Designing for Ubiquity: The Perception of Privacy

Can users offer informed consent when they don't understand a technology or forget that it exists? These were among the issues that emerged in a real-world study of ubicomp users.

Richard Beckwith
Intel Research

Ubicomp researchers have long argued that privacy is a design issue,[1] and it goes without saying that successful design requires that we understand the desires, concerns, and awareness of the technology's users. Yet, because ubicomp systems are relatively unusual, too little empirical research exists to inform designers about potential users.

Complicating design further is the fact that ubicomp systems are typically embedded or invisible, making it difficult for users to know when invisible devices are present and functioning.[2] As early as 1993, ubicomp researchers recognized that embedded technology's "unobtrusiveness both belies and contributes to its potential for supporting potentially invasive applications."[1] Not surprisingly, users' inability to see a technology makes it difficult for them to understand how it might affect their privacy. Unobtrusiveness, nevertheless, is a reasonable goal because such systems must minimize the demands on users.[3]

To investigate these issues further, I worked with Scott Lederer to conduct an ethnographic study of what we believe is the first US eldercare facility to use a sensor-rich environment.[4] Our subjects were normal civilians (rather than ubicomp researchers) who lived or worked in a ubiquitous computing environment. We interviewed residents, their family members, and the facility's caregivers and managers. Our questions focused on how people understood both the ubiquitous technology and its effect on their privacy. Although the embedded technology played a central role in how people viewed the environment, they had a limited understanding of the technology, thus raising several privacy, design, and safety issues.

Research context

There are two main types of ubiquitous systems: *personal systems*, which are independent of physical location, and *infrastructure systems*, which are instrumented locations.[2] The technology we studied is an infrastructure system. It consists of sensors and other technologies that are deeply embedded in buildings and in the surrounding campus to monitor the people who live and work there.

Ubicomp technologies

The facility's ubicomp system uses *programmable logic controllers* throughout public and private areas to control lighting, overhead fans, heating, ventilation, and air conditioning. Although standard controls such as light switches appear to offer direct control, they actually send a signal to one of the PLCs. In addition:

- A central server monitors the state of each device.
- Switches on every door continuously monitor whether they are open or closed.
- Stationary movement sensors in both public and private areas measure and record human movement in every room (see Figure 1).

Published by the IEEE CS and IEEE ComSoc ■ 1536-1268/03/$17.00 © 2003 IEEE

Figure 1. A typical view of a resident's ceiling, which includes a smoke alarm, IR sensor, sprinkler heads, and track lighting. All rooms also have monitoring switches on doors and stationary movement sensors. Although some features, such as the track lights, have wall switches, they are controlled through programmable logic controllers.

- Load cells on the beds monitor residents' weight and movement.

Finally, and most apparently, all residents and staff wear badges with unique IDs (see Figure 2). These mobile badges broadcast the ID in infrared for indoor location monitoring and in radio frequency for outdoor, on-campus location monitoring. Badges also include a call button that sends IR and RF signals.

The facility stores data from each of these sources in perpetuity.

Methodology

In addition to informal observations, we derived much of the research we report here from semistructured interviews with people who create and consume the data collected at the eldercare facility. We conducted 29 interviews over several months; our subjects included:

- Ten family members of residents (focusing on those who made decisions about the resident's care)
- Nine residents (with varying levels of dementia)
- Eight direct-care staff
- Two facility managers

In the interviews, we asked participants a set of core questions about a range of issues, from their daily routines to how they selected this facility (to live or work at) to their views of possible future technologies. Our goal was to uncover not only how people viewed the ubicomp technology, but also to investigate what additional technologies they might find useful. Among the facility's existing technologies, we focused more closely on the badges and load cells as they were the most obvious. But, despite the fact that many of the other technologies were invisible, everyone we interviewed viewed the environment as an instrumented space.

Figure 2. A mobile badge that broadcasts identification in infrared for indoor location monitoring and in radio frequency for outdoor, on campus location monitoring.

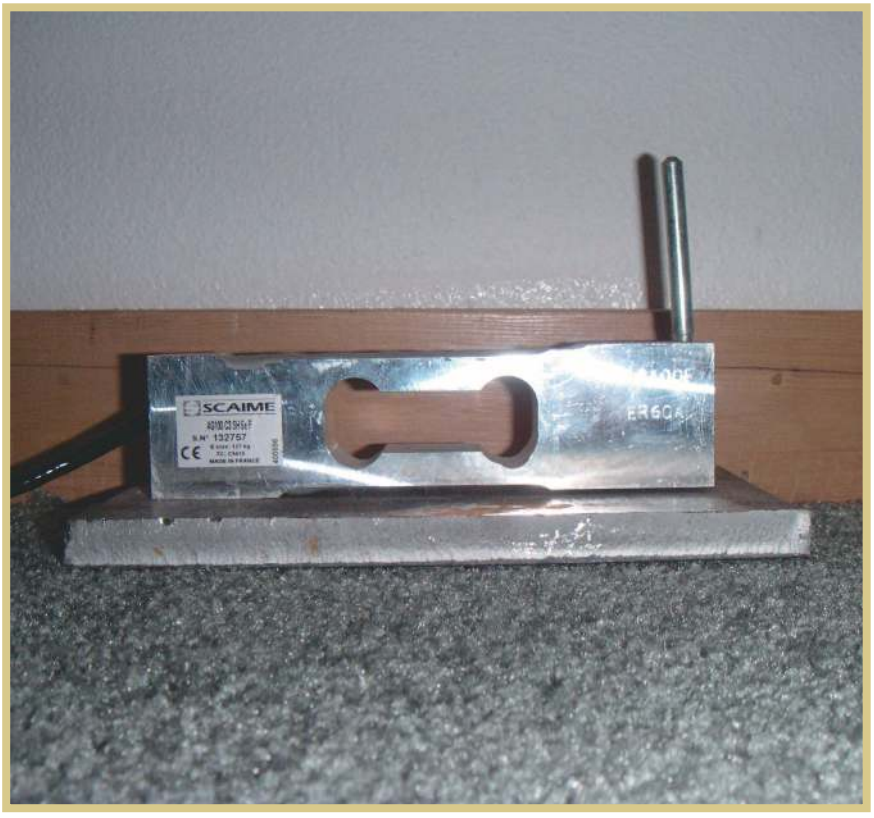

Figure 3. A load cell. The facility attaches a load cell to each bed leg to monitor residents' weight.

User perceptions of technology

User perceptions of risk and benefit can determine their willingness to adopt technology. In fact, research has found that people are more likely to accept potentially invasive technology if they think its benefits will outweigh its potential risks.[1] In our study, however, when participants discussed their analysis of the risk and benefits, they didn't mention (or seemingly consider) the technology's actual risks and benefits. They essentially viewed the technology as a "black box" with limited inputs and outputs.

Badge technology

Because all staff and residents must wear badges on the outside of their clothing, it is the most overt and the best understood of all the technologies. However, many people appeared to be unaware of the extent of the badge's monitoring capabilities. Therefore, we shouldn't take "best understood," to mean "well understood."

Residents view the badge technology as a call system and most believe that this is its sole function. However, the badges also track the location of all residents and staff on campus, which makes various interventions possible. If certain residents are at the stove alone, for example, the system shuts off the gas. The service also alerts the staff if certain residents leave the building. Residents are not aware of such uses, which isn't surprising: the system has no user interface for location-based badge functions, and thus such functions are invisible to residents.

The staff is aware of location tracking. In fact, facility managers study location data to see where employees spend their time and then suggest different strategies for using that time. Still, the staff's understanding of the technology is not great. One worker suggested that people might get away with a longer cigarette break by taking off the badge and leaving it in the kitchen before going outside. Such a strategy suggests a limited understanding of the environment: Even without the badge, motion sensors would detect workers moving through the space and door sensors would detect them leaving the building.

Load cells

As Figure 3 shows, the facility's load cells are large metal units that are fairly conspicuous. Load cells are installed on each leg of the residents' beds, primarily to track trends in weight gain or loss over time. Such trends are a significant heuristic for health, and the government requires that facilities collect weight data on every resident and note significant changes. Still, residents do not understand the load cells; one resident thought their purpose was to warm up the bed.

Like the badges, the facility can use load cell data in ways that residents do not clearly understand. Staff members might, for example, use load cell data to determine when residents leave their bed during the night. This capability is in place now. Other uses are also possible. For example, the load cells can gauge fitfulness in sleep. If the data indicates significant, uncommon movement during the night, the caregiver might investigate whether the person is having trouble sleeping. (At this point, actual sleep monitoring isn't in place, but it is in development. Once the application is implemented, residents' families will be able to view sleep patterns by tunneling into the network on the Web.)

Reasoning about privacy

To analyze users' privacy risks, we used a model that borrows freely from Anne Adams.[5,6] In particular, we focused on three aspects of personal information that Adams found determined people's reasoning about privacy:

- *Information receiver*. Who will use or have access to the data?
- *Information usage*. How will the information be used, and what do I stand to gain and lose from its use?

- *Information sensitivity*. How sensitive is the data?

The interplay of these three subjective aspects determines how people perceive privacy and potential violations.

Information receiver. Some of the more straightforward aspects of our results involve the information receiver, or "who monitors whom." In terms of monitoring, residents are clearly the focus. Also, management monitors caregivers' locations. Managers also wear badges, but no one regularly consumes that data.

In terms of data consumption, the caregivers are the main consumers, but management, family, and health providers can also consume residents' data. Most of the people we interviewed were unaware of this, however, and the data has rarely, if ever, been shared.

Information usage. In this case, how people use the information is more complicated than who receives it. The system was installed with a general purpose in mind: Gathering data to enhance the residents' lives. Everyone involved—the residents, family, caregivers, and managers—are aware of this goal and accept it as truth. How this goal is reached, however, and how the target information is used, is somewhat cloudier.

Data fusion raises a particularly insidious set of problems. Data from various sensors can be merged to yield second-order data, such as what time a resident entered his room, who entered with him, and what movements (and, to some extent, activities) occurred thereafter. For residents involved in campus romances, for example, load cell data could prove embarrassing. Data fusion is a general problem. It's difficult to imagine various uses for fused data when you don't even consider that a fusion could take place.

Although the facility has protections against some problems, nefarious activities are still possible. Load cell data indicating that residents are sleeping could leave them vulnerable to theft, for example, as could data indicating that their rooms are empty. For obvious reasons, this particular facility has been quite careful with data access. We must encourage designers of vulnerable ubicomp systems to be equally cautious, especially in cases where typical users are unlikely to understand the technology.

Information sensitivity. Information sensitivity, of course, is a function of what information is shared. In this case, the information includes the person's physical location: data consumers can determine with a fair degree of accuracy where people are on campus. They can also determine who they're with. Such data would be generally considered quite sensitive, but in this study we found that people's lack of understanding of the technology rendered them unable to judge.

One resident summed up the general consensus when he said that the badge's purpose is so that "someone can come and help." As we noted earlier, the load cells are equally misunderstood.

Privacy and unawareness: Research implications

In part, user ignorance of technology is a direct result of the double-edged sword of "distraction-free" computing.[7] In this case, the facility owners introduced the technology to simplify and improve the lives of both staff and residents, not to complicate them. Nonetheless, reliable, inconspicuous sensing of personal information is problematic because users do not always understand the extent or methods of data collection and thus cannot adequately evaluate privacy issues.

Distributed misunderstanding

How important is this lack of understanding? In our study, it's perhaps unrealistic to expect residents of a care facility to fully understand the technology and make decisions about privacy and data sharing. Most of this facility's residents do have conservators with power of attorney who could make such decisions for them. Unfortunately, we did not find a greater awareness of the technologies among the family members and conservators with whom we spoke.

Family members we interviewed seemed to know only that the technologies are there for the residents' well being; they did not understand what data was being collected to this end. They stated clearly that they wanted to balance their loved one's privacy with a better quality of life. However, they rarely actually considered their loved one's privacy needs. One family member, for example, said

> *Those kinds of [technologies] can help you live a life that's a little bit more independent than would be otherwise. I see it as very positive. The risk of somebody having the information about your being monitored in such a way? I guess I am not sure what risk there is, except embarrassment. And when you get to be 80 years old, you don't embarrass that easily anymore anyway.*

Another family member said that the technologies had no effect on privacy but then added, "[but I] don't know the possibilities."

Reliable, inconspicuous sensing of personal information is problematic because users do not always understand the extent or methods of data collection.

Caregivers also lack understanding of the technology. Many do not understand potential uses for the various data beyond the simplest functions, such as finding a resident. They rarely considered any function beyond responding to call buttons. When asked about how she thought about privacy, one caregiver said, "You trust it because that's what you have."

The bottom line is that the people mak-

Related Research

Although large ubiquitous computing deployments have only begun to include "civilian" participants, researchers have continually investigated various aspects of privacy and data sharing that are important in a real-world context. Web services research has offered relevant work, as has work using thought experiments or ubiquitous technology deployments within technologically savvy research facilities.

Web standards and practices

There are two primary standards for collecting personally identifiable information on the Web: TRUSTe and Platform for Privacy Preferences (P3P). Corporations must meet TRUSTe's set of requirements to post a TRUSTe certification on their site (www.truste.org/webpublishers/TRUSTE_ License_Agreement_Schedule_A_7.0.doc). According to the organization, TRUSTe "enables individuals and organizations to establish trusting relationships based on respect for personal identity and information." Notice and consent are central to TRUSTe's vision of privacy and control. The technology's guiding principles are as follows:

- A Web site must have a posted privacy policy.
- The policy must include "notice and disclosure" of collection and use practices.
- Sites must give users choice about and consent over how their data will be used.
- Sites must implement data security measures.

The World Wide Web Consortium's P3P provides a specification for Web services aimed at the development of client applications (such as browser plug-ins) that facilitate the establishment of user privacy preferences. With P3P tools, users can set up preferences that the system automatically compares against a Web site's privacy policy. If that policy conflicts with their preferences, users get a message warning them of the incompatibility. Thus, P3P automates aspects of the standard notice and consent procedure.

P3P researchers have also investigated how to build user interfaces for Web sites.[1,2] Mark Ackerman and Lorrie Cranor note the challenges privacy poses for human–computer interaction, because programs must "present an extremely complex information and decision space" and do so seamlessly, without interfering with events in the environment.[2] For these reasons, they propose that the system borrow settings from earlier (similar) events or that users establish preferences a priori. Ackerman and his colleagues surveyed hundreds of users and found that automatic data transfer, without user notification, was among the least attractive of all scenarios.[3] Yet, this finding conflicts with the need for users to set preferences seamlessly and without a distracting interface.

Beyond the Web

Although standards are leading us toward transparency for e-commerce and various other Web activities, they don't necessarily extend to ubiquitous computing and monitoring. The standard regime of notice and consent, which is the backbone of many privacy and security standards, falls apart in the ubicomp domain; matters are further complicated in that we remove informed consent from the data collection point.

Privacy research in ubiquitous computing in general, and location privacy in particular, addresses some issues that fall outside the Web-based privacy realm. Victoria Bellotti and Abigail Sellen argue that appropriate feedback and control levels could preserve privacy in ubiquitous computing.[4] Obviously, feedback is difficult in a ubiquitous computing environment—imagine multiple environmental sensors notifying everyone in a room of surveillance with each occurrence, for example—and real-time control can be difficult without an input device. Still, if well designed, more limited feedback and the use of default control parameters might offer considerable protection.

Recent location-privacy research offers our most reasonable shot at solving the control problem.[5–7] Like P3P, this work seeks to min-

ing the decisions do not always know who is consuming the information, how sensitive the data might be, or even what it might be used for.

In the case of embedded sensor technologies, it would be practically impossible to teach anyone the system's full implications. With data fusion from various sources becoming increasingly possible, we can imagine any number of unintended consequences that would further complicate the issue. As our study's context shows, the caregivers and family members who interact with the system and make decisions that might compromise residents' privacy do not sufficiently understand the potential consequences. They simply trust the system to be benign. In this case, the system is benign, but such trust should be cautiously granted. Users' full understanding of the system—and thus a well-reasoned trust—is likely impossible, even when system operators train users about the issues.

Designing for privacy

Given the facility's residents and that a residential care facility differs dramatically from the outside world, generalizing our findings to other ubicomp deployments might be questionable. We believe, however, a generalization is warranted because the staff and family were no better prepared

imize user interactions by automating privacy policy decision making. The systems are based on machine-readable privacy policies; they store users' privacy preferences and apply them when decision-making situations arise.

However, in a situation such as the one in our study, a slight problem emerges. Notice mechanisms that might work with many systems, such as a cell phone-based system for people moving within a given city, would not likely work in a home or workplace setting. For example, Marc Langheinrich proposes a "privacy beacon," a short-range wireless link that constantly announces the privacy policies of the service.[7] This might work when users are constantly entering and leaving regions with varying policies, as new negotiations could ensue at each service threshold based on the users' preferences. Our users tended to stay in one place, however, and they had a very different problem: They forgot the system existed.

In monitoring situations, users might even forget what they have consented to[4] and behave in ways they never thought they would. Consider, for example, the use of monitoring cameras. Although many people believe video cameras are at least somewhat invasive, researchers have found an interesting phenomenon: People forget that the camera is on them. This is considered a benefit for researchers, who can collect more naturalistic data. One researcher, for example, noted that "…eventually the camera operator disappears into the woodwork. Children, for example, forget about the camera and display the behavior of daily life. The anthropologist can then collect a visual transcription of normal existence.[8] And this doesn't hold only for children: Researchers have also found that subjects in workplace studies quickly forget about the camera.[9]

These findings raise many questions. If people forget about cameras, what kind of feedback can overcome this? How can we assume that notice and consent is an effective way for users to preserve their privacy? Can subjects or users give informed consent when we're depending on them to forget that we're collecting data? If people forget about video camera observation—where data collection is overt—what kind of consent is possible from someone being monitored by "distraction free" technology?

REFERENCES

1. M. Ackerman, L. Cranor, and J. Reagle, "Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences," *Proc. ACM Conf. E-Commerce,* ACM Press, 1999, pp. 1–8.
2. M. Ackerman and L. Cranor, "Privacy Critics: UI Components to Safeguard Users' Privacy," *Proc. ACM Conf. Human Factors in Computing* (CHI 99), ACM Press, 1999, pp. 258–259.
3. A. Adams and M.A. Sasse, "Privacy in Multimedia Communications: Protecting Users Not Just Data," *Joint Proc. Human-Computer Interaction/Interaction d'Homme-Machine* (IMH-HCI 01), 2001, Springer- Verlag, pp. 49–64.
4. R. Bellotti and A. Sellen, "Design for Privacy in Ubiquitous Computing Environments," *Proc. 3rd Euro. Conf. Computer Supported Collaborative Work*, Kluwer, 1993, pp. 77–92.
5. G. Myles, A. Friday, and N. Davies, "Preserving Privacy in Environments with Location-Based Applications," *IEEE Pervasive Computing*, vol. 1, no. 1, Jan.–Mar. 2003, pp. 56–64.
6. M. Langheinrich, "Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems," *Proc. 3rd Int'l Conf. Ubiquitous Computing*, Springer-Verlag, 2001, pp. 273–291.
7. M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments," *Proc. 4th Int'l Conf. Ubiquitous Computing*, Springer-Verlag, 2002, pp. 237–245.
8. E. Covington, "The UCLA-Sloan Center Studies the Everyday Lives of Families," *UCLA Inquiry: News from the Humanities and Social Sciences Division*, Univ. California, Los Angeles, 2002; www.celf.ucla.edu/news2.html.
9. M. Summers, G. Johnston, and F. Capria, "Don't Tell Me, Show Me: How Video Transforms the Way We Analyze and Report Data from Field Studies," *Proc. 11th Conf. Humanizing Design,* Usability Professionals' Assoc., 2002; www.upassoc.org/new/conferences/2003/downloads/dont.tell.pdf.

to make privacy decisions. Moreover, existing efforts in the literature validate our results (see the "Related Research" sidebar). Some existing work might help solve some of the problems we encountered, though not others—such as people forgetting they were being monitored—which many different settings will likely share and researchers have yet to resolve.

In a recent study, wireless provider Omnipoint reported that 20 percent of its users regularly lied about their location while on their cell phones.[8] Clearly, some people do understand the desirability of keeping their location private. However, many people assume that sharing personal data such as location is only a problem for those involved in wrongdoing. As a caregiver in our study put it, "[privacy] only matters if you're not doing what you're supposed to." In many ways, users think that if you want to ensure your privacy, you have something to hide. Obviously, these people have not thoroughly considered how data might be used. As systems designers, we must keep that fact in mind.

Wisely or not, users trust system designers to protect them from these unintended consequences. Yet unanticipated data use is rife with problems for privacy and security. Anderson describes design-based solutions of this sort as "inference control."[9] Restricting data use and keeping the num-

ber of potential consumers low can approach a solution to this problem.[9,10]

Researchers have suggested various algorithms—including Bayesian networks, reinforcement learning, and neural networks—for developing trending information from sensor data. Although such analysis requires raw data, systems vary in how long they need raw data to be saved. Algorithms that let operators delete raw data as soon as possible might better protect privacy. We must keep in mind that particularly sophisticated algorithms can negatively impact a person's ability to understand what the system does[1] and thereby be a barrier to intelligent decision making about risks the system poses.

Because users trust systems to be benign, we must set conservative default states. Such defaults must be easily understandable and well defined,[3,10] so that users can depend on them to protect their data. Establishing user profiles (that users can modify) lets them reveal personal data in exchange for desirable services. The user, or users' proxy, must be able to do this easily, with as full an understanding of the consequences as possible.

Furthermore, as researchers, we must consider the ramifications of intruding on or distracting users to get them to renew informed consent. Given general human forgetfulness, we might need something that requests continued user consent even after surveillance has begun. Because of the data collection's unobtrusiveness, users forget they're being watched. We might use an intelligent system to determine opportune times to remind them of this. My colleagues and I are currently trying to understand how best to design these "jack-in-the-box" interfaces.

The arguments here are not meant to discourage designers from exploring ubicomp. Quite the contrary, ubicomp systems will allow numerous services that will enhance many users' lives. However, we must be cautious in designing such systems, to merit the trust that many users have already put in our hands. P

the AUTHOR

Richard Beckwith is a senior research psychologist in the People and Practices Research Group at Intel Research. His current research interests are in examining the human side of wireless technology innovations. He has a PhD in developmental psychology from Columbia University. Contact him at JF3-377, 2111 NE 25th Ave., Hillsboro, OR, 97124; richard.beckwith@intel.com.

ACKNOWLEDGMENTS

I thank the staff and residents of the assisted living facility where we did our research. Scott Lederer, now a student at UC Berkeley, collected data and did the early analyses. I also thank Miriam Walker and Sunny Consolvo of Intel Research Seattle who helped with data collection; Olivia Laing, who read and edited an early and difficult version of this paper; and the reviewers, who gave invaluable feedback and pointers to related work.

REFERENCES

1. R. Bellotti and A. Sellen, "Design for Privacy in Ubiquitous Computing Environments," *Proc. 3rd European Conf. Computer Supported Collaborative Work*, Kluwer, 1993, pp. 77–92.
2. R. Want et al., "Disappearing Hardware," *IEEE Pervasive Computing*, vol. 1, no. 1, Jan.–Mar. 2002, pp. 36–47.
3. G. Myles, A. Friday, and N. Davies, "Preserving Privacy in Environments with Location-Based Applications," *IEEE Pervasive Computing*, vol. 1, no. 1, Jan.–Mar. 2003, pp. 56–64.
4. R. Beckwith and S. Lederer, "Designing for One's Dotage: Ubicomp and Residential Care Facilities," Conf. Home-Oriented Informatics and Telematics (HOIT 03), Center for Research on Information Technology and Organizations, 2003; www.crito.uci.edu/noah/HOIT.
5. A. Adams, "Users' Perception of Privacy in Multimedia Communication," *Proc. AMC Conf. Human Factors in Computing* (CHI 99), ACM Press, 1999, pp. 53–54.
6. A. Adams and M.A. Sasse, "Privacy in Multimedia Communications: Protecting Users Not Just Data," *Joint Proc. Human-Computer Interaction/Interaction d'Homme-Machine* (IMH-HCI 01), Springer Verlag, 2001, pp. 49–64.
7. D. Garlan et al., "Project Aura: Towards Distraction-Free Pervasive Computing," *IEEE Pervasive Computing*, vol. 1, no. 2, Apr.–June 2002, pp. 22–31.
8. A.M. Townsend, "Life in the Real-Time City: Mobile Telephones and Urban Metabolism," *J. Urban Technology*, vol. 7, no. 2, 2000, pp. 85–104.
9. R.J. Anderson, "Privacy Technology Lessons from Healthcare," *Proc. IEEE Symp. Security and Privacy*, IEEE CS Press, 2000, pp. 78–79; www.truste.org/webpublishers/TRUSTE_License_Agreement_Schedule_A_7.0.doc.
10. M. Langheinrich, "Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems," *Proc. 3rd Int'l Conf. Ubiquitous Computing*, Springer Verlag, 2001, pp. 273–291.

For more information on this or any other computing topic, please visit our Digital Library at http://computer.org/dlib.