Privacy Mirrors:
Understanding and Shaping
Socio-technical Ubiquitous Computing Systems

David H. Nguyen and Elizabeth D. Mynatt

Everyday Computing Lab
College of Computing and GVU Center
Georgia Institute of Technology
Atlanta, GA 30332-0280
{dnguyen, mynatt}@cc.gatech.edu

Abstract. Privacy is a known issue in ubiquitous computing, exasperated by an oft-cited feature of ubiquitous computing — invisibility. Dangers of invisible computing are interfaces that do not give people the needed tools of awareness and control to understand and shape the behavior of the system. By definition, ubiquitous computing systems are socio-technical, encompassing three environments: social, technical, and physical. We argue that addressing or presenting solutions in any one environment alone cannot solve the privacy issue in ubiquitous computing. Privacy is addressed best by giving users methods, mechanisms, and interfaces to understand and then shape the system in all three environments. We introduce Privacy Mirrors, a framework for designing socio-technical ubiquitous computing systems that will integrate into people's on-going needs, practices, values, and aesthetic sensibilities.

1 Motivation

An oft-cited feature of ubiquitous computing (ubicomp) is invisibility [31]. When done well, designing for invisibility leads to computing environments that are integrated into people's on-going needs, practices, values, and aesthetic sensibilities. Invisible computing often leverages implicit input from people, thereby minimizing the threshold of effort required to gain benefits from the system. However, invisible computing has many dangers as well. An example of this danger is a system that secretly collects information and disseminates that information inappropriately. Another example is a system that normally transmits data, but this fact is not relayed to an unknowing new user of the system. Such systems are not well integrated into the social practices of their users. Clearly, privacy is an issue in ubicomp [17].

More subtle dangers of invisible computing are interfaces that do not give people the needed tools of awareness and control to understand and shape the behavior of the system. Too often ubicomp designers favor the benefits of implicit input without considering the dangers of invisibility. For example, a system that tracks the location of a cell phone may make it easier for others, including emergency assistance, to find the user. However, without reasonable interfaces that convey how this information is disseminated and logged, people are left to trust that the system's designers have similar values and will "do the right thing."

This lack of awareness and control is not simply a privacy issue, addressing the question "Do the wrong people know things about me?" It presents fundamental issues in people not understanding the capabilities of a system, and thus not being able to shape that system to meet their particular needs, practices, values, and aesthetic sensibilities. Without the former (understanding the system), the latter (shaping the system) is impossible. Current ubicomp systems have no mechanism for people to reflect upon the system, to see how they and their information affect, contribute, interact, or participate in the system. Understanding the system also means helping users to understand the limitations and constraints of a system. For example, a kitchen system that helps a person maintain groceries in the house will have sensing limitations, which may be dynamic, based on sensors and situations. Effective use of this tool requires understanding what the sensing system missed so that a person can compensate. As ubicomp systems rely on implicit sensing that is naturally ambiguous or error-prone, designers must help users comprehend the limitations of the system.

2 Related Work

Because our focus is on ubicomp systems and privacy, the work that influences our research is varied and numerous. We are obviously influenced by the various privacy guidelines and legislation from the United States as well as those in Asia and Europe. An early precursor to ubicomp systems is media spaces. We draw on previous research in this area, especially the work of Victoria Bellotti and Abigail Sellen with their notion of *control* and *feedback*. Other influences on our research include Tom Erickson and Wendy Kellogg's work on social translucent systems and Stephen Kaplan and Rachel Kaplan's work in environmental psychology. We will describe these related topics in greater detail in the rest of the paper.

3 Understanding and Shaping the System

Ubicomp systems are inherently socio-technical. By definition, ubicomp systems cover three environments: social, technical, and physical. Ubicomp, like other computational systems, creates a technical environment. Moreover, ubicomp espouses computation being ubiquitous, being off the desktop, and being proliferated throughout the physical environment. The physical environment is then an integral part of ubicomp. And much like groupware, ubicomp enables people to be connected, not only in work but also in play. This makes the system and the users part of a social environment. These three environments (social, technical, physical) are intrinsic to ubicomp systems and are tightly integrated to each other — a change in one will affect another. For example, in an instrumented room, changing the lighting conditions (physical environment change) will affect camera and perhaps vision performance (technical environment change) and consequently may change usage of the system (social environment change). Thus, when we use the term "understanding and shaping the *system*," we mean understanding and shaping the social, technical, and physical environments.

Thus addressing or presenting solutions in any one environment alone cannot solve the privacy issue in ubicomp. Speaking about privacy and control in media spaces, a precursor to ubicomp, Paul Dourish wrote, "…we suggest that a purely, technical notion of protection and control is not only inappropriate, but impossible" [5]. And Victoria Bellotti and Abigail Sellen pointed out, "…it is dangerously complacent to assume that social and organizational controls over accessibility of personal information are sufficient, or that intrusions into privacy will ultimately become acceptable when traded against potential benefits" [2].

Moreover what constitutes *privacy* is dependent on the person being asked. A piece of information that is private to one person might not be so private to another. Privacy also depends on situation and context. Personal information may be comfortable to share within a small work group, but may be uncomfortable within a larger group [3]. Speaking to individuals is very different than speaking to the world [16].

Acknowledging this complexity in privacy, we introduce Privacy Mirrors, a framework for designing socio-technical ubicomp systems. A Privacy Mirror will allow users to understand how their personal information may be used by others, to understand how they and their information participate in the system, to understand the *socio-technical ubiquitous computing system*. We use the term *mirrors* because we want methods, mechanisms, and interfaces to *reflect* the history, current state, and nature of socio-technical ubicomp systems.

4 Privacy Mirrors Framework

Privacy Mirrors help users understand the socio-technical system and consequently be able to shape it to fit the users' privacy needs. They bring to the foreground the flow, state, and history of what once may have been invisible information.

Privacy Mirrors cover five characteristics in all of the three environments stated previously. The five characteristics of a Privacy Mirror are: history, feedback, awareness, accountability, and change. Privacy Mirrors provide *history* of the information flow and interactions throughout the three environments. History information, flow, and current states of the environments are provided through visibility and *feedback* to users. This feedback provides *awareness* and *accountability*. All this, in turn, enables users to enact *change* in any of the three environments, and thus, change the system.

To ground the framework, we will present it along with an example. Many of the challenges of a groupware calendar system (GCS) are similar to the challenges of ubicomp systems, particularly privacy in a socio-technical system [21]. We will describe the five characteristics of the framework, note how the framework has been applied to the design of a Privacy Mirror for a GCS being developed by our group called Augur [29], and present some questions designers might want to consider for each characteristic.

4.1 Provide History

Recording history is not an entirely new and novel concept. As the adage goes, interpreting the path of the future is made easier by understanding the past. The physical world records its own history (e.g. the rings in a tree trunk or the wear of a hiking trail). Some digital systems record their status and activity in logs (e.g. web server access and error logs, credit card transactions, phone usage, automatic tollbooth logs). However, what is fundamentally different in digital (especially ubicomp) technology is its ability to record and process massive amounts of history.

Working upon visions by luminaries such as Bush, Engelbart, Weiser, and Bell, researchers have used digital technology to record and process classroom lectures [1], meetings [22][24], and general experience [11][4][28]. The amount of information collected through these systems is large; every interaction, every state change in the digital system can be saved. In digital systems, designers can have the system track and log as many or as few states and interactions as they want. This is a unique aspect of digital technology.

History contains a wealth of information. This information could be a person's communications for the day, to be reflected upon at a later time. This information could be who and how many people accessed a research group's web page. With history, people can more accurately and more easily reflect upon the past and infer emerging trends for the future.

However, because the information resides in a social system as well as a technical system, we want users to understand not only technical state changes but also how people interact with that information (i.e. access and usage, who was involved, where it took place, when it took place, and so on). Much like a hiking trail, social systems do not form instantly, they take weeks, months, sometimes years to gather collective acceptance of rules and norms. Having history information will give people greater insights into the social systems in which they are a part.

Let's see how history has affected the design of Augur. Most important for privacy is the history of the social environment. Augur logs all accesses as the group shares their calendars, because as a group shares their individual calendars and uses them in everyday practice, they form social norms. These norms are manifested in the way people use the system and are revealed in the trails of social history left by the group [10][29] — who looked at whose calendar, when, how often, from where, and so forth. Thus, the better a group understands the technical workings as well as the social norms of the system, the better they can shape that system to fit their privacy needs.

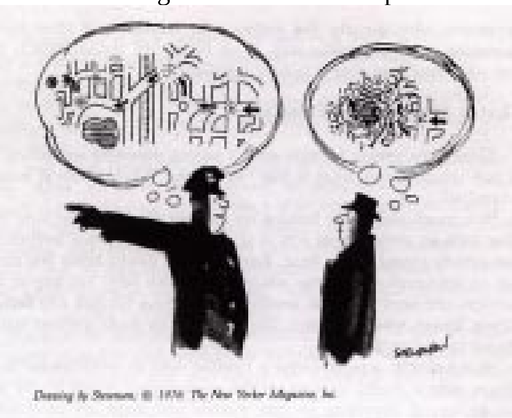
Some questions designers might want to consider are: How to summarize the past so people can more accurately and more easily understand it? What do people want to know? What trends and patterns are people interested in? What specific questions do people want answers to? What needs to be recorded? What doesn't need to be recorded (what needs to be left out)? What is socially unacceptable to record? How does context get recorded alongside the data? Should data deteriorate over time? What needs to be forgotten? Should history be exact, especially when its recall is not framed in the same context?

4.2 Provide Feedback

History is useful and important. However, it has little value if it is not presented, even detrimental if users do not know that history is being recorded. We need to make invisible information visible, and we need to present it in appropriate ways. But what is appropriate? What is the best way to present the flow, state, and history of invisible information to the users?

Depending on the information and the situation, certain media may be better received than others. Because humans are predominantly “sight animals,” visual media work well [20]. And in the realm of sight, certain visuals are more compelling and salient than others, e.g. faces are better recognized than written names. However, visual information is not the only available channel to present information to the users. Feedback can focus on the other four senses as well.

Another appropriate way to present feedback is through levels. Someone who is new to the system will neither want nor be able to understand all information about the system at once (see figure 1). Someone who is busy will not want information from the system to distract his attention away from his current task. However, people do want to make sense out of their environments [15]. So we must take into account the users’ current needs and their cognitive models as we present the feedback.



Drawing by Stevenson; © 1976 The New Yorker Magazine, Inc.

Figure 1. Providing appropriate cognitive models

As users gain more experience with the system, their cognitive model of the system will grow appropriately. Privacy Mirrors support differing cognitive models by providing information at different levels – glance, look, and interactive. *Glancing* at a Privacy Mirror will give a small amount of information, much in the same sense as when a person walks by an actual mirror and notices in the reflection that something is stuck on his shirt. An example of a *glance* interface is an ambient display, designed to give information without requiring extra attention or effort from its audience [13]. Stopping and *looking* at a Privacy Mirror will give more information, because more time is spent scrutinizing the reflection. An example of a *look* interface is an informational display, designed simply to give information to its audience. Flight arrival and departure screens at airports are typical *look* interfaces. And *interacting* with a Privacy Mirror will give the user the most amount of information. The user can ask the system to provide more information, to give greater detail, or to narrow or widen the scope of inspection. An example of an *interactive* interface is any of the interactive programs that are normally seen on desktop computers.

When providing information at different levels, it is important not to overload the user. However, this also means that at the top levels, only a small and select amount of information can be presented to the user. That select amount of information should be what the user wants to know in that particular situation. An ideal interface will encompass all three levels, so users can always dig for more information. Brad Rhodes had a similar notion to lessen disruptions; he called it “ramping interfaces” [23].

The levels are also reminiscent of Ben Shneiderman’s Visual Information-Seeking Mantra: overview first, zoom and filter, then details on demand [26]. This is not surprising because feedback has the potential to have a very large dataset. However, the glance level of a Privacy Mirror does not necessarily mean an overview of the dataset. It could be one specific piece of information that the user is interested in.

Yet another consideration for appropriateness of feedback is the location at which to present the information. Some information, in a sense, does have a “native habitat.” Using our GCS example, electronic calendar information can reside just about anywhere because it is only a pattern of zeros and ones. However, to people, schedules are in Palm devices, in Outlook, or at Yahoo! Calendar. The native habitat for their individual calendar is where they go to find that information. Unfortunately, not all information have a defined sense of location. We want feedback to be presented to users; so sometimes we will need to present the feedback in both “user space” (user’s physical space) and “information space” (the information’s “native habitat”).

Focusing on privacy, Augur users know who has accessed their calendar, how recently, what was looked at specifically, and from where? Users want this information, because for example, a stranger accessing calendar information from the same building will invoke different comfort levels from a stranger accessing calendar information from a foreign country. Knowing actual usage of their calendar information will give users better insights on how to shape the system to satisfy their privacy needs and comfort levels.

Visibility and feedback are fundamental aspects of HCI [19]. Thus it is a natural extension for ubicomp systems to provide feedback, to present not only history information, but also the flow and state of the invisible information of the system to users. With appropriate feedback, users will understand and be more aware of the system. And thus make the system more intelligible. We address awareness in the next section.

Some questions designers might want to consider are: How to address the senses effectively for feedback? How to provide different levels of information? Where to provide feedback? How to provide feedback to groups as well as individuals? What feedback is important to people?

4.3 Provide Awareness

Feedback provides people with information about the flow, state, and history of invisible information. Awareness arises when people process that information. In particular, when we say *awareness*, we mean that people are aware of:

1. How they participate in the socio-technical system
2. How others participate with respect to them and their information
3. How everyone can and cannot participate (features and constraints) in the socio-technical system

With awareness, people can interpret their relationship with the social, technical, and physical environments in which they live and work:

Social – They may find out that their calendar information is not used or seen by their supervisors, but rather that their calendar information is more likely used by their subordinates [9]. They may be able to better understand and predict their colleagues' needs because they are more aware of their colleagues' action with respect to them.

Technical – They may be able to understand that any new calendar information will not be shared with others until they synchronize their Palm devices.

Physical – With awareness, they may realize that opening their window blinds allows in sunlight that overexposes their cameras, affording them a little privacy by controlling how much video information leaves their space.

A user's needs and practices will dictate how much awareness he requires. For example, the system may be able to display who has looked at the user's calendar information. However, if a user does not really care who has read his schedule, then there is no need to provide this service to him. People have only a finite amount of attention to give; providing unneeded information is more of a hindrance than a service.

Awareness of the system will better form the user's comfort level and his usage of that particular system. Monitored workers experience higher levels of depression, tension, and anxiety, and lower levels of productivity than those who are not monitored [25]. Privacy Mirrors strive to give users a better understanding of the flow, state, and history of information throughout that system. With this better understanding the user can see if his personal comfort level for privacy fits within the current workings of the system. And because the information is presented at different levels, he will be better able to incorporate that information into his work. In the case of being monitored, he may change the monitoring to a level he can tolerate.

Most legislative and normative efforts have aimed at providing greater awareness of the recording of personal information. For example, in 1973, the Department of Health, Education, and Welfare created a commission to study the impact of computers on privacy. That commission created a "bill of rights" for computers and digital information – the Code of Fair Information Practices. This code is based on five principles:

1. There must be no personal data record-keeping systems whose very existence is secret. [*Feedback and awareness*]
2. There must be a way for a person to find out what information about the person is in a record and how it is used. [*History, feedback, awareness, and accountability*]
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent. [*Change*]
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

One can see how the privacy principles have influenced Privacy Mirrors. *History* satisfies principle #2. *Feedback* satisfies principles #1 and #2. *Awareness* satisfies principles #1 and #2. *Accountability* satisfies principle #2. *Change* satisfies principle #3. Principles #4 and #5 are not explicitly addressed through the Privacy Mirrors. However, such properties are needed to engender trust of any ubicomp system.

In the Far East, similar guidelines have been passed, for example, the Hong Kong Personal Data (Privacy) Ordinance [18]. The European Union passed the EU Directive 95/46/EC of 1995[8]. One of the biggest impacts from this directive is the notion of *explicit consent* to the processing of personal data. This requires the user to unambiguously give his consent before his personal information can be process. In effect, the directive has added accountability, a principle we will address in the next section.

Some questions designers might want to consider are: How to convey cognitive models of larger socio-technical systems? What are different awareness needs? Do users want affirmation that someone is looking? Do users want to see social dynamics of particular users? Do users want to see social dynamics of a workgroup?

4.4 Provide Accountability

Tom Erickson and Wendy Kellogg suggest social translucent systems have three characteristics: visibility, awareness, and accountability. Visibility and awareness go hand in hand; visibility creates awareness. Awareness "brings our social rules into play to govern our actions" [7]. For example, knowing that their professors cannot hear or identify them, students can give a more candid critique of their professors. Accountability provides the "I know that you know," to socially govern people's actions. This information "provides a basis for inferences, planning, and coordination" [7].

Social translucence uses properties of the physical world to design systems to support communication. While Erickson and Kellogg are "making social information visible," we are attempting to make the socio-technical system visible.

Privacy Mirrors will provide the mechanism necessary to make a ubicomp system a social translucent system. Thus making the system a benefit in the interactions of the occupants amongst themselves and the system.

Accountability plays a large role in social translucence. It also plays a large role in Privacy Mirrors, because social and personal information is an intrinsic part of a ubicomp system. When someone accesses a piece of private information, the owner of that information should be able to determine who accessed that information. At the same time, when someone accesses a piece of private information, the person doing the accessing should also know that his actions have been processed in some way. The feedback to both parties creates a *you-know-that-I-know-that-you-know* condition that as we have just said, brings already well-defined social and cultural practices into the situation [7]. Social codes of conduct will influence how both people and technical systems perform. Knowing that *you-know-that-I-know-that-you-know* affect people's behavior, in both sharing and obtaining data. A complex, technical security system may not be needed if social pressure will keep people from accessing each others' information. And because people will know what the technical system is doing, accountability will play in a role in which systems may log data, which may transmit data, or which may process any data at all.

As an additional benefit, accountability also plays a role when a vague or not well-formed privacy space is approached. Knowing that *you-know-that-I-know-that you-know* gives a concrete subject and shared understanding for people to communicate and form social norms for that space.

It is also interesting to note that the owner of the information is not necessarily responsible for the usage of that information. Sometimes the responsibility can be delegated to the recipient. For example, people have their parents' phone numbers. However, it is not up to the parents to set when their children can and cannot call. The caller shares some responsibility for that before each call.

Back to our GCS example, much like peeking one's head into a colleague's office, visualizing calendar accesses will give both parties involved the awareness and accountability. From the calendar viewer's perspective, accountability brings in social norms for viewing others' calendars — perhaps, in this group, viewing another's calendar every 10 minutes is frowned upon. From the calendar owner's perspective, knowing who and how often someone has looked at his calendar may change his comfort level for sharing calendar information. If no one looks at his calendar, it won't matter how he maintains his calendar. If a trusted colleague is looking at his calendar often, he might initiate contact to see if his help is needed.

Some questions designers might want to consider are: How to provide accountability while maintaining social lubricants such as plausible deniability? What kinds of interfaces will hold people more accountable than others, especially in the disembodied digital world?

4.5 Enable Change

Change is the ability to use Privacy Mirrors to shape the socio-technical. We do not want to focus just on the technical part of the system, but also the social practices and physical environment of the system. Privacy Mirrors give people a cognitive model so they can anticipate the socio-technical system and adjust it appropriately, through technical, social, and physical means.

The system gives certain information as feedback. The user should be able to utilize that information to form an awareness of the things he finds important. If he is aware of a beneficial flow of information, he may want to provide more information to feed that flow. If he is aware of an unhelpful flow of information, he may want to stop that flow altogether, he may restrict that flow, or he may want to modify the information involved in the flow. Being aware of and understanding the system, the user can change technical, social, and physical workings of the environment to better fit his needs.

For example, if a user knows how his calendar information is being accessed, he can affect the flow of that information by changing the permissions of those accessing the calendar information. Affecting a change through this type of technical means may be an engineering challenge. As another option, the user can elect to produce change through more social means. The user might want to change his coding scheme, such that while the descriptions are still available, they only make sense to him. For example, an appointment with Dr. Morgan changes from “Dr. Morgan” to simply “Morgan.”

Paul Dourish, Annette Adler, Victoria Bellotti, and Austin Henderson's experiences with video-mediated awareness systems point to the need for users to be able to see how their image is projected to others. By knowing how others saw them, media space users understood how the system worked. Media space users often experimented over a period of time with the placement and range of video cameras and microphones [6]. By having the feedback to show how video was transmitted, they were able to experiment with the placement of video cameras to best fit their needs. Because of technical limitations, sound feedback was not as straight forward as video feedback. And without feedback, sound usage and microphone placement were more problematic.

The experimentation of placement and range on audio and video equipment inspired Bellotti and Sellen to address the issue of privacy in media spaces and consequently ubicomp environments through their notion of control and feedback [2].

- **Control**: Empowering people to stipulate what information they project and who can get hold of it.
- **Feedback**: Informing people when and what information about them is being captured and to whom the information is being made available.

Before one can fully implement control, one needs the feedback to understand the possible different types of information to control. After understanding the feedback, the occupant of the ubicomp system will be more aware of the different kinds of information available to the system. With this awareness, the person can control and manage this information. Feedback will help with the control and management. Then the cycle continues.

Some questions designers might want to consider are: How to present the language of change to people? What is the language of technical change? Is it direct manipulation of the feedback provided by the system? Could it be setting privacy preferences by example and letting the system work out the rules of information flow?

4.6 Summary of the Privacy Mirrors Framework

	Social environment	Technical environment	Physical environment
History of	Being in the social environment and having feedback of its history will give insights into the customs, norms, rules, and practices of a group	Web server logs, automatic tollbooth logs, and credit card transactions are examples	Rings of a tree trunk, wear of a hiking trail, and stacks of recently read papers are examples
Feedback of		Numbers, rates, and status. What the system knows and how to display it	Physical space already has its own feedback mechanism.
Awareness of	Knowing customs, norms, rules, and practices	Knowing how and what the technical system is doing	Knowing the physics of the current space
Accountability of	*You-know-that-I-know-that you-know* and the cultural norms that accountability brings into play	Technical system tells people what it knows, how it knows it, and what it plans to do with that information	Having spent their entire life in the physical environment, people know the accountability of it well.
Change of	Modifying customs, norms, rules, and practices. Changing descriptions in one's calendar is an example.	Modifying permission settings is an example.	Rearranging furniture is an example.

To summarize the five characteristics, history and feedback provide users with awareness and accountability. The awareness and accountability then help users to change one or more of the social, technical, or physical component of the socio-technical system.

Privacy Mirrors will allow users to "play" with the system – enacting change and seeing the feedback reflected back to them. See an unwanted web page access? Change that web page or add a password and see the access patterns to that web page change. See more people viewing calendar information than expected? Change the calendar and see how the access patterns change.

The characteristics of Privacy Mirrors combine to enable users to make sense of the socio-technical system in which they live. Privacy Mirrors allow people to understand the system better by revealing the system's capabilities as well as the system's constraints. Understanding the socio-technical system will allow users to be better informed when requesting new technical features and functions. Privacy Mirrors also give people another perspective in understanding the actions of others because access to information is tracked and accountability becomes a part of the system. They will help users find social improvisations, if a technical function is missing. Privacy Mirrors allow people to make sense of the world around them.

"What people prefer and care about both influences and is influenced by the thought process. People's comfort, their sense of feeling at home, and their confidence in any given setting are all inseparable from their knowledge of that environment and from how readily knowable that environment is."

– Kaplan and Kaplan [15]

By enabling people to understand and shape the socio-technical system, we hope to allow people to make sense of their environment (in all three social, technical, and physical environments), giving users comfort and confidence. From environmental psychology, we know that people prefer environments that are more likely to meet their needs. Just as people need food and affection, making sense of their environment is a continuing concern throughout their lifetime. People are more likely to favor a situation where there will be enough to eat, where they will be received with affection, and so on. In this way, people have a preference to environments that are more likely to meet their needs for the future.

Thus, we can use environmental psychology to inform the design of Privacy Mirrors, as a whole. A well-liked environment has [15]:

1. **Coherence**: how easy it is to organize and structure
2. **Complexity**: too little would be boring, too much undesirable
3. **Mystery**: a preferred environment is one that give the impression that people could acquire new information if they were to travel deeper into it
4. **Legibility**: an environment that looks as if people could explore extensively without getting lost

Now that we have outlined the Privacy Mirrors Framework, we will use that framework to critique an early prototype of a Privacy Mirror.

5 Critique Web Server Log Mirror

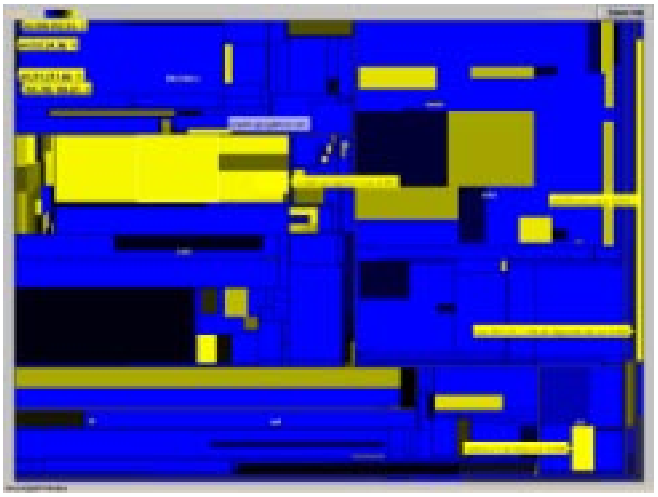


Figure 2. Web Server Log Mirror on a peripheral display

The World Wide Web is an inherently public, shared space. However, homepages and websites can contain all sorts of information, from personal details to random trivia. Outside of the website administrator, few have access to information on who visits these pages or which pages were visited. WebAware displayed which pages were accessed in a galaxy-like format using a large LCD [27]. It was a great conversation piece, spurring many conversations about their website. We build upon that work to make the Web Server Log Mirror (WSLM), bringing erstwhile invisible information to a peripheral display (see figure 2). The WSLM uses Treemaps to visualize pertinent information found in the logs of web servers [14] [12].

Using Treemaps, we have implemented two versions of the WSLM. One shows who has visited a website (any part of the site). In this version, the Treemap is divided using the domain and host names associated with each HTTP request. This means machines coming from ".edu" are in one rectangle and machines coming from ".com" are in another rectangle. Within each rectangle, the domain and host names are broken down by sub-domain names, until a specific machine occupies a single rectangle within rectangles of similar domain and hostnames. For each machine, the number of hits coming from that specific machine determines the size of the rectangle. An additional dimension of time is added using color. The rectangles vary in color between the shades of blue and yellow. The more yellow the rectangle, the more current the last visit has been. Bright blue rectangles contain visits that are two or more weeks old.

The other version of the WSLM shows which page was visited (by anyone). The rectangles in this version represent specific pages on the site. The hierarchical nature of Treemaps is mapped to the hierarchical structure of web ages stored on the file system. The use of color to distinguish the dimension of time remains the same.

History –

History is shown through the size and color of each rectangle. For example, in the first version that tracks machines accessing a particular web site, one can see that a machine name gigan.cc.gatech.edu has accessed the site many times (large rectangle) and the last access was approximately one week ago (middle shade). However, a finer understanding of the access history is not to be had through this interface. There is no way to use this interface to see the distribution of accesses through a week — nine days of no activity followed by a surge of 1000 accesses look the same as 100 accesses spread over the last 10 days.

Feedback –

This prototype presents an aspect of history with the limitations stated above. It also shows who (which machine) has accessed the web site and which particular page was accessed.

The prototype implements the three levels of glance, look, and interactive. One can glance at the interface and gather from the color patterns to see if the site has been visited lately. One can look to see which domains have visited the site more often than others. And interactively, one can drill down to see the activity of a specific machine.

One missing aspect of feedback is that we do not tell visitors that we are logging them. The feedback, as it stands, only benefits the owner of the web site. One simple solution is to state on the web page that logging is taking place. A better solution might be to let the viewers see what kind of information the web site has logged with respect to the viewing machine. However, because machines may have multiple users, giving the current user history information of the machine may invite other privacy issues.

Another consideration is to present feedback on the web page itself. This would put the feedback in “information space.” However, people usually do not visit their own web site all that much. So in this case, putting the feedback in the web site is not a good idea.

Awareness –

When we first started running the WSLM, the version that visualized which pages were accessed the most, we saw a large number of accesses to pages which started with “/script.” We were not aware of any “/script” directory on our Apache web server. Those pages under “/script” did not exist and the web server reported it so, but attempts to access the “/script” directory continued. Though it made no sense at the time, it was quite apparent from this Privacy Mirror that the “/script” directory was popular. Within a few days, it was national news that various web server worms were trying to exploit security holes in the Microsoft web server and “/script” was where the security hole was.

The web is public in nature. However, we were still surprised by the actual usage of our web site. We did not realize so many people from different countries visited our web site. We did not realize search engines crawled through our web site so many times. And with the constant feedback, we now have an understanding of the web space’s activity and an added sense of awareness.

Accountability –

This prototype logs hostnames and IP addresses. So for the most part, individuals are not held accountable for their browsing patterns, because most of the time, it is not easy to connect a person with a hostname. Moreover, the server is not held accountable for its logging practices because that fact is never revealed to the viewers. Visitors do not know that the web page owners can see what they are viewing. Thus this does not create the sense that you-know-that-I-know-that-you-know. While the owners may know the visitor’s activities, no social norms and values are brought in to govern actions of the visitors. Only the owners’ actions are changed, as we will see in the next section.

Change –

We decided it was time to change our group’s website. However, like many other research groups, our list of things to do is long and our time limited. The WSLM was presented to the group as a proof of concept. After many weeks, the WSLM reflected the history of our group’s website back to us. Now that we have a better understanding of the system, we can shape it through changing the content of the site (social) or adding passwords (technical) or do nothing at all. Because of a bug we later found, this Privacy Mirror told us that no one was visiting our group’s site. Believing in the Privacy Mirror, we changed our behavior and decided that it was acceptable to do nothing for a while and delay the update of the group’s site.

In this case, even though it was erroneous, the Privacy Mirror did change behaviors.

6 Discussion

Privacy Mirrors and their history, feedback, awareness, accountability, and change have been greatly influenced by prior research in privacy policies, media spaces, social translucent systems, as well as environmental psychology. One greater goal for Privacy Mirrors is to bring "physics" to ubiquitous computing. We want to create "worlds that give concrete existence to abstract entities operating according to a physics of our choice." [10]

Humans can be quite adept at reading the environment. In a physical setting, people are good at estimating how far their voice can travel and change their activity or conversation accordingly. In the current digital environments, there's no way to tell how far a person's voice or other personal/private information may flow. What if the architecture of the physical environment is incorporated to show sensing and computation? How can displays and cues of data collection and processing be a part of the architecture as bay windows and kitchen islands are a part of a house? When done right, the physical world provides what Erickson and Kellogg termed *social translucent systems* [7]. That is, systems in which humans interact gracefully with each other because people and their activities are visible to one another.

Because of exposure to everyday space, socially accepted expectations in physical space have developed. When people enter a restaurant, people become instantaneously aware of the space. They know how to act and behave depending on the environment. There are formal restaurants and there are Burger Kings, but most people act accordingly in the appropriate place. In a well-designed restaurant, people will know where the restrooms are without needing to ask. In a dance club, people are "persuaded" through the architecture and interior design to gather at the bar, to dance on the dance floor, or to sit at booths and tables. The design of the space tells people where to dance, where to drink, and where to talk (or rather to shout).

This is about being aware of the place, understanding the place, understanding the physics of the place (dancing is appropriate on the parquet floor and not so appropriate on the carpet), and having the society agree to expectations for that place.

In the digital world, we are gods. We create our own physics. We can create our own models for history, for wear, for any aspect of physics. We agree with Hill and Hollan; it is "crucial to emphasize that the physics can be motivated by understandings of the characteristics of cognition and tasks." The physics of the new space should help people in the process of recognition, prediction, evaluation, and action.

Because we design the underlying physics model, we can imbue the model with characteristics not found in the real world. For example, in the real world, it is difficult to manage the traces we leave as we traverse the world. Once we wear down a book, it is difficult to take back that "wear." However, in the digital world, if we, the designers, wanted a digital world in which we could manage our traces, in which we could take back the traces we left behind, it would only be a matter of design and implementation.

With a consistent physics model, all users will share and experience the same model. People will work together better when they share the same model. They will all have similar understandings of the features and constraints of the system. They will share similar expectations from the system.

Through understanding the physics and the history of a space, people will understand and know what is appropriate for the space they happen to be in, even if that space does straddle the technical, social, and physical worlds.

What we will have are not just Privacy Mirrors, but Mirrors, in general, to understand and shape the system, whether for privacy, productivity, or entertainment.

7 Conclusion

To conclude, privacy is a known issue in ubicomp [17], exasperated by an oft-cited feature of ubicomp — invisibility [31]. Adding to the complexity, ubicomp systems are inherently socio-technical, spanning three environments: social, technical, and physical. Ubicomp, like media spaces, is socio-technical in nature and is embedded within social and cultural contexts. To address privacy issues and solutions in only one environment (be it social, technical, or physical) is inappropriate and imprudent [2][5].

We have introduced Privacy Mirrors, a framework for designing socio-technical ubiquitous computing systems. Privacy Mirrors help users understand the socio-technical system and consequently be able to shape it to fit the users' privacy needs. Enabling a system for understanding and shaping brings to the foreground and makes visible the flow, state, and history that once had been in the background and invisible. Further, understanding and shaping the system not only helps resolve privacy issues, but will also allow people to make sense out of the world around them, to effectively and confidently incorporate the system into their needs, practices, values, and sensibilities. It makes for both a usable system and useful system.

8 Acknowledgment

This work is partially supported by an NSF HCI Traineeship and a Sloan Foundation Grant. We would like to thank Anind Dey, Carlos Jensen, danah boyd, Joe Tullio, Karrie Karahalios, Khai Truong, Mark Guzdial, Xin Wei Sha, and the members of the ECL for their thoughtful comments on the research and writing of this paper.

9 References

1. Abowd, G. D. "Classroom 2000: An experiment with the instrumentation of a living educational environment." IBM Systems Journal 38(4) (1999) 508-530.
2. Bellotti, V. and Sellen, A. Designing for Privacy in Ubiquitous Computing Environments, In the Proceedings of ECSCW `93. Milan, Italy. September 1993.
3. Bradner, E., Kellogg, W., Erickson, T. The Adoption and Use of "Babble": A Field Study of Chat in the Workplace. In Proceedings of the 6th European Conference on

Computer Supported Cooperative Work (ECSCW’99). Copenhagen, Denmark. September 12-16, 1999. pp. 139 - 158. (1999).

4. Deitz, P. and Yerazunis, W. Real-Time Audio Buffering for Telephone Applications. In the Proceedings of UIST'01 Orlando, Florida. (2001).
5. Dourish, P. 1993. Culture and Control in a Media Space. In Proc. Third European Conference on Computer-Supported Cooperative Work ECSCW'93 (Milan, Italy). Dordrecht: Kluwer. (1993).
6. Dourish, P., Adler, A., Bellotti, V. and Henderson, A. Your Place or Mine? Learning from Long-Term Use of Audio-Video Communication. Computer-Supported Cooperative Work, 5(1): 33-62. (1996).
7. Erickson, T. & Kellogg, W. Social Translucence: An Approach to Designing Systems that Support Social Processes. ACM Transactions on Computer-Human Interaction, 7, 1, 59-83. (2000).
8. European-Commission, Directive 95/46/ec of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to Processing of Personal Data and on the Free Movement of Such Data. November 1995.
9. Grudin, J. 1994. Groupware and Social Dynamics: Eight Challenges for Developers. Communications of the ACM, 37, 1, 92-105.
10. Hill, W.C. and Hollan, J.D. History-enriched digital objects, Third ACM Conference on Computers, Freedom and Privacy, San Francisco, CA, ACM, 917-20. (1993).
11. Hindus, D. and Schmandt, C. Ubiquitous Audio: Capturing Spontaneous Collaboration. In the Proceedings of Computer Supported Collaborative Work 1992 Toronto, Canada.
12. http://www.smartmoney.com/marketmap/
13. Ishii, H., and B. Ullmer. Tangible Bits: Towards Seamless Interfaces between People, Bits and Atoms. In CHI'97, pages 234 - 241, 1997.
14. Johnson, B., Shneiderman, B. Treemaps: a space-filling approach to the visualization of hierarchical information structures Proc. of the 2nd International IEEE Visualization Conference (San Diego, Oct. 1991) 284-291.
15. Kaplan, S. and Kaplan, R.. Cognition and Environment: Functioning in an Uncertain World. 1982. Praeger Publishers.
16. Krackhardt, D. The Ties That Torture: Simmelian Tie Analysis in Organizations. Research in the Sociology of Organizations 16:183-210. 1999.
17. Langheinrich, M. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In Ubicomp. 2001.
18. Lau, S. The Hong Kong Personal Data (Privacy) Ordinance. Computers, Freedom, and Privacy 2000. Toronto, Ontario, Canada, April 4-7, 2000.
19. Norman, D.A. The Design of Everyday Things. Doubleday, New York, 1990. Originally published as `Psychology of Everyday Things'
20. Ornstein, R. and Ehrlich, P. New World New Mind: Moving Toward Conscious Evolution. 1990. Touchstone Books.
21. Palen, L. Social, Individual & Technological Issues for Groupware Calendar Systems, in the Proceedings of CHI’99 (Pittsburgh PA, May 1999), ACM Press, 17-24
22. Pedersen, E. R., K. McCall, et al. Tivoli: An Electronic Whiteboard for Informal Workgroup Meetings. In the Proceedings of ACM INTERCHI '93, Amsterdam, The Netherlands (1993) 391-398.
23. Rhodes, B. J. (2000) Margin Notes: Building a Contextually Aware Associative Memory, In Proceedings of Intelligent User Interfaces (IUI '00,) ACM, New Orleans, LA USA, pp. 219-224.

24. Richter, H., G. D. Abowd, et al. Integrating Meeting Capture within a Collaborative Team Environment. In the Proceedings of Ubicomp 2001, Atlanta, GA (2001).
25. Rosen, J. The Unwanted Gaze: The Destruction of Privacy in America. 2000. Random House.
26. Shneiderman B. The Eyes Have It: A Task by Data Type Taxonomy for Information Visualizations, In Proceedings IEEE Visual Languages, pages 336-343, Boulder, CO, Sept 1996.
27. Skog, T. and Holmquist, L.E. WebAware: Continuous Visualization of Web Site Activity in a Public Place Student poster presentation, Computer-Human Interaction 2000, April 1-6, The Hague, The Netherlands.
28. Stifelman, L.J. The Audio Notebook. Ph.D. Thesis, Media Laboratory, MIT (1997)
29. Tullio, J., Goeckes, J., Mynatt, E.D, and Nguyen, D.H. Augmenting Shared Personal Calendars. Submitted to UIST'02 Paris, France.
30. Viégas, F. and Donath, J. PostHistory: Visualizing Email Networks Over Time. Proceedings of the International Sunbelt Social Network Conference XXII. New Orleans, USA, February 13-17, 2002.
31. Weiser, M and Brown J. S., "The Coming Age of Calm Technology," Beyond Calculation: The Next Fifty Years of Computing. P. Denning and R. Metcalfe, Editors, Springer-Verlag, Inc., New York (1997).