Privacy has been an important topic in ubicomp research for many years. Indeed, it was technological change that first triggered Samuel Warren and Louis Brandeis to fear of a world without privacy,1 when, in 1888, George Eastman presented the “Kodak snap camera.” This invention suddenly made photographic equipment portable and gave rise to the new “paparazzi” profession. Pervasive computing, with its multitude of sensors, ability to derive complex life situations (“context”) from raw data, and “cradle to grave” coverage of our lives, goes beyond even the wildest dreams of Warren and Brandeis.

UNDERSTANDING PRIVACY

Much has been written about privacy, yet simple definitions, such as “the right to be let alone,”2 hardly serve as a useful working model for today’s complex information flows. Yet complex scholarly discussions (such as privacy rights as property rights3) are often difficult to put into practice—especially for an engineer not schooled in the finer points of philosophical or legal debate.

Early work on computer privacy, mostly in the area of communication networks and databases, focused largely on general security issues—that is, confidentiality and access control. As Mark Weiser pointed out, “The [social] problem [associated with ubiquitous computing], while often couched in terms of privacy, is really one of control.”4 Yet “control” isn’t that easy to implement in a world full of sensors and smart devices.

Over time, researchers have realized that even simple problems—for example, controlling which website gets to place a cookie on my hard disk—are frustratingly difficult to get right, and most users don’t bother with using controls that are provided. Following legal practices, such as the Fair Information Principles, offers some guidance to the “default” behavior of smart environments,5 but falls short of explaining what and when to record and with whom to share data. Leysia Palen and Paul Dourish’s work on “unpacking” privacy for a networked world offers a much richer theory of privacy, illustrating the “dynamic and multidimensional nature of privacy.”6

There’s no silver bullet or “one size fits all” solution. We need to “fit” technology into cultural practice to support privacy’s role of “resolving tension” between various boundaries—such as between privacy and publicity, the self and others, and our past and future.

THE CHALLENGE OF PRIVACY BY DESIGN

The idea of privacy by design—that is, incorporating privacy principles at design time rather than as an afterthought—was proposed in the 1990s by Ann Cavoukian,7 Abigail Sellen and her colleagues’ work on the “Whereabouts Clock” beautifully illustrates how privacy can become an active design ingredient.8 First, they created a wall clock that could only be seen by people in the home—supporting implicit and intuitive “access control.” Then, they purposefully made it coarse grained to show if people were at home, work, or school (in line with users’ actual
Technology—and thus computing—is information needs) instead of simply showing detailed coordinates on a map. Finally, their wall clock design made it a shared, reciprocal tool, rather than a parental control element.

Privacy by design, combined with a rich understanding of an application’s individual context in actual use practices, is an approach that enables (in principle) the design of ubicomp systems that begin to address the problems of protecting user privacy. However, such an inherently contextual design process represents a major undertaking and could be error-prone. Recent work by Sarah Spiekermann and Lorrie Cranor aims to make privacy by design easier for “the rest of us” by packaging privacy theories and legal approaches into concrete guidelines.9

However, this still falls short of what a real contextual design could accomplish. One of the key problems for many engineers has also been the elusive, definition-resistant nature of privacy. Some have tried to make privacy more “engineerable” by quantifying it—true to the old adage, “you can’t manage what you can’t measure.” Although this has been favorably received in security circles, designers have questioned such attempts to obtain “universal answers in terms of people’s ‘general’ privacy practices.”10

Maybe what’s truly holding up the widespread adoption of privacy by design in both ubicomp and beyond is a lack of awareness and responsibility among those who build such systems. Early work in the context of the EU’s Disappearing Computing Initiative showed that many researchers in the field had given up on privacy, saw it as a road-block, or simply assumed that someone else would take care of it.11 Recent large-scale surveys among IT professionals regarding their views on IT surveillance echo these findings.12

THE FUTURE
Technology—and thus computing—is intimately connected with privacy. As technology changes and makes new things possible (such as a portable camera that lets people take a snapshot of others), we need to re-evaluate (or make explicit) the value we give certain aspects of our lives. Google Glasses, for example, could be a game changer. How do we balance people’s desire to use Google Glass to share their daily activities in high definition with others, versus our desire not to be recorded in public? Or what about computerized cars that record (and transmit) detailed use logs: should insurers be allowed to offer discounts to those who agree to have all of their travels tracked? What about health insurance discounts for letting insurance companies access to your smart shirt and shoes?

As a community, we’ll face numerous challenges that affect all aspects of system design—from placing controls on what hardware can record to creating user interfaces that let users express their privacy requirements. We’re beginning to understand the problems, but the solutions remain to be discovered.

FEATURE ARTICLES AND DEPARTMENTS
This issue also presents two feature articles on mobile and pervasive systems. In “Context-Based Applications in Converged Networks: Beyond SIMPLE Presence,” the authors tackle the problem of providing generic support for presence applications. This is an important problem that will of interest to anyone building distributed applications that use presence to communicate user states.

While presence information is often explicitly set and communicated by users, the next article, “Extracting Social Semantics from Multimodal Meeting Content,” focuses on a study of extracting social semantics from multimodal meeting content captured with video cameras, microphones, and motion sensors.

We also have a strong selection of departments in this issue. The Conferences department reports on the AutomotiveUI 2012 conference, while the Education & Training department reviews a postgraduate pervasive computing program offered via distance learning at the Hellenic Open University.

Our “Notes from the Community” department offers a curated summary...
Of interesting news and research in pervasive and mobile computing with content drawn from submissions from a shared community on the social news site Reddit, available at www.reddit.com/r/pervasivecomputing.

Next, our Innovations in Ubicomp Products department explores the use of ubiquitous computing in creating new experiences while skiing. Continuing the theme of privacy, in our Smartphones department, we look at the use of personal electronic tokens that can be used to help identify our touches.

Last issue, we successfully relaunched our Pervasive Health department, and in this issue we build on this success with a fascinating look at the evaluation of pervasive systems in health research. The article reports on important experiences gained from conducting a long-term study of the effectiveness of a behavior change applications and contains important insights for anyone engaged in this type of work.

Finally, in our Wearable Computing department, Thad Starner discusses how he got hooked on head-up displays and why he thinks wearable interfaces, such as Google Glass, can help empower users.

Creating a Reviewer Panel

One of the key challenges facing any publication venue is how to ensure a sufficient pool of high-quality reviewers are available to assist in assessing submissions.

To continue to meet the demand for peer review, we’ve decided to create a panel of “recognized reviewers” for IEEE Pervasive Computing. This is a very exciting step for the magazine. Members of this panel perform an invaluable service—agreeing to conduct around four reviews during their two-year term on the panel. Panel members will be appointed after being nominated by the editorial board and will be listed on the Pervasive’s website. We hope to grow this panel over the coming months, so thank you to all those who have accepted our invitation so far.

Finally, a warm welcome to Steve Hodges, who joins the Pervasive’s editorial board as an Associate Editor in Chief. AEICs perform a crucial role for Pervasive, leading the review of all papers in their area. Hodges will be known to many readers for his work on projects such as SenseCam, Gadgeteer, Touch Mouse, and ThinSight. We’re delighted that he’s able to join us.

References