The Design of a Context-Aware Home Media Space for Balancing Privacy and Awareness

Carman Neustaedter and Saul Greenberg

University of Calgary
Department of Computer Science
Calgary, AB, T2N 1N4 Canada
[carman *or* saul]@cpsc.ucalgary.ca

Abstract. Traditional techniques for balancing privacy and awareness in video media spaces, like *blur filtration,* have been proven to be ineffective for compromising home situations involving a media space. As such, this paper presents the rationale and prototype design of a context-aware *home media space (HMS)*—defined as an always-on video media space used within a home setting—that focuses on identifying plausible solutions for balancing privacy and awareness in compromising home situations. In the HMS design, users are provided with *implicit* and *explicit control* over their privacy, along with *visual* and *audio feedback* of the amount of privacy currently being maintained.

1 Introduction

A *home media space* (HMS) is an always-on video-based media space used within a home setting. It is designed specifically for the telecommuter who chooses to work at home, but who still wishes to maintain a close-working relationship with particular colleagues in remote office environments. Like all media spaces, the video provides the telecommuter with awareness information about their collaborator's availability for conversation, and a way to easily move into casual communication over the same channel. Unlike office-based media spaces, a home media space has to pay considerably more attention to how the system appropriately balances privacy and awareness, because privacy concerns are far more problematic for home users.

In this paper, we describe the rationale and prototype design of our own context-aware home media space. Specifically, we detail how and why:

1. existing privacy mechanisms are leveraged for use in home-based video conferencing systems;
2. implicit actions using context-aware technology can regulate privacy;
3. no implicit action will ever decrease the amount of privacy without first warning the user and providing the opportunity to stop the operation;
4. explicit actions using dedicated physical controls and gesture recognition can regulate privacy; and,

5. visual and audio feedback makes the state of the system easily discernable at any time.

We begin by briefly describing our motivation: casual interaction and informal awareness. Next, we outline the privacy concerns that can arise from telecommuting, and how previous work suggests that context-aware computing offers solutions for balancing privacy and awareness in a HMS. Finally, we discuss the rationale and design of our context-aware HMS and the privacy-protecting strategies it offers.

2 Casual Interaction *vs.* Privacy in Home Telecommuting

To set the scene, this section briefly summarizes the importance of casual interaction and awareness. We describe how video-based media spaces can provide rich awareness for distance-separated telecommuters, but at the expense of privacy violations.

2.1 Casual interaction, awareness, and media spaces

Throughout a typical day, co-workers naturally interact amongst each other in what is known as c*asual interaction:* the frequent and informal encounters that either occur serendipitously or are initiated by one person [11, 16]. These interactions have been shown to foster knowledge and help individuals accomplish both individual and group work [11, 18]. Casual interaction is held together by i*nformal awareness*: an understanding of who is around and available for interaction. It is this awareness that helps people decide if and when to smoothly move into and out of conversation and collaboration [18]. Informal awareness is easily gained when people are in close physical proximity, but deteriorates over distance [13, 18]. As a result, casual interaction suffers when co-workers are distributed.

One possible solution for providing awareness between distance-separated collaborators is the *media space*: an always-on video link that connects remote locations [4, 6, 10, 11, 13, 14, 19, 20, 23]. Its advantage is that the always-on video channel can provide rich awareness in a manner that is easily understood by individuals. In practice, video media spaces have found some limited success in office situations, albeit primarily at research laboratories (e.g., 11, 17, 20). The problem is that these media spaces also broadcast information that individuals may consider to be privacy sensitive [5, 6, 7, 14, 16].

In an effort to help mitigate privacy concerns over video links, researchers have studied many techniques, with one of the most popular being *distortion filters:* algorithmic reduction of image fidelity that hides sensitive details in a video image while still providing awareness [7, 14, 16, 21, 25]. Distortion filters have proven successful at balancing privacy and awareness for mundane and benign office situations, e.g., people working or reading, people chatting, people eating lunch [7].

In spite of this (and other) research, most media space installations simply ignore privacy issues. There may be several reasons for this: risks are fairly low in office settings; installations are between close colleagues or early adopters; and simple pri-

vacy safeguards often suffice, e.g., people can explicitly switch off the video channel, or turn the camera around to face the wall.

2.2 Privacy in home-based media spaces

With the declining cost of PC cameras and several companies offering free video conferencing software (e.g., Webcam for MSN Messenger, Yahoo! Messenger), video is increasingly being used in the home. Its prevalence is indicated by the growing number of live webcam sites on the Internet.

Privacy concerns become complicated when people choose to work from home as telecommuters, while still desiring close contact with colleagues at work. The big problem is that privacy risks increase drastically for the telecommuter (compared to the office worker), as well as for others in the home. Privacy threats increase for several reasons:

- ***The home is inherently private in nature.*** Normally people are more relaxed at home and able to deviate from social customs [1]. This makes it easier for people to do unconscious acts such as picking one's nose, scratching one's rear, or other potentially embarrassing actions that can be inadvertently captured by the camera.

- ***The telecommuter lives a dual role as worker and home occupant.*** Appearances and behaviours that are appropriate for the home may not be appropriate when viewed at the office. For example, it is appropriate for a telecommuter to work at home shirtless or in pajamas, yet the same level of dress may not be appropriate when seen at the office and may violate the telecommuter's privacy.

- ***The dual purposes typical of most home offices.*** The home office may also be a corner of a living room, or a spare bedroom. Unknowingly, home occupants may be caught on camera in precarious situations as a result. For example, a house guest may be using the home office/spare bedroom in the evening when the camera accidentally captures her changing clothes (because the 'owner' may have forgotten to either warn the guest or turn off the camera).

- ***Threat/benefit disparity.*** Individuals in the home who may gain little or no benefit from the HMS still incur its privacy threat. For example, a spouse who does not want to be captured on camera may be recorded just by simply entering the home office. This situation could be quite privacy-sensitive if (say) the spouse came in to the home office to kiss his or her mate!

These increased privacy risks suggest that home media space systems must incorporate techniques that somehow mitigate privacy concerns. Of course, one possibility is to simply adapt techniques already proposed for office media spaces. Unfortunately, most have not been tested for 'high risk' situations such as those arising in the home. Consequently, as motivating work for our current research, we evaluated *blur*

filtration—a distortion technique that produces a blurred video image—for its effectiveness in balancing privacy and awareness for compromising home situations [21].

In our study, people were shown video scenes ranging from little risk to extreme risk. Each scene was first shown extremely blurred, with subsequent showings less blurred until eventually the scene was shown in full fidelity. We looked for the thresholds at which people could just extract awareness information from the scene, and also the thresholds at which people would judge as violating privacy. The results clearly showed that blur filtration is not able to balance privacy and awareness for risky home situations, i.e., the blur level that let people garner just enough information to judge someone's availability was above what people felt was 'safe' to show others. Our study also showed that as privacy risk increases, people begin to abandon filtration as a strategy for preserving privacy and choose to simply turn off the camera. As well, people preferred direct control of their privacy, e.g., being able to position the camera, control the blur level, turn the camera on/off, and so on.

3 The Design Philosophy of our Context-Aware HMS

This section outlines the five principles behind the design of our context-aware HMS. First, we provide background knowledge of social psychological theories of privacy mechanisms. Second, we use this knowledge to explain each of our design principles and why they are included in our design philosophy. Third, to set the scene of our design, we describe the design elements that arose from our five principles.

3.1 Design Principles for a Context-Aware HMS

The results of our study on blur filtration [21] highlighted the importance of providing user control over information conveyed through a video media space. To provide natural mechanisms for users to control this information, we began investigating how humans regulate privacy in everyday life through various behaviours and actions called *privacy mechanisms* [2]. We will use the terms "privacy mechanisms" and "privacy-protecting strategies" interchangeably for the remainder of this paper. Each and every culture has used privacy mechanisms to regulate interaction with others [2]. When individuals require more privacy, they use these mechanisms to let others know they desire less interaction. Just the same, when individuals require more interaction, they use these mechanisms to let others know they desire less privacy. These privacy mechanisms are very natural and often form an unconscious act [1]. The privacy mechanisms used by humans can be classified into four categories [1]:

1. ***Verbal behaviours**:* the use of the content and structure of what is being said;
2. ***Non-verbal behaviours**:* the use of body language, e.g., gestures and posture;
3. ***Environmental mechanisms**:* the use of physical artifacts and features of an environment, e.g., walls, doors, spatial proximity, timing; and,
4. ***Cultural mechanisms**:* the use of cultural practices and social customs.

Research has shown that different cultures employ mechanisms from different categories [2]. Western culture typically relies on environmental mechanisms (e.g., the physical architecture of our homes), whereas other communal cultures rely more on cultural mechanisms (e.g., when and where people gather in a house).

Based on this research, we believe the design of a HMS should use the following design principles:

1. existing privacy mechanisms should be leveraged for home-based video conferencing systems;
2. implicit actions using context-aware technology can regulate privacy;
3. no implicit action should ever decrease the amount of privacy without first warning the user and providing the opportunity to stop the operation;
4. explicit actions using dedicated physical controls and gesture recognition can regulate privacy; and,
5. visual and audio feedback makes the state of the system easily discernable at any time.

The first principle helps to create privacy mechanisms for a HMS that are both easy to understand and natural to use because they are based on techniques already familiar to humans. Our design supports this principle by providing users with privacy-protecting strategies from the same four categories used by humans in everyday life (discussed in more detail later).

Privacy regulation in real life is lightweight and often transparent. Such implications should also be available to HMS users. Thus, as the second principle states, privacy-protecting strategies in a HMS should also be lightweight and transparent. Our design supports this principle by using context-aware computing as a tool for balancing privacy and awareness through implicit means. Unlike previous work in context-aware computing [22, 24], we enable one specific location—a home office/spare bedroom—with technology that senses who is around and then infers privacy expectations through a simple set of rules.

There is still a considerable gap between human expectations and the abilities of context-aware systems [9]. Context-aware systems can make mistakes and it is important that these mistakes do not increase privacy threat; the third design principle addresses this problem. Our design supports this principle by first warning users that an implicit action has initiated a privacy decreasing operation; and second, by providing an opportunity for users to override this operation.

The fourth principle also addresses the previously mentioned problem by recognizing that we need to keep the user in the "control loop." Our design supports this principle by providing users with dedicated physical and graphical controls, where explicit actions such as adjusting a physical slider or gesturing towards the camera will alter the privacy level. We recognize that explicit control must absolutely be lightweight and executed with almost trivial effort.

The fifth principle is important because users must be able to fine tune the privacy/awareness balance as desired. To do this fine tuning, they must know how much privacy is currently being maintained. Our design supports this principle by providing feedback of the achieved privacy level through audio and visual cues, ren-

dered on both physical displays (such as LEDs) and on the screen. This feedback is both understandable and continually available.

3.2 Elements of a Context-Aware HMS

To foreshadow the details of our design, this section outlines the elements of our HMS that arise from the five design principles. The subsequent section describes their importance by outlining how they work together to regulate privacy.

Figure 1 shows the HMS's graphical user interface (GUI) as seen by the telecommuter: the top window shows a mirrored image of the telecommuter as it is captured, and the bottom window shows the telecommuter's colleague. A third window contains additional options (Figure 2) and is displayed by clicking the configuration button in the telecommuter's toolbar (Figure 1, top, fourth button from the left). The other graphical controls are described below. Figures 3 and 4 show the layout of the HMS in the home office/spare bedroom of a telecommuter. The design is specific to this room layout, but the ideas presented can be applied to a variety of home settings.

Fig. 1. The HMS GUI: the telecommuter (top) and colleague (bottom).

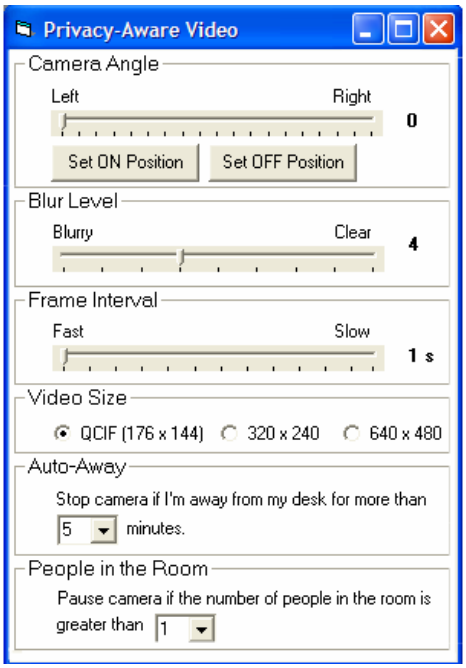

Fig. 2. A configuration window to adjust various HMS attributes.

Fig. 3. The layout of the HMS within the home office/spare bedroom.

We support the five HMS design principles, discussed previously, by including specific elements within our design:

Camera state. The camera can be in one of three states: Play (Figure 1), Pause (Figures 5, 6), and Stop (Figure 7). In the play state, the camera is capturing and broadcasting video to other HMS participants (Figure 1). In the pause state, the camera no longer captures and broadcasts video to other HMS participants; however, other availability information is sent including the last video frame captured of the user and a count of the number of people in the room (Figures 5, 6). In the stop state, like the pause state, the camera no longer captures video and the last image broadcast is of the wall (Figure 7). The major difference between the pause and stop states is that it is more difficult to move out of the stop state (described in more detail later). Users can explicitly move between states by clicking the play, pause, and stop buttons (three leftmost buttons, respectively in Figures 1, 5, 6, and 7).

Capturing angle. The camera, mounted on a rotating motor [7], is placed near the door and, given the desired camera angle, can capture any region of the room, except the doorway (Figures 3, 4: Camera). This is important as the living room is not visible (Figure 3). We provide the

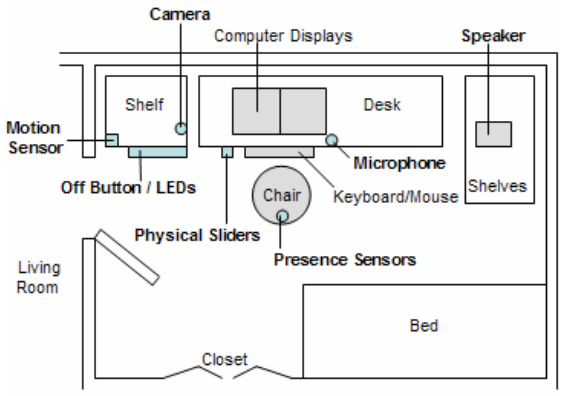

Fig. 4. An overview of the HMS layout.

Fig. 5. The HMS paused with the telecommuter leaving his chair.

Fig. 6. The HMS paused with multiple people in the room.

Fig. 7. The HMS stopped and camera facing the wall.

user with dedicated physical sliders (Figures 3, 4: Physical Sliders, Figure 8-top) and graphical sliders (Figure 2) to explicitly alter the capturing angle.

Video fidelity. Users can adjust the captured video's fidelity by explicitly adjusting the level of blur filtration used (Figures 1, 2, 8-middle), the camera's frame rate (Figures 2, 8-bottom), or the camera's frame size (Figure 2). We provide the user with dedicated physical (Figure 3, 4: Physical Sliders) and graphical controls to explicitly adjust these three components of video fidelity.

Gesture-activated blocking. Users can easily turn off the camera by explicitly blocking it with their hand. We detect this gesture with a proximity sensor mounted on top of the camera (Figures 3, 4: Camera, Figure 9). This can also be done using computer vision techniques [7].

Gesture-activated voice. Users can easily open an audio channel by explicitly moving their hand over a microphone (Figures 3, 4: Microphone, Figure 10). Moving one's hand away from the microphone closes the audio channel. We detect this gesture with a light sensor mounted on top of the microphone. This can also be done (perhaps more accurately) using other sensors, such as proximity sensors.

Easy-off button. Users can easily turn off the camera by touching an off button

Fig. 8. A user adjusts the blur level with a dedicated physical slider.

Fig. 9. A user blocks the camera with his hand to turn it off.

Fig. 10. A user moves his hand over the microphone to open an audio link.

Fig. 11. A sign containing LEDs at the top and an off button.

(Figures 3, 4: Off Button, Figure 11). We detect this explicit action with a capacitive sensor acting as the button, but this could also be done (and appear more realistic) with a control resembling an actual, real-world push button [17].

Telecommuter detection. We know if the telecommuter is present at the computer by detecting (with a light sensor, Figures 3, 4: Presence Sensors) the implicit act of someone sitting down in or standing up from the desk chair. We use a radio frequency identity (RFID) tag in the pocket of the telecommuter and a RFID reader (Figures 3, 4: Presence Sensors) in the chair to identify if the individual sitting is the telecommuter. If the telecommuter is not present, we can tell how long she has been away from the computer. Our *telecommuter detection* is not a realistic solution because of limits imposed by our RFID reader, yet it works for our prototype. Other approaches could include embedding RFID tags within 'work' shirts worn by the telecommuter. This helps because it can ensure the telecommuter is appropriately dressed before the HMS can be used; however, now people must wear this special garment.

Family/friend detection. We know if family/friends are present in the room by using an infrared motion detector (Figures 3, 4: Motion Sensor) to detect the implicit act of walking into and out of the room. This could be done more accurately with computer vision techniques; however, our solution does not require a camera to always be capturing the room's activities.

Visual feedback. We use several visual cues to let the user know how much privacy is currently being maintained, e.g., a sign (Figure 11), LEDs (Figure 11-top), the camera's direction, mirrored video (Figure 1, top), and the position of physical and graphical controls.

Audio feedback. We also use audio cues to let the user know how much privacy is currently being maintained, e.g., the sound of a camera clicking and the sound of the camera rotating [12].

There are many ways to create each of these elements and more accurate sensors exist than the ones we have chosen to use for our prototype. We have chosen methods and sensors that allowed us to rapidly and inexpensively prototype each element.

In the next section, we describe how these elements work together, along with a set of rules, to reduce privacy threats. We demonstrate this with a series of scenarios based on real telecommuting situations.

4 Rules for Balancing Privacy and Awareness in a HMS

Our HMS design uses each element within the HMS, along with a set of rules, to balance privacy and awareness for the telecommuter and others in the home. Table 1 summarizes how the design elements are either: controlled, used for explicit or implicit control, or used as feedback. Each row in the table describes how one media space attribute (column 1) is controlled either explicitly (column 2) or implicitly (column 3). The fourth and fifth columns describe the *audio* and *visual feedback* that indicate to the users that the attribute in column 1 has changed and what its current value is. The first five rows of the table describe the transitions between the three *camera states*. The remaining three rows describe other HMS attributes that can be controlled. The HMS elements, previously discussed, are *italicized* within the table.

We now present a series of scenarios that detail the privacy risks involved with us-

	1	2	3	4	5
	Attribute Controlled	**Explicit Control**	**Implicit Control**	***Audio Feedback***	***Visual Feedback***
1	Stop to Play	Play button	None	Camera clicking; Camera rotating	LEDs on; Camera rotates to face you; Mirrored video
2	Pause to Play	Play button	*Telecommuter detection; Family/friend detection*	Same as above, Camera Twitches	Same as above, Camera Twitches
3	Play to Stop	Stop button; *Gesture-activated blocking; Easy-off button*	None	Camera rotating	LEDs off; Camera rotates to face the wall; Mirrored video
4	Play to Pause	Pause button	*Telecommuter detection*; *Family/friend detection*	Same as above	Same as above
5	Pause to Stop	Stop button; *Gesture-activated blocking; Easy-off button*	*Telecommuter detection*	None	Mirrored video
6	*Capturing angle*	Physical or graphical slider	Change in *camera state*	Camera rotating	Slider position; Camera position; Mirrored video
7	*Video fidelity*	Physical or graphical control	None	None	Control position; Mirrored video
8	Audio link	*Gesture-activated voice*	None	Own voice	None

Table 1: Control and feedback mechanisms found in the HMS.

ing a HMS, the set of privacy rules we have created to address them, and how the HMS implements each rule to balance privacy and awareness.

4.1 Providing Awareness While Masking Embarrassing Acts

The first scenario illustrates one typical use of the HMS by a telecommuter, named Larry, who is working at home and using the media space to provide awareness to a close-working colleague at the office. Larry enters his home office/spare bedroom, dressed in casual pants and a golf shirt. While Larry is working at his computer, he suddenly sneezes. Naturally, he proceeds to blow his nose. Forgetting that the camera is capturing him, Larry begins to pick his nose at great length.

Privacy Risks: Larry is dressed appropriately to be seen at an office, yet he does not want his colleague to view him doing embarrassing, unconscious acts like picking his nose.

Rule 1: If just the telecommuter is present at the computer, the HMS assumes more awareness and less privacy is desired.

Design: This is Larry's first use of the HMS today and the *camera state* is Stop when Larry sits down at the computer. To turn the *camera state* to play (Table 1: Row 1), Larry must explicitly click the play button (Figure 1, leftmost button). Once the *telecommuter detection* has identified that it is indeed Larry at the computer, the HMS provides more awareness by moving the *capturing angle* away from the wall to record Larry. *Visual* and *audio feedback* lets Larry know the camera is now capturing (Table 1: Row 1). Larry can fine tune the awareness information and mask embarrassing acts with *video fidelity* (Table 1: Row 7).

4.2 Providing Privacy When Others Use the Computer

The second scenario illustrates what happens when the telecommuter leaves his desk and others use the computer. Larry is working at his computer when he leaves to get a coffee from the kitchen. Larry's wife, Linda, who is still in her pajamas, comes in to the home office to quickly check her email. Linda leaves the room just as Larry returns. Larry sits down and continues working.

Privacy Risks: Larry is appropriate to be viewed on camera and faces no privacy risks. Linda is not appropriate to be viewed, nor does she want to be viewed: Linda faces a threat/benefit disparity.

Rule 2: If someone other than the telecommuter is present in the room, the HMS assumes more privacy and less awareness is desired.

Design: The *telecommuter detection* knows that Larry has left his desk chair and changes the *camera state* to paused (Table 1: Row 4). *Visual* and *audio feedback* lets Larry know the camera is no longer capturing (Table 1: Row 4). The colleague maintains awareness by seeing Larry leave his chair in the last image broadcast (Figure 4).

When Linda enters the room, the *family/friend detection* flashes the LEDs and plays the sound of the camera clicking to warn Linda to make sure the camera is off. *Visual feedback* shows her that the *camera state* indeed remains paused (Table 1: Row 4). Linda checks her email and is not captured on camera.

When Larry returns to his desk chair, the *telecommuter detection* unpauses the camera, but first warns Larry this is about to happen by twitching the camera left and right (Table 1: Row 2); just as people signal their intentions, so does the camera. This complies with our third design principle. *Visual* and *audio feedback* shows Larry that the *camera state* is again Play (Table 1: Row 2).

4.3 Using Gestures to Regulate Privacy

The third scenario illustrates how the telecommuter can use gestures to control HMS attributes, which in turn affect his privacy. Larry is working at his computer composing an email and drinking his coffee. Just then, Larry knocks his mug and coffee spills all over his shirt! Larry removes his shirt and then notices the camera facing him. Larry blocks the camera with his hand then tells his colleague (through the HMS) that he has to go get a new shirt.

Privacy Risks: Larry does not want to be seen shirtless, yet he still wishes to maintain a level of awareness with his colleague.

Rule 3: The HMS must provide simple lightweight means to immediately disable the capturing device, yet still maintain awareness through alternate channels.

Design: Larry can choose one of two explicit methods to instantly stop the camera: *gesture-activated blocking* or *easy-off button* (Table 1: Row 3). *Visual* and *audio feedback* lets Larry know the *camera state* has changed (Table 1: Row 3). Larry wants to maintain awareness and tell his colleague of his predicament without using the video channel so he uses *gesture-activated voice* to open the optional audio link.

4.4 Providing Privacy When Others Enter the Room

The fourth scenario illustrates what happens when multiple people enter the home office/spare bedroom. Larry is working at his computer in the home office/spare bedroom when Linda, who has just finished taking a shower in the bathroom next door, walks into the room to retrieve her bathrobe from the closet. Linda puts on her bathrobe and leaves the room.

Privacy Risks: Linda does not want to be captured on video, especially while she is naked! Linda again faces a threat/benefit disparity, while Larry still wants to provide awareness information to his colleague.

Rule 4: If more than just the telecommuter is present in the room, the HMS assumes more privacy and less awareness is desired.

Design: The *family/friend detection* knows that Linda has entered the room and moves the *camera state* to paused (Table 1: Row 4). *Visual* and *audio feedback* indicates that the *camera state* has changed (Table 1: Row 4). Larry's colleague maintains a level of awareness with the presentation of alternate awareness information when the camera is paused: the number of people in the room, and the image of Larry sitting at his desk (Figure 5). Using these two pieces of information, it is possible for Larry's colleague to infer that Larry is still working at his desk.

Once the *family/friends detection* knows that Linda has left the room (Table 1: Row 2) and the *telecommuter detection* indicates that Larry is still at the computer,

the *camera state* will return to Play once it first warns Larry with *visual* and *audio feedback* (Table 1: Row 2).

4.5 Finishing Work and Leaving the Space

The fifth scenario illustrates what happens when the telecommuter finishes working and leaves the HMS. Larry has finished working for the day and leaves the home office.

Privacy Risks: The HMS is still active when the telecommuter is finished working; future use of this room may threaten privacy.

Rule 5: If the telecommuter is away from the computer for an extended period of time, the HMS will move to a permanent, non-recording state.

Design: The *telecommuter detection* notices Larry leaving and the *camera state* pauses. After being away from his desk for five minutes, the *camera state* moves to Stop and now the last image shown to Larry's colleague is of the wall (Figure 7). This timeout interval can be customized in Figure 2. The non-recording state is permanent in the sense that to start working again, Larry must explicitly click the play button (Figure 1). Until this time, the camera will not turn on and no video will be captured; thus, no privacy violations will occur while Larry is not working.

5 Supporting Privacy Mechanisms

We now describe how we have leveraged the four categories of privacy mechanisms by designing privacy-protecting strategies for a HMS that fall into the same categories of mechanisms used by humans for privacy regulation in everyday life.

5.1 Verbal Behavior: Sound and Voice

Verbal behavior consists of the use of content and structure of what is said to control privacy [1]. For example, if a family member approaches the home office while the telecommuter is currently working she may say, "I'd like to be left alone," if she would like to have more privacy or alternatively, "please come in," if she desires interaction. We use verbal behaviors in two ways within our design:

1. verbal instructions between media space users; and,
2. verbal instructions or sounds cues from devices in the media space to media space users.

The first approach is trivially supported in the HMS's design for co-located HMS users (e.g., the telecommuter and others in the home): they can simply speak to others in the same location. Distance-separated users of the HMS must rely on a voice channel for this approach. The tradeoff is that we want an audio link, yet not the additional privacy threats found with a continuous audio link [16]. For this reason,

our design provides an optional audio link where *gesture-activated audio* allows users to easily engage and disengage the audio link.

The second approach offers a crucial component of privacy feedback. Feedback of the level of privacy being attained is most easily presented through visuals or with audio. In the case that visuals go unnoticed, *audio feedback* becomes vital.

5.2 Non-Verbal Behaviors: Presenting and Using Gestures

Non-verbal behavior consists of the use of body language, such as gestures and posture, to control privacy and can either be implicit or explicit [1]. When people are located close together, non-verbal behaviours increase [1]. For example, in an exam situation, people may try to block or cover their test paper, indicating their desire for privacy. We use non-verbal behaviours in two ways within our design:

1. gesture-based input for devices within the media space; and,
2. non-verbal instructions between media space users.

The first approach can compliment verbal behaviours much like in face-to-face situations. Gesture-based input offers a lightweight means to control devices; users can give the media space explicit instructions using recognized hand or body motions. Our HMS uses *gesture-activated blocking* and *gesture-activated voice.*

The second approach is simply a replication of that which is done in face-to-face situations where people implicitly or explicitly use body language to control privacy. Co-located users (e.g., the telecommuter and others at home) should have little trouble with this, yet users separated by distance must rely on the video channel for presenting their non-verbal behaviors. *Video fidelity* must be high enough for other participants to easily interpret gestures and postures. As an alternative, Greenberg and Kuzuoka [14] use physical surrogates (e.g., children's toys) as a means for presenting gestures between distance-separated colleagues.

5.3 Environmental Mechanisms: Virtual Fences, Blinds, and Doors

Environmental mechanisms consist of the use of physical artifacts and features of an environment to control privacy [1]. For example, to limit neighbors from viewing one's backyard, a fence may be built or a large row of trees could be planted. Just as individuals can control their own environment in the physical world, they should be able to control their environment in a HMS. The environmental mechanisms for a HMS that we support can be grouped into three categories:

1. lightweight mechanisms for altering the media space's physical environment;
2. self-appropriation for controlling physical appearance and behavior; and,
3. adjustable personal space.

In the first approach, providing users with lightweight mechanisms to alter the environment, allows for easy and simple privacy regulation. Our design allows explicit

control over *camera state, capturing angle,* and *video fidelity*; and implicit control over *camera state* and *capturing angle.*

The second environmental approach lays in the hands of media space users. Self-appropriation involves creating an appearance and behavior suitable for the current situation [3]. Given enough *visual* and *audio feedback* of the level of privacy currently being attained, users have the power to control their own privacy by simply appropriating themselves correctly [3]. This can be difficult in a HMS however. Participants at the home location may be forced to appropriate themselves for the office, which itself can be an infringement on their autonomy. To help alleviate this problem, users can rely on lightweight controls to help users appropriate themselves correctly for both home and the office, e.g., *video fidelity*. 'Work' shirts with embedded RFID tags could also provide an interesting solution to this problem.

The third environmental approach allows HMS users to utilize personal space for controlling privacy, just like in face-to-face situations. First, the media space can be setup in any location within the home. Our HMS is setup within a home office/spare bedroom because this type of room offers users a large amount of control over their privacy because it is not commonly used by many people within the home. Second, within the media space, the camera can be positioned in any number of locations; camera placement determines what background information is captured. This typically becomes unremarkable over time [21], but care can be taken so that background information does not include areas such as an open doorway where others may be able to see through the doorway into other rooms.

5.4 Cultural Mechanisms: Social Solutions

Cultural mechanisms consist of the use of cultural practices and social customs to control privacy [1]. Although it may often go unnoticed, each culture contains a set of learned social practices and customs that have evolved and developed over time [1]. We feel that in a HMS, social practices should develop about several key issues:

1. the purpose of the media space;
2. who is allowed to view what is captured; and,
3. what content is appropriate to be seen.

Since the HMS has yet to be extensively used by individuals, we are not able to describe the use of cultural mechanisms to regulate privacy. The importance, however, is that given an established set of social protocols, users can rely on them to regulate privacy when technology does not suffice. In the case that social norms are not followed, social ramifications may be in order.

6 Software and Hardware

The HMS is designed as an ActiveX® Control, which can be easily used with languages supporting Microsoft COM technologies, e.g., Visual C++, C#, Visual Basic.

Two toolkits, developed in our research lab, were used to develop the HMS prototype. The first, Collabrary, makes it easy to create software with video and audio links and alter attributes such as video fidelity [8]. In the HMS, the Collabrary's shared dictionary component is used to capture and transmit video and audio between users of the HMS. The second toolkit, Phidgets™, which contains pre-packaged physical devices and a corresponding software Application Programming Interface (API), makes it easy to rapidly prototype physical interfaces and sensing environments [15]. In the HMS, all of the sensors and controls are Phidget™ devices and are accessed using the Phidget™ API.

The importance of these two toolkits is that they allowed us to move our research focus away from the underlying implementation of the HMS. As such, we were able to focus our time and effort on deciding and exploring how context-aware computing could be used, what its effects would be, and if our techniques were appropriate given our research goal of balancing privacy and awareness.

7 Conclusion

This paper presents the rationale and prototype design of a home media space (HMS). The HMS is designed specifically for the telecommuter who chooses to work at home, but who still wishes to maintain a close-working relationship with particular colleagues at remote office environments. Our contribution is a set of five design principles for a HMS and a prototype HMS which illustrates these principles. Specifically, we explain how and why:

1. existing privacy mechanisms are leveraged for use in home-based video conferencing systems;
2. implicit actions using context-aware technology can regulate privacy;
3. no implicit action should ever decrease the amount of privacy without first warning the user and providing the opportunity to stop the operation;
4. explicit actions using dedicated physical controls and gesture recognition can regulate privacy; and,
5. visual and audio feedback makes the state of the system easily discernable at any time.

Using these five design principles, we have created a set of privacy rules that regulate how privacy and awareness are balanced in a HMS. Our actual use of context-aware software and dedicated physical controls has yet to be evaluated for its effectiveness in balancing privacy and awareness. However, we provide a general approach for integrating the privacy mechanisms used by people in their physical environments into a HMS. By using two toolkits, including a set of pre-packaged physical devices and sensors, we were able to focus our research on understanding how context-aware computing can be used in real-world applications. This provides a valuable contribution to context-aware computing in general.

While we have concentrated on one specific use of video in homes, our paper contributes ideas that have a broader significance for home-based videoconferencing in

general. Irregardless of the specific use of video in a home, people need and desire methods to regulate their privacy; many video conferencing systems (e.g., Webcam for MSN Messenger, Yahoo! Messenger) ignore these user requirements.

Acknowledgments

We would like to acknowledge NSERC and Microsoft Research for their partial funding of this research. A special thanks to Michael Boyle for the use of the Collabrary, Chester Fitchett for the use of Phidgets™, and Stacey Scott for help with editing.

References

1. Altman, I.: The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding, Wadsworth Publishing Company (1975) pp. 1-51, 194-207.
2. Altman, I., and Chemers, M.: Culture and Environment, Wadsworth Publishing Company (1980) pp. 1-12, 75-119, 155-214.
3. Bellotti, V.: Design for Privacy in Multimedia Computing and Communications Environments, in Technology and Privacy: The New Landscape, Agre and Rotenberg eds., MIT Press, (1998) pp. 63-98.
4. Bellotti, V.: What you don't know can hurt you: Privacy in Collaborative Computing, Proc. HCI '96, Springer, (1996) pp. 241-261.
5. Bellotti, V., Back, M., Edwards, K., Grinter, R., Hnderson, A., and Lopes, C.: Making Sense of Sensing Systems: Five Questions for Designers and Researchers, Proc. CHI 2002 [CHI Letters 4(1)], ACM Press, (2002) pp. 415-422.
6. Bly, S., Harrison, S. and Irvin, S.: Media spaces: Bringing people together in a video, audio, and computing environment, Communications of the ACM 36(1), ACM Press, (1993) pp. 28-46.
7. Boyle, M., Edwards, C. and Greenberg, S.: The Effects of Filtered Video on Awareness and Privacy, Proc. CSCW'00 [CHI Letters 2(3)], ACM Press, (2000) pp. 1-10.
8. Boyle, M., and Greenberg, S.: GroupLab Collabrary: A Toolkit for Multimedia Groupware, in J. Patterson (Ed.) ACM CSCW 2002 Workshop on Network Services for Groupware, (2002).
9. Erickson, T.: Some problems with the notion of context-aware computing, Communications of the ACM, Vol. 45(2), February 2002, (2002) pp. 102-104.
10. Fish, R.S., Kraut, R.E., and Chalfonte, B.L.: The VideoWindow System in Informal Communications, Proc. CSCW'90, (1990) pp. 1-11.
11. Fish, R.S., Kraut, R.E., Rice, R.E., and Root, R.W.: Video as a Technology for Informal Communication, Communications of the ACM, Vol. 36, No. 1, ACM Press, (1993) pp. 48-61.

12. Gaver, W. W.: Everyday listening and auditory icons. Doctoral Dissertation, University of California, San Diego (1988).
13. Greenberg, Saul: Peepholes: Low Cost Awareness of One's Community, Proc. Of CHI'96, Companion Proceedings, ACM Press, (1996) pp. 206-207.
14. Greenberg, S. and Kuzuoka, H.: Using Digital but Physical Surrogates to Mediate Awareness, Communication and Privacy in Media Space, Personal Technologies, 4(1), January (2000).
15. Greenberg, S. and Fitchett, C.: Phidgets: Easy Development of Physical Interfaces through Physical Widget, Proc. UIST 2001, ACM Press, (2001) pp. 209-218.
16. Hudson, S.E., and Smith, I.: Techniques for Addressing Fundamental Privacy and Disruption Tradeoffs in Awareness Support Systems, Proc. CSCW'96, (1996) pp. 248-257.
17. Jancke, G., Venolia, G.D., Grudin, J., Cadiz, JJ, and Gupta, A.: Linking Public Spaces: Technical and Social Issues, Proc. CHI 2001, ACM Press, (2001) pp. 530-537.
18. Kraut, R., Egido, C., and Galegher, J.: Patterns of contact and communication in scientific observation, Proc. CSCW '88, (1988) pp. 1-12.
19. Lee, A., Girgensohn, A., Schlueter, K.: NYNEX Portholes: Initial User Reactions and Redesign Implications, Group '97, ACM Press, (1997) pp. 385-394.
20. Mantei, M., Baecker, R., Sellen, A., Buxton, W., Milligan, T., and Wellman, B.: Experiences in the use of a media space, Proc. CHI '91, ACM Press, (1991) pp. 203-209.
21. Neustaedter, C., Greenberg, S., Boyle, M.: Balancing Privacy and Awareness for Telecommuters Using Blur Filtration, Report 2003-719-22, Department of Computer Science, University of Calgary, January (2003).
22. Schilit, B., and Themier, M.: Disseminating Active Map Information to Mobile Hosts, IEEE Network 8(5), (1994),pp. 22-32.
23. Tang, J.C., Isaacs, E., and Rua, M.: Supporting Distributed Groups with a Montage of Lightweight Interactions, Proc. CSCW '94, ACM Press, (1994) pp. 23-34.
24. Want, R., Hopper, A., Falcão, V., and Gibbons, J.: The Active Badge Location System, ACM Transactions on Information Systems, Vol. 10, No. 1, January, ACM Press, (1992) pp. 91-102.
25. Zhao, Q.A., and Stasko, J.T.: Evaluating Image Filtering Based Techniques in Media Space Applications, Proc. CSCW'98, ACM Press, (1998) pp. 11-18.