MIT Libraries | DSpace@MIT

MIT Open Access Articles

Dynamic privacy management in pervasive sensor networks

The MIT Faculty has made this article openly available. ***Please share*** how this access benefits you. Your story matters.

Citation: Gong, Nan-Wei, Mathew Laibowitz, and Joseph A. Paradiso. "Dynamic Privacy Management in Pervasive Sensor Networks." Ambient Intelligence. Ed. Boris Ruyter et al. Vol. 6439. Berlin : Springer Berlin Heidelberg, 2010. 96-106. (Lecture notes in computer science ; 6439)

As Published: http://dx.doi.org/10.1007/978-3-642-16917-5_10

Publisher: Springer Science + Business Media B.V.

Persistent URL: http://hdl.handle.net/1721.1/66150

Version: Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

Terms of use: Creative Commons Attribution-Noncommercial-Share Alike 3.0

Massachusetts Institute of Technology

Dynamic Privacy Management in Pervasive Sensor Networks

Nan-Wei Gong, Mathew Laibowitz, Joseph A. Paradiso
Responsive Environments Group, MIT Media Laboratory
E14-548, 75 Amherst Street, Cambridge 02142, USA
{nanwei, mat, joep}@media.mit.edu

Abstract. This paper describes the design and implementation of a dynamic privacy management system aimed at enabling tangible privacy control and feedback in a pervasive sensor network. Our work began with the development of a potentially invasive sensor network (with high resolution video, audio, and motion tracking capabilities) featuring different interactive applications that created incentive for accepting this network as an extension of people's daily social space. A user study was then conducted to evaluate several privacy management approaches – an active badge system for both online and on-site control, on/off power switches for physically disabling the hardware, and touch screen input control. Results from a user study indicated that an active badge for on-site privacy control is the most preferable method among all provided options. We present a set of results that yield insight into the privacy/benefit tradeoff from various sensing capabilities in pervasive sensor networks and how privacy settings and user behavior relate in these environments.

Keywords: dynamic privacy management, ubiquitous computing, active badge system, pervasive sensor networks.

1 Introduction

As we move into the era of Ambient Intelligence, we will see a shift in how people interact with information. Just as we are now noting users evolve into often using mobile devices instead of desktops and laptops, we will see a shift into everywhere interaction with pervasive smart environments when sensing, actuation, and display are embedded ubiquitously into our surroundings, and our digital "cloud" manifests on whatever devices and information portals are available and appropriate. The user interface to this environment will accordingly also be abstracted into a ubiquitous sensor network that acts as the perceptive "nervous system" of ambient intelligence. The sea of sensors that surround us are already mushrooming, as we bring more and more sensing into our presence on the back of devices we acquire for specific services. Once common standards enable applications to share sensor data across devices, we will see an explosion of development similar to what happened when the Web united networked servers and PCs. It's vital, however, that before we reach this point, the sensors rushing into in our lives respond intrinsically to our dynamic desires for privacy [1,2] – there will just be too many to manually turn off or disable. Accordingly, this paper relates a set of studies that we have run at our laboratory to determine how users accommodate such a large pervasive multimodal sensor/display network and gain insight into how their behavior adapts to a set of dynamic privacy protocols that we have developed.

We began the study of privacy in ubiquitous interactive sensor networks with the installation of 45 "Ubiquitous Media Portals" (UMPs) in our building. This potentially invasive sensor network is equipped with high-resolution video, audio and motion tracking capabilities. The UMPs ran several applications [2-4] to engage users

IPR2025-01308; Samsung
Ex. 1015 - Page 2

to interact with those sensing affordances. The video and audio captured by each sensor node can be streamed between different nodes for image sharing and message broadcasting, as well as to online platforms such as Second Life for ubiquitous virtual-reality applications [3]. We also developed several wearable sensors that augment this network with on-body sensing to assemble meaningful content, such as a user-generated documentary video [4-5]. The displays on each UMP can show information of general interest, such as the latest RSS feeds. They also allow users to capture and share images or text messages that are broadcast to all the other nodes throughout the building. During an 8-month pilot study before we constructed the privacy management system, we implemented four different applications to explore acceptance by our building-wide users. The results verified that applications allowing sufficient, transparent interaction and providing generally useful information are effective ways to increase the percentage of nodes remaining active without being physically disabled by our users [2]. Learning from this experience, we subsequently built a dynamic privacy management system on the UMPs. Our privacy system consisted of two parts: onsite privacy control (with beacons from active wearable devices, physical switches, and touch screen inputs) and remote privacy settings (via web browsers for setting pre-established privacy preferences).

1.1 Previous Work

Privacy Protocol Design. Substantial research has been devoted to design strategies and policies for privacy issues in ubiquitous computing environments. The major approach for controlling privacy status within sensor networks is through constructing secure protocols and code verification mechanisms for system developers to follow and examine as they deploy the infrastructure for data acquisition and post data processing. Bellotti and Sellen were pioneers with their work on privacy in the context of ambient video based on the experience of the RAVE media space at EuroPARC. They first proposed a privacy-protected framework in 1993 [6] for designing ubiquitous computing environments and described the ideal state of affairs with respect to each of four types of behavior – Capture, Construction, Accessibility and Purposes. Their argument is that providing obvious "feedback and control" over information in a ubiquitous computing environment can help assuage privacy concerns (Sellen and colleagues have recently demonstrated a system of networked cameras and pen-enabled displays for interhousehold interaction in Microsoft's Wayve system [7]). Drawing upon their work, many toolkits have been developed to provide programming support and abstractions for protecting privacy in a ubiquitous computing environment such as Confab [8] and Mist [9].

Context-Aware Systems. Researchers have explored protecting privacy through pseudonyms, dummy users, and storing privacy information as a watermark to blur users' information, especially location-specific data, in computer vision [10-12, 13]. Recently, research into privacy protection in context-aware pervasive systems has advanced to the design of self-configuring privacy management infrastructures. Ortmann et al. proposed a self-configuring privacy management architecture for pervasive systems [14]. Further, Moncrieff and coworkers [15] presented a dynamic method for altering the level of privacy in the environment based on inferred context and local situation. Beyond research on dynamic privacy configuration that exploits fixed sensor infrastructure, the concept of automatically inferring mobile privacy settings is also explored through monitoring the use of personal electronic devices such as cell phones [16-17]. All of the above examples demonstrate the idea of creating a smarter and sophisticated system that could better suit users' needs of privacy within their environment. However, without direct user control, the construction of an ideal system that can suit everyone's needs is almost impossible.

IPR2025-01308; Samsung
Ex. 1015 - Page 3

Sensing Type and Location Control. Another major method for improving the design of privacy protection in sensor networks is through the physical approach — the privacy-concious choice of sensors and location/direction of sensing elements. In [18], Reynolds and Wren examined the ethical implications of choosing camera networks vs. infrared motion detector networks. Their results indicate that for most participants, infrared sensors were significantly less invasive than pan-tilt-zoom cameras. This comes at the cost, however, of not implanting sensors that can facilitate more complex applications. Although it has been proven that data collected from motion sensing can indirectly lead to approximate personnel identification and localization [19], the coarse level of interaction provided by a motion sensor network still can not yield all functions increasingly desired in evolving ubiquitous networks. Therefore, we try not to compromise our sensor system design, but rather to control the quality of the data provided according to the dynamic privacy level requested by the users' privacy management settings.

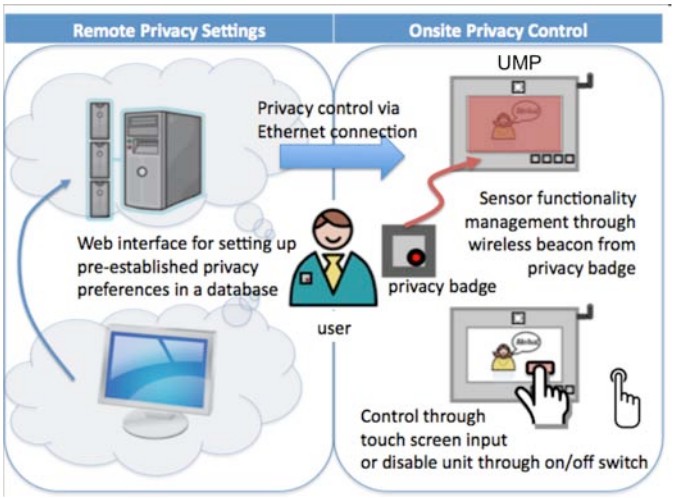


Fig. 2.1. System block diagram.

2 Design and Implementation

The goal of our system is to construct a user-centric privacy management system for ubiquitous computing and use it to obtain real-world experience with a potentially invasive pervasive sensor network. There are two major parts in our privacy management system – onsite privacy control and remote privacy settings (Fig 2.1).

Our sensor network can communicate with the wearable privacy badges through a building-wide 802.15.4 ZigBee radio network allowing the badges to change the sensing parameters onsite, i.e., turn on or off different sensors according to the settings prespecified by each individual badge user (Sec. 2.2). Also, local users can physically disable the sensing units through touch screen inputs or an on/off power switch.

On the other hand, users can set up their privacy preference online from a web interface by setting the allowable sensor modalities that can stream from each node when they are nearby . Their privacy level can also be dependent on the group status of the client browsing the sensor network—the badge user can assign different levels of privacy to different groups of people (e.g. taking an analogy to UNIX file system permission: "user/group/world"), i.e., individuals who are socially closer to the user

IPR2025-01308; Samsung
Ex. 1015 - Page 4

can be allowed to have more access. Physical means of providing immediate privacy are also afforded (e.g., physically obstructing the sensors and turning the obviously-located power switch off).

2.1 Active Privacy Badges and Ubiquitous Media Portals

In order to provide active control, we designed and implemented active privacy badges for the UMPs and demonstrated the possibility of integrating the wearable electronics into everyday accessories. Fig 2.2(a) shows the badge we used for our user study. This simple wearable sensor has 4 LED indicators to display users' dynamic personal privacy settings, a blocking button for requesting immediate privacy, and a vibration motor to alert upon unexpected events, such as a user's privacy setting being over-written by another nearby user with high priority. It communicates with our UMP sensor network using 802.15.4, through which we have attained room-level RF location accuracy, which is sufficient to disable any UMPs that are in sensing range of the badge wearer. Subsequent badges that we have developed for other projects have added a small display (Fig 2.2(b) [7,8]) that can alert people near the user to their privacy level or data streaming status.

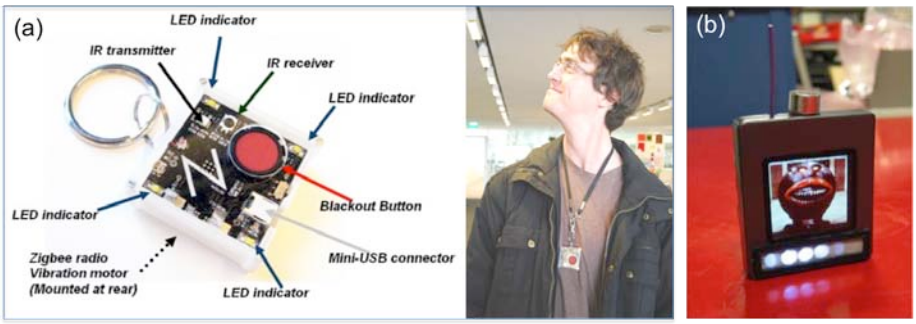


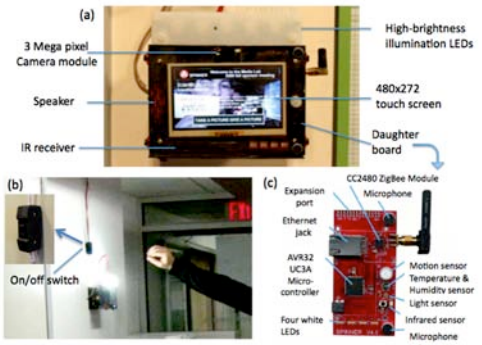
Fig. 2.2. (a) Privacy Badge – diagram and worn. (b) Subsequent badge featuring OLED display

The need for a privacy system was inspired by our pervasively-deployed multimodal sensor and display Ubiquitous Media Portal (UMP, see figure 2.3) network. The 45 UMPs that we built comprise a sensor network that was distributed throughout the Media Lab. Each UMP, mounted on a pan/tilt platform, has an array of sensors, as well as audio and video capabilities (see Figure 2.3 for the list of features). Video and images are acquired with a 3 MegaPixel camera above a touch screen display. The video board is driven by a TI DaVinci processor (an ARM9 running Linux paired with a C64x+ DSP core for video processing), and features a touch-screen LCD display, LED floodlight, & speaker. The sensors and an 802.15.4 radio that talks to and tracks wearable sensors are mounted on a daughter card, which runs an AVR32 microcomputer (AV32UC3A1256) and features stereo microphones, PIR motion sensor, humidity/temperature sensor, light sensor, and 2 protocols of IR communication (for detecting active badges within the line of sight) [7].

2.2 Data Server and Web Interface

For personalized remote privacy control, users can register on the web interface with their unique badge ID and edit their privacy preferences on each node. Although the work by Beresford and Stajano [13] indicated that in a restricted space, pseudonymous ID could be cracked by the location information of each badge, our active badge can disable forwarding of tracking information by proximate UMPs if the user wants to remain anonymous.

IPR2025-01308; Samsung
Ex. 1015 - Page 5



Sensors	I/O Channels
3M pixel auto focus camera with pan and tilt control and 5 Watt LED illuminator	480x272 LCD touch screen
Stereo microphones	Speaker
Passive Infrared Sensor	4 LEDs for status report
Temperature and humidity sensor (SHT15)	Zigbee 802.15.4 transceiver
Light sensor	IR communication

Fig. 2.3. Left: (a) Overview of a UMP node and one example application ("Cloud of Images") showing RSS feeds and the last captured image. (b) UMP, in action illuminating subject for video capture, and switch for manually deactivating UMP's power. (c) Sensor daughter board. Right: List of features in the sensing system.

Users can edit privacy/sensor preferences on a location basis via a web form. For example, in Fig 2.4, the user is editing the behavior of node 311 and turning off the video recording when they are present at this location. An "edit all sensors" page was also provided to specify globally common settings. Results from how people use this page can give us insight into how our system is perceived [20] – e.g., whether specific locations or the nature of different sensors is the greatest privacy threat for most people. In all of our experiments, the default setting for all sensors was on (making an opt-out system).

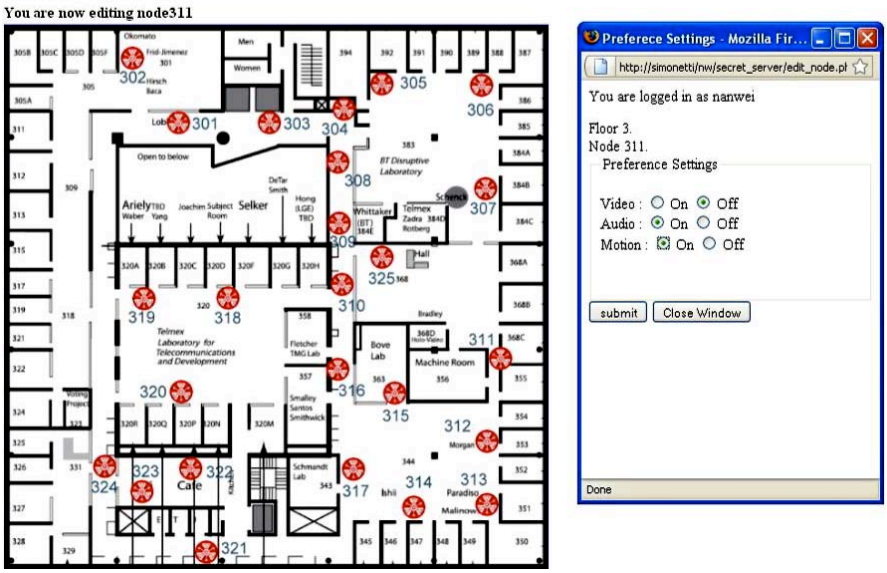


Fig. 2.4. The "edit sensor" page allows users to click on each node on an interactive map and edit sensor settings on a location basis.

One of the most important aspects about users' privacy protection in a ubiquitous computing sensor network is having the ability to post-process our personal

IPR2025-01308; Samsung
Ex. 1015 - Page 6

information flow. While our system has the ability to collect video, audio and images and display that information recorded for each user individually, it could also be tailored to share users' information with others. In the edit group permission page, the users are allowed to reveal their information according to social hierarchy -- user / group / world, like a UNIX file permission system (e.g. family, friends, and world in real life). Further, users are able to create their own group and send out invitations for other users to join their group. This framework can not only allow the users to customize how they appear to who is looking, but also can be used as a social networking tool similar to Google Tracker, which let you follow your friends' or families' locations and show ubiquitously-collected images or videos in real-time.

3 Evaluation

We conducted several user studies to gain insight into dynamic privacy management. The first study included four different applications with different levels of control and interaction on the users' end. Users coulld enable or disable the UMPs with the physical power switch onsite. Our results, collected across an 8-month study, indicate that applications allowing sufficient, transparent interaction and providing generally useful information are effective ways to increase the percentage of nodes remaining on. Detailed application and statistics information can be found in [3]. With this experience, we conducted another user study that featured our active badge system. Users had three different ways to disable sensor streaming— disabling UMPs by cutting their power, using the privacy badge's "NO" button to immediately block data transmission, and modifying their online settings to automatically disable sensor streaming at specific locations when nearby. The on/off switch will kill the entire UMP until it is powered/booted again and rejoins the system (taking many minutes), while the privacy button and the online preset behavior only disable the UMPs temporarily. In these tests, the default blackout time instigated by the privacy button is 10 seconds, which is approximately the typical time needed to walk by a UMP node or sufficient time to blank minimal personal identifying information during a conversation.

Twenty-four people (out of 90 people working on the same floor where all portals were installed) volunteered to participate in this weeklong study. The recruitment requirements [20] include selecting people whose offices are located near the UMPs and obtaining a diverse group of people, including students, staff and faculty members in our building (65% had engineering/science background – the remainder had background in arts, humanities, or other expertise). All were well aware of the privacy threats that our system posed, and knew that video/audio could be streamed from each portal.

3.1 User Study Results

Results from Active Badge Usage. Fig. 3.1 (left) shows the normalized distribution of on-site "NO" button presses versus time. The users generally press the NO button on their badge when there is a conflict between the location-specified privacy of their online settings and the location of an unexpected private event, or when unquestioned privacy is immediately needed. During our one-week user study, the average number of button presses per day was 71; 3 button presses per user per day. The peak correlates with afternoon break / lunch (2-3 PM) with broad tail late into the afternoon when more social interaction is typically exercised and users tend to desire more confidentiality.

IPR2025-01308; Samsung
Ex. 1015 - Page 7

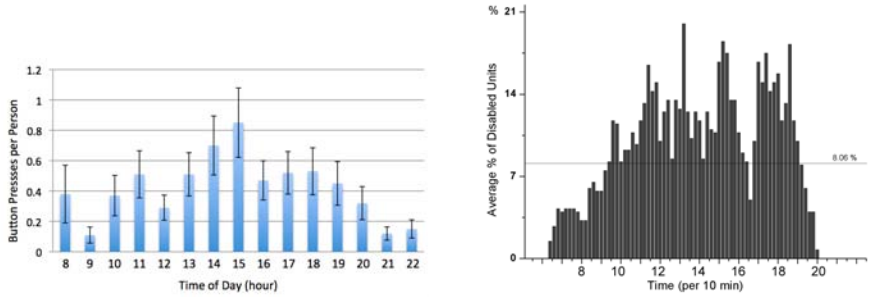


Fig. 3.1. Left: Ratio of NO button presses per the number of users (error bars are derived from the number of people per bin). Right: Normalized histogram of disabled UMPs over time (the average fraction of disabled UMPs is 8%)

Although we built the active badge system to solve the privacy issue for dynamic situations, gaining a balance between maintaining the full function of a ubiquitous interactive sensor network while preserving users' privacy in every way is still an unsolved issue. Figure 3.1 (right) shows the average fraction of disabled UMP units from both button presses and automatic shuttering (determined by user proximity to the UMP and their web-assigned preferences) per 10-minute interval. We see up to 20% of the units disabled by privacy requests at peak social intervals.

Results from Users' Online Settings. From the web database, we observed that 70 percent of participants set up their privacy preferences online and 66 percent of all participants chose to block all video transmission through active badge proximity (50 percent set all audio off), whereas only 34 percent set all motion sensors off. As for the privacy settings on individual nodes, 50 percent of all participants set up individual privacy on a location basis. On their daily route, 33 percent turned off the video recording/broadcasting, another 17 percent disabled both video and audio, but merely 4 percent disabled the motion sensors. The remaining 8 percent did not set up preferences from this page, and just used their on-badge button.

Figure 3.2 explores the relationship between different privacy management methods versus the location of individual UMP units. This plot is segmented according to the location of each UMP. Nodes in group A are in the corners and hallways where people pass by, generally with less social interaction. These nodes are on most of our users' routing path; however, less people set up intrinsic privacy control there online. Group B are nodes in common areas such as our café and kitchen, where most social interactions take place – accordingly, these places encountered both significant online scripted blocking and spontaneous button presses. The last group, C, are nodes located in office clusters and around intersections between different paths. Fewer users marked those places as high privacy risks online, but lots of unexpected private events happened as we can see from the high percentage of privacy button presses.

Results from Questionnaire and Interview. After the evaluation period, each user was asked to complete a post-experiment questionnaire that asked about the usability of this system and the acceptance of each privacy protection method. When users were asked about which approaches could better suit their need for privacy control, 40% answered "online privacy settings", 33% answered "on-site badge control" and another 19% and 8% answered "button on the touch screen" and "cutoff switch" respectively.

We also interviewed the users and ask them to list the scenarios in which they used the active badge system for privacy incidents. 75 percent of users listed "to block

IPR2025-01308; Samsung
Ex. 1015 - Page 8

audio recording from an unexpected private conversation"; 50 percent listed "to block the video recording". One interesting finding is that, among the users who listed "video blocking" as one of their rationales, some mentioned that they prefer not to be recorded when they are alone in a public area, such as in front of the elevator or in the kitchen. This result supports the idea that privacy is a dynamic factor and cannot be generalized easily.

Also, 21 percent indicated that they pressed the NO button to block location tracking occasionally. Though it is possible to block all sensor data collection, many people decided to keep the motion/location tracking on and block the more invasive signals via the privacy badge – these people tried to create a participatory "location presence" in front of their colleagues. On the other hand, 12.5 percent of users never used the badge and commented that they didn't care about being recorded or tracked in their workspace. This indicated that it is impossible to define a standard privacy scenario. Only a personalized system with dynamic controlling capabilities can provide a privacy-enhanced ubiquitous media environment. Our active badge system satisfied this for most of our users.

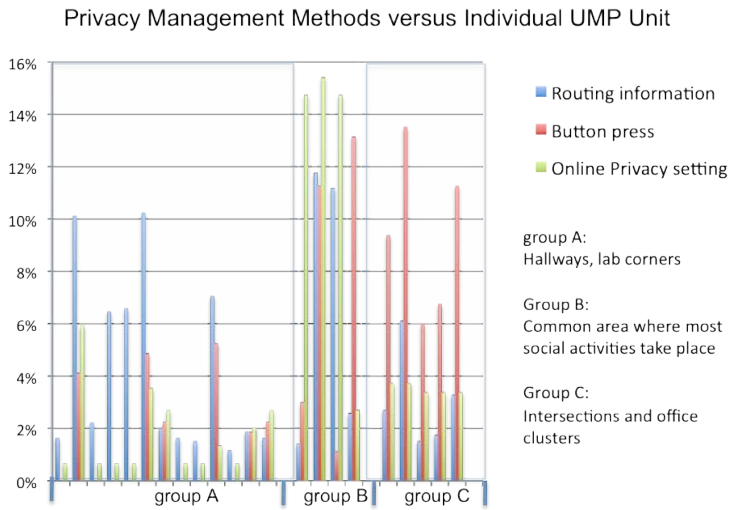


Fig. 3.2. Relationship between privacy management methods versus individual UMP location. The "Routing Information" shows how much of the user's specified daily route through the buiding passes near that portal – "Button Presses" are the recorded NO events at that location, and the last quantity shows the percentage of people who chose online to disable that portal when they were nearby.

4 Conclusions and Future Work

In this paper, we presented multiple approaches for personal privacy management in ubiquitous sensor networks. The major contribution to privacy research in ubiquitous computing environments is providing a user-centric privacy-protected platform and obtaining experiences with the deployment of a potentially invasive sensor network.

We have evaluated the usability of an active privacy badge system and the possibility of using this system as a building-wide privacy protection facility. Our results indicated that an active badge system for privacy control is the most acceptable method among all the tested options (disabling data transmission from an active badge system, on/off switches, or the touch screen displays). The results from these tests also suggested that if occupants of moderately denser buildings block data

IPR2025-01308; Samsung
Ex. 1015 - Page 9

transmission in their vicinity at the rates we see now, the availability of the sensor network will be compromised. Therefore, it is crucial to find a balance between protecting privacy and maintaining enough data flow for the value-added applications utilizing the network at the same time. Ongoing research by various teams (e.g., [21]) is exploring ways of removing particular individuals from audio/video and sensor streams when privacy is desired, maintaining network function. Our future work will explore this avenue, as well as integrating our privacy badge functionality into commodity cell phones and common short-range radio standards like Bluetooth.

This project focused more on interfaces for privacy management and control rather than network security – the protocols and systems that we used were minimally secured, which wouldn't be permissible in an actual deployment. For this type of system to be really used, trusted, and ultimately accepted, communication protocols, software, and hardware need to be implemented that are secure and resistant to attack [22] so that security and privacy can be certifiably protected according to individual choice. More detailed information is available, including all the collected data, higher resolution images, source code, and schematics, in the associated graduate thesis [20].

4 Acknowledgments

We thank our colleagues at the Media Laboratory who participated in the user study and the deployment of this system, especially Bo Morgan for developing the SPINNERD server. This work was supported by the Things That Think Consortium and the other research sponsors of the MIT Media Laboratory.

References

1. Davies, N. and Gellersen, H.-W., "Beyond Prototypes: Challenges in Deploying Ubiquitous Systems," *IEEE Pervasive Computing*, January–March, vol. 1, no.1, (2002), 26–35.
2. Gong, N-W., Laibowitz, M., Paradiso, J. A.: "Experiences and Challenges in Deploying Potentially Invasive Sensor Systems for Ubiquitous VR Applications," *Cloud-Mobile Convergence for Virtual Reality Workshop (CMCVR 2010),* Waltham MA, March 20, 2010.
3. Lifton, J., Laibowitz, M., Harry, D., Gong, N.W., Mittal, M. and Paradiso, J. A., "Metaphor and Manifestation – Cross Reality with Ubiquitous Sensor/Actuator Networks," *IEEE Pervasive Computing Magazine*, July-September, vol. 8, no. 3 (2009), 24-33.
4. Laibowitz, M., Gong, N-W., Paradiso, J.A., "Wearable sensing for dynamic management of dense ubiquitous media," in *Proceedings of 6th international workshop on wearable and implantable body sensor networks (BSN 09)*, Berkeley, CA, June 3-9, 2009, pp. 3–8.
5. Laibowitz, M., Gong, N-W., Paradiso, J.A., "Multimedia Content Creation using Societal-Scale Ubiquitous Camera Networks and Human-Centric Wearable Sensing," in *Proc. of ACM Multimedia 2010*, Florence Italy, October 25-29, 2010.
6. Bellotti, V. and Sellen, A., "Design for privacy in ubiquitous computing environments," In *Proceedings of the 3rd European Conference on Computer-Supported Cooperative Work (ECSCW'93)*. Kluwer Academic Publishers, Norwell, MA, (1993), pp. 77-92.
7. S.E. Lindley, R. Harper, and A. Sellen, "Design of a Technological Playground: A Field Study of the Emergence of Play in Household Messaging," *Proc. of CHI 2010*, Atlanta GA, April 10-15, 2010, pp. 2351-2360.
8. Hong, J. I. and Landay, J. A., An Architecture for Privacy-Sensitive Ubiquitous Computing," in *Proceedings of MobiSys 04*, Boston MA, June 6-9, 2004, pp. 177-189.
9. Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane1, G., and Mickunas, M. D., "Towards security and privacy for pervasive computing," in *Proceedings of International Symposium on Software Security*, Tokyo, Japan, November 8-10, 2002, pp. 1-15.
10. Zhang, W., Cheung, S.-C. S., and Chen, M., "Hiding privacy information in video surveillance system," in *Proc. of ICIP '05*, Genova, Italy, September, 11-14, 2005, Vol. II, pp. 868–871.

IPR2025-01308; Samsung
Ex. 1015 - Page 10

11. Schiff, J., Meingast, M., Mulligan, D., Sastry, S. and Goldberg, K., "Respectful cameras: Detecting visual markers in real-time to address privacy concerns," In *International Conference on Intelligent Robots and Systems (IROS)*, Oct. 29-Nov. 2, 2007, pp. 971 - 978.

12. Kindberg, T., Fox, A., "System Software for Ubiquitous Computing," *IEEE Pervasive Computing*, January–March, Vol. 1, No. 1 (2002), 70-81.

13. Beresford, A. and F. Stajano, "Location Privacy in Pervasive Computing," *IEEE Pervasive Computing*, Vol. 2, No. 1 (2003), 46-55.

14. Ortmann, S., Langendörfer, P., Maaser, M., "A Self-Configuring Privacy Management Architecture for Pervasive Systems," in Proc. of the *5-th ACM International Workshop on Mobility Management and Wireless Access (MOBIWAC)*, Chania, Crete Island, Greece, October 22, 2007, pp. 184 - 187.

15. Moncrieff, S., Venkatesh, S., Andwest, G., "Dynamic privacy in a smart house Environment," in *Proceedings of the IEEE International Conference on Multimedia and Expo*, IEEE Computer Society, July 2-5 2007, pp. 2034-2037.

16. Gisch, M., De Luca, A., Blanchebarbe, M., "The Privacy Badge - A Privacy-Awareness User Interface for Small Devices," in *ACM International Conference On Mobile Technology, Applications, And Systems*, Singapore, September 10-12, 2007, pp. 583-586.

17. Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., Rao, J., "Understanding and capturing people's privacy policies in a mobile social networking application," *Personal and Ubiquitous Computing*, Vol.13 No.6 August 2009, pp. 401-412.

18. Reynolds, C. J. and Wren, C. R., "Worse is better for ambient sensing," *Workshop on Privacy Trust and Identity Issues for Ambient Intelligence (Pervasive 2006)*, Technical Report TR2006-005, Mitsubishi Electric Research Laboratories (MERL), May 2006.

19. Beresford, A.R. and Stajano, F., "Location Privacy in Pervasive Computing," *IEEE Pervasive Computing*, Vol. 2, No. 1, Jan.-Mar. (2003), pp. 46-55.

20. Gong, N-W., *Configurable Dynamic Privacy for Pervasive Sensor Networks*, MS thesis, MIT Media Laboratory, 2009.

21. J. Wickramasuriya, M. Alhazzazi, M. Datt, S. Mehrotra and N. Venkatasubramanian: "Privacy-Protecting Video Surveillance," in *Proc. of the SPIE International Symposium on Electronic Imaging (Real-Time Imaging IX)*, San Jose, CA, February 25, 2005, pp. 64-75.

22. Stajano, F., *Security for Ubiquitous Computing*, John Wiley and Sons, New York, 2002.

IPR2025-01308; Samsung
Ex. 1015 - Page 11