintain an individual's ACL for that location. The infrared LED worn by the user is emitting signals at an interval of every 5 seconds. Whenever there is a person in sight, the receiver detects the infrared ID and transmits it to the smart phone, where the ACL is referred and the sensor is signaled, whether to sense the information around or not. As the infrared light is not viewable by human eye, thus, it substantiates the invisibility of unwilling person. The life log system keeps the identification of the passerby who has restricted others to capture him/her; hence, in this unique way the spirit of the life logging is still preserved, even while the privacy policies are in operation.

The system ensures that the privacy constraints defined by the user of the system are strictly followed during the course of maintaining personal life log. These constraints desist anonymous capturing by the life log devices of the people in the vicinity of the person wearing the proposed life log device.

EVALUATION

At first, we identify the key research challenges of this study which are being listed in the next subsection. Subsequently, the results of experiments being performed on the prototype application are presented. The motivation behind the first and second research challenges is to emphasize the need of a restriction mechanism which may help the users feel more contented while wearing the life log device. The third and fourth research challenges are related to the efficiency and effectiveness of the proposed mechanism.

Research Challenges

The research tries to answer the following questions.

1. Does the user wearing life log device literally amend the neighbor's behavior if the restriction policies are not in function?
2. How does the user feel when s/he has the trigger to the life log sensor of the person in sight?
3. Are the contextual parameters, in this case geographic location and time allocation for privacy constraints, enough or is there is a need to add another parameter?
4. Is the proposed mechanism influential in eradicating the threat of anonymous logging and what is the success rate of the system?

Experiments and Results

The first question was answered by asking 16 users (12 male and 4 female) to allow a stranger to take a picture of them during their routine work. All the users denied being captured by a stranger and most of them agreed that they would intentionally change their behavior in case they knew they were being photographed.

In the next step, the users were asked if they had the authority over the remote control of the camera shutter directed towards them. In response to the second question, 87.5% users replied that, in this case, the decision would depend upon their mood and situation. The rest of the users declined of allowing unfamiliar person to capture them even when they were given the command over their camera shutter. This conclusion strengthens the idea of creating a mechanism which may protect from anonymous logging.

The next two questions were asked by allowing the users to utilize the prototype application and select the restricted locations and timings of where and when they would not tolerate someone else to record them. The system was assessed by users in pairs to verify the prototype working and the results are shown in Figure 9.

In answer to question 3, 75% of the users warranted that the geo and temporal constraints are enough to ensure privacy and that the system is very easy to operate. Four users claimed that there can be some other contextual parameters apart from geo and temporal constraints, two of them had no other option in mind at that time. One user asserted that an option of broadening and curtailing of the restricted area should be supplemented in the prototype, which positively allots more authority in the hands of the user. The other user replied that while performing a certain activity we may switch off being logged by neighbors.

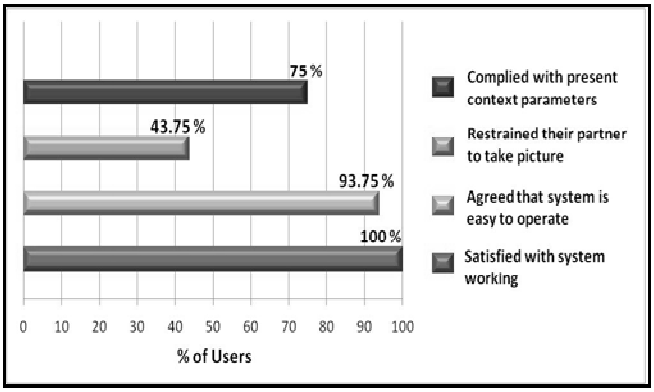


Figure 9. Evaluation of the prototype application

Question 4 was answered with 43.75% users inhibiting their partner from capturing them, while the remaining users allowed their partner to log them at their current location. The users who refrained from being captured were satisfied with the working of the system, because they were cloaked from the sensors of the partner, and the only information being logged was their name, time and location. According to them, it was easy to inscribe a privacy policy and apply restrictions over the passerby's life logging device. The system worked successfully all the time due to the fine range

of the infrared LED and receiver that helped in instant detection of human proximity.

The users were also asked to specify which of the constraints suited them the most. Among them, 43.75% voted for geo constraints, 6.25% voted for temporal constraints and 50% voted for both. The reasons behind their preferences were very definite. One of the geo constraint preferring users presented the argument that he would not want his lab mates to capture him while in the lab, because at times he is found slumbering in his chair. A temporal constraint preferring user on the other hand did not want to be captured the whole day when he was wearing lousy clothes. Table 1 shows the users' preference towards geo-temporal constraints.

A weak spot of the prototype appeared when four users complained that the pictures taken with the smart phones were either blurry or the people in sight were sliced. The reason is that, even though the length of the neck strap on all users was the same, the people wearing it differed in their respective heights. Moreover, the smart phone camera did not produce very good results when the users were in motion.

RELATED WORK

There are two ways to impose privacy over the life log data. One method addresses privacy during live capture while the other deals with post capture distortion to maintain privacy. Most of these approaches employ computer vision techniques which has some serious flaws such as missed detection and false alarm, as discussed in [14].

Various privacy issues while capturing video or recording voice were discussed in [15]. The wearable life log system attempted to protect the privacy of life log video recordings in real time. The system used face detection, tracking and blocking algorithm to obfuscate the faces of the subjects with solid-color block, but this approach is vulnerable to missed detection in bad light conditions. Furthermore, the system depends upon skin color detection algorithm, which fails even with a tiny movement of the shoulder where the camera is mounted. The audio identity of the subject is distorted using a time-based pitch shifting algorithm.

In [3], the users were allowed to decide whether to log and share photos or videos taken by the life log device and concerns were shown for neighbors' pictures and videos; however, no mechanism was proposed to avoid such circumstances.

In [15], Makino et al. developed a tactile sound based life logging system employing a piezoelectric device on finger nail and recording the touch sound propagating through a fingertip. The mechanism enhanced privacy by avoiding camera, microphone and GPS sensors, however, the essence of life logging cannot be achieved as the captured information of touched objects is not rich enough to assist in the course of reminiscence.

In contrast to these techniques, we have developed a runtime mechanism to stop neighbors' logging unless acknowledged by the owner, hence inducing a sense of consent before being captured by the life log device of others.

	Geo context	Temporal context	Both
Users	7	1	8
%	43.75%	6.25%	50%

Table 1. User's preference towards geo-temporal constraints

CONCLUSIONS AND FUTURE WORK

In the near future, wearable life log devices will be widespread and dominant. The act of logging everything and everyone is cumbersome, but easy to achieve at the same time. The threat of being monitored might drive people to behave in an unnatural way. The proposed framework attempts to prevent anonymous logging by specifying the privacy policies on the user's life logging devices, thus, ensuring their privacy pertaining to a specific location or during certain time slots of the day, or both. Furthermore, the system conceals the reluctant individuals who insist on their privacy and disagree to expose themselves to other users of the system.

The prototype system has gained a positive feedback from the experimenters and strengthened the idea of applying geo-temporal policies to restrict others to capture people in their daily life. In the next step, we are planning to extend the framework which can recognize hand gestures at runtime and discontinue the operation of life logging devices worn by people in the vicinity, since we might forget to inscribe a privacy policy for a place or time span where we are not willing to be recorded by others.

ACKNOWLEDGMENTS

Many thanks to Simona Vasilache for her valuable suggestions and comments.

REFERENCES

1. Gemmell, J., Bell, G., Lueder, R., Drucker, S., Wong, C. MyLifeBits: fulfilling the Memex vision . In *Proc.* Multimedia (2002). ACM; 2002 . p. 235–238.
2. Kim, I.J., Ahn, S.C., Kim, H.G. Personalized life log media system in ubiquitous environment. In *Proc.* Ubiquitous convergence technology 2007. Springer-Verlag; 2007. p. 20–29.
3. Kärkkäinen, T., Vaittinen, T., Väänänen-Vainio-Mattila, K. I don't mind being logged, but want to remain in control: a field study of mobile activity and context logging. In *Proc.* Human factors in computing systems 2010. ACM; 2010. p. 163–172.
4. Allen, A.L., Gemmell, J. Dredging up the past: Lifelogging, memory, and surveillance. The University of Chicago Law Review. 2008;75(1):47–74.

5. Cheng, W.C., Golubchik, L., Kay, D.G. Total recall: are privacy changes inevitable? In: *Proc.* Continuous archival and retrieval of personal experiences 2004. ACM; 2004. p. 86–92.
6. Nguyen, D.H., Marcu, G., Hayes, G.R., Truong, K.N., Scott, J., Langheinrich, M., et al. Encountering SenseCam: personal recording technologies in everyday life. In *Proc.* Ubiquitous computing 2009. ACM; 2009. p. 165–174.
7. Intille, S. S., Tapia, E.M., Rondoni, J., Beaudin, J., Kukla, C., Agarwal, S., Bao, L., Larson, K. Tools for studying behavior and technology in natural settings. In *Proc*. UBICOMP 2003; Springer; 2003: 157–174.
8. Kern, N., Schiele, B., Schmidt, A. Recognizing context for annotating a live life recording. Personal Ubiquitous Comput. 2007 Apr;11(4):251–263.
9. Li, Y., Landay, J.A. Activity-based prototyping of ubicomp applications for long-lived, everyday human activities. In *Proc*. SIGCHI Human factors in computing systems 2008. ACM; 2008. p. 1303–1312.
10. Blum, M., Pentland, A., Troster, G. InSense: Interest-Based Life Logging. IEEE Multimedia. 2006 Dec;13(4):40–48.
11. Aizawa, K., Tancharoen, D., Kawasaki, S., Yamasaki, T. Efficient retrieval of life log based on context and content. In: *Proc.* Continuous archival and retrieval of personal experiences 2004. ACM; 2004. p. 22–31.
12. Choudhury T., Pentland A. The Sociometer: A Wearable Device for Understanding Human Networks. In Workshop on Ad hoc Communications and Collaboration in Ubiquitous Computing Environments. 2002.
13. Arduino Mega ADK Board http://www.arduino.cc/en/Main/ArduinoBoardADK
14. Senior, A., Pankanti, S., Hampapur, A., Brown, L., Tian, Y.L., Ekin, A., et al. Enabling video privacy through computer vision. IEEE Security & Privacy. 2005 Jun;3(3):50– 57.
15. Chaudhari, J., Cheung, S. S., Venkatesh, M.V. Privacy Protection for Life-log Video. In: IEEE Workshop on Signal Processing Applications for Public Security and Forensics, 2007. SAFE '07. IET; 2007. p. 1–5.
16. Makino, Y., Murao, M., Maeno, T. Life log system based on tactile sound. In *Proc.* Haptics 2010. Springer-Verlag; 2010. p. 292–297.