Personal Privacy through Understanding and Action: Five Pitfalls for Designers

Scott Lederer, **Jason I. Hong**
Computer Science Division
University of California, Berkeley
Berkeley, CA USA
{lederer,jasonh}@cs.berkeley.edu

Anind K. Dey
Intel Research Berkeley
Berkeley, CA USA
anind@intel-research.net

James A. Landay
Computer Science and Engineering Dept
University of Washington
Seattle, WA USA
landay@cs.washington.edu

ABSTRACT

People cannot participate in meaningful privacy practices without *understanding* the extent of a technical system's alignment with the relevant practice and without opportunities to conduct discernible social *action* through intuitive engagement of the system. It is a challenge for designers of interactive systems to empower understanding and action through the limited technical mechanisms of feedback and control. To help meet this challenge, we present five pitfalls to avoid when designing interactive systems with personal privacy implications, on or off the desktop. These pitfalls are: obscuring potential information flow, obscuring actual information flow, emphasizing configuration over action, lacking coarse-grained control, and inhibiting existing practice. These pitfalls are based on the literature, on analyses of existing privacy-affecting systems, and on our own experiences designing a user interface for managing privacy in ubiquitous computing. We illustrate how some existing research and commercial systems—our prototype included—fall into these pitfalls, and how some avoid them. We suggest that privacy-affecting systems that avoid these pitfalls can help their users appropriate and engage them in alignment with relevant privacy practice.

INTRODUCTION

One possible explanation for why designing privacy-sensitive[1] systems is so difficult is that privacy simply lives up to its name. Instead of exposing an unambiguous public representation of itself for all to see and comprehend, it cloaks itself behind an assortment of meanings depending on who's watching. When sociologists look at privacy, they see nuanced processes that engineers overlook. When cryptologists look at privacy, they see technical mechanisms that everyday people ignore. When the European Union looks at privacy, it sees moral expectations that American policymakers do not. Amidst this fog of heterogeneous practices, technologies, and policies that characterize privacy, designers of interactive systems face increasing market pressure and a persistent moral imperative to design privacy-sensitive systems.

This article cannot dispel that fog, but it does attempt to shine some light through it by offering a partial set of guidelines for designers of privacy-affecting interactive systems, on and off the desktop. We say "partial set" because this article is not a self-contained how-to guide. We do not mean to imply that systems that follow these guidelines will decidedly support privacy. We *do* mean to imply that systems that *ignore* any of these guidelines without careful rationale face significant risk of disrupting or inhibiting users' abilities to manage their personal privacy. For this reason, we present our guidelines as a set of *pitfalls* to avoid when designing privacy-affecting systems. Avoiding a pitfall does not ensure success, but ignoring one can potentially lead to disaster.

In addition to using our guidelines, designers of privacy-affecting ubiquitous computing systems should consult Bellotti and Sellen's framework for feedback and control [7], Langheinrich's translation of the fair information practices [26], Palen and Dourish's sociologically informed analysis of privacy as boundary negotiation [34], and Jiang *et al.*'s principle of minimum asymmetry [24]. Our work synthesizes some of the core lessons of those frameworks to inform our analysis of common privacy problems we identified across a broad range of existing systems.

Common Design Flaws

There has been a tremendous amount of research on privacy in the context of technical systems. For example, many polls have shown considerable public concerns about privacy on the Internet [12, 39, 40]. There have also been interviews and surveys exploring privacy design issues for context-aware systems [20, 25, 27]; studies exposing privacy perceptions and practices in groupware [33], multimedia environments [2], and location-aware systems [5]; and experiments revealing usability problems affecting privacy in email [44] and file-sharing [18] applications. Despite this abundance of research and design knowledge, many systems still make it hard for people to manage their privacy on and off the desktop.

[1] We will use the term *privacy-affecting* as a general description of any interactive system whose use has personal privacy implications. We will use the term *privacy-sensitive* to describe any privacy-affecting system that, by whatever metrics are contextually relevant, successfully avoids invading or disrupting personal privacy. This article is intended to help minimize the number of privacy-affecting systems that are *not* privacy-sensitive.

We suggest this is because the designs of these systems inhibit peoples' abilities to both *understand* the privacy implications of their use and to conduct socially meaningful *action* through them. We further suggest that designs that avoid our five pitfalls will go a long way towards helping people achieve the understanding and action that personal privacy regulation requires. Although some of these pitfalls may appear obvious, we will demonstrate below that many systems continue to fall into them. Some of these systems have encountered privacy controversies (*e.g.*, web browsers), while others that have avoided the pitfalls have enjoyed considerable commercial or social success (*e.g.*, instant messaging).

Our investigation into these pitfalls began when we fell into them ourselves in the design of a user interface prototype for managing personal privacy in ubiquitous computing environments [28]. Despite the input of our formative interviews, surveys, and literature review, an evaluation indicated a series of fundamental missteps in our design rationale. Further analysis showed that these missteps fall into several categories of common missteps in many existing commercial and research systems. While we cannot enumerate every possible privacy design flaw, we can offer these categories—formulated as design pitfalls—to the design community as cause for concern.

To help designers remember these pitfalls, we have clustered them into those that primarily affect users' *understanding* of a system's privacy implications and those that primarily affect their ability to conduct socially meaningful *action* through the system.

Understanding

1. *Obscuring potential information flow*. Designs should not obscure the nature and extent of a system's *potential* for disclosure. Users can make informed use of a system only when they understand the scope of its privacy implications.
2. *Obscuring actual information flow*. Designs should not conceal the *actual* disclosure of information through a system. Users should understand what information is being disclosed to whom.

Action

3. *Emphasizing configuration over action*. Designs should not require excessive configuration to manage privacy. They should enable users to practice privacy as a natural consequence of their normal engagement of the system.
4. *Lacking coarse-grained control*. Designs should not forgo an obvious, top-level mechanism for halting and resuming the disclosure.
5. *Inhibiting established practice*. Designs should not inhibit users from transferring established social practices to emerging technologies.

Before further articulating and providing evidence supporting these suggestions, we will elaborate on the meaning of our title: Personal Privacy through Understanding and Action.

Personal Privacy

Legal and policy scholar Alan F. Westin asserted that "no definition of privacy is possible, because privacy issues are fundamentally matters of values, interests and power" [43] (as quoted in [16]). We will not be so bold as to define privacy, but we will attempt to qualify within the scope of this article the phrase *personal privacy*.

Years prior to the assertion quoted above, Westin described information privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" [42]. Largely intended for policymakers, the reasoning behind this formulation served as the basis for the *fair information practices*, a set of flexible policy guidelines that continue to shape privacy legislation throughout the world. Since many privacy-affecting interactive systems are developed or deployed by organizations beholden to some interpretation of the fair information practices, Westin's formulation is a good place to start when elucidating personal privacy to designers. But we cannot end there, for there is more to privacy than this rather deterministic, libertarian formulation conveys.

Building on the work of social psychologist Irwin Altman [4], Palen and Dourish offer a more organic, sociologically-informed view that "privacy management in everyday life involves combinations of social and technical arrangements that reflect, reproduce and engender social expectations, guide the interpretability of action, and evolve as both technologies and social practices change" [34]. In this sense, privacy is less about a definitive entitlement to determine the flow of one's personal information and more about the intuitive fulfillment and maintenance of one's compound roles in the evolving, overlapping socio-technical contexts of everyday life.

While neither formulation excludes the other, one might say—at the risk of oversimplification—that Westin's formulation emphasizes privacy as *conscious process*, while Palen and Dourish's emphasizes privacy as *intuitive practice*. Clearly, however, people regulate their privacy in ways both deliberate and intuitive. Drawing directly from each formulation, then, what we are trying to signify by the phrase *personal privacy* is this set of both deliberate and intuitive practices by which an individual exercises her claim to determine personal information disclosure and which constitute, in part, her participation in the co-evolving technologies and expectations of everyday life.

A useful term that can make this discussion more concrete is Palen and Dourish's *genres of disclosure*, which are "socially-constructed patterns of privacy management," or

"regularly reproduced arrangements of people, technology and practice that yield identifiable and socially meaningful styles of interaction, information, *etc*." [34]. Examples might include creating and managing accounts at shopping websites, taking (or not, as the genre may oblige) photographs at social events, exchanging contact information with a new acquaintance, and revealing personal history to strangers. These all involve recognizable, socially meaningful, "normal" patterns of information disclosure and use. A genre of disclosure creates social expectations of its participants. Amidst a given genre, people expect each other to disclose *this*, to withhold *that*, and to use information in *this* but not *that* way. A person cooperates with (or antagonizes) a genre of disclosure through her performance of her role in that genre, and the degree to which a system does *not* align with that genre is the degree to which it fails to support the user's (and genre's) privacy regulation process. In this sense, what we call personal privacy in this article is simply the role the individual plays within a given genre of disclosure.

Of course, personal privacy can also include acting *contrary* to expectation. As technologies evolve, so do the practices that involve them. New modes and expectations of disclosure emerge as people both embrace *and* resist technologies and practices. Regardless of the case, a person can neither fully participate in nor effectively defy a genre of disclosure without understanding whether the system at hand aligns with that genre and without the ability to act in (or out of) alignment with it.

Understanding and Action

To be clear, we do not intend this dyadic formulation of *understanding* and *action* as a contribution to the theory of privacy, but simply as a conceptual framework for the arguments in this article. We frame our arguments using these straightforward terms in the hope of reaching as broad an audience as possible, for the sooner that designs improve their ability to support personal privacy regulation, the better.

With respect to genres of disclosure, we are proposing that a person cannot fulfill her role in the apposite genre of disclosure if she does not *understand* the degree to which the system at hand aligns with that genre and if she cannot conduct socially interpretable *action* involving the system. We suggest that a system that falls into any of our pitfalls without due rationale can disrupt its users' abilities to appropriate it in accordance with the relevant genre of disclosure. In so doing, it would by definition disrupt the genre itself or—if it is an emerging genre—make it unnecessarily complex. A privacy-sensitive interactive system will sustain the appropriate genre of disclosure—and will help their users do the same—through cues, affordances, and functions that empower users to understand and influence their privacy implications.

Empowering understanding and action is similar in meaning to bridging Norman's gulfs of evaluation and execution [32]. We feel the terms we have chosen convey a richer sense of the *social* implications of privacy-affecting systems than do Norman's terms, which seem to best address the perceptual/cognitive/motor problem of single-user human-device interaction. Privacy regulation does not conform to a plan-act-evaluate cycle; it is a continual, intuitive, multidimensional balancing act that requires nonlinear social dexterity. That said, at the end of this article we will examine another of Norman's canonical contributions—his elucidation of the role of mental models in the design process—and extend it to accommodate the social dimension of the privacy design process.

The rest of this paper is organized as follows. First, we briefly discuss the design and evaluation of *Faces*, our UI prototype for managing personal privacy in ubiquitous computing settings. The negative results of the evaluation motivated our investigation into the design missteps encoded in our five pitfalls. We then describe the five pitfalls, with illustrative examples from both our own and related work. We then discuss the pitfalls' implications for the design process, including an extension of Norman's elucidation of mental models. Finally, we offer negative and positive case studies of systems that, respectively, fall into and avoid the pitfalls.

FACES: (MIS)MANAGING UBICOMP PRIVACY

Our investigation into the pitfalls began after we encountered them firsthand while designing *Faces*, a prototype for specifying privacy preferences in ubiquitous computing (ubicomp) environments. Ubicomp envisions computation embedded throughout everyday environments to support arbitrary human activities [41]. But by distributing and concealing displays and sensors, it complicates interaction [6]. This can leave users unaware of or unable to intentionally influence the disclosure of personal information—such as location and identity—as they go about their activities in augmented environments. To address this, we designed Faces to (1) provide feedback about information disclosures in a log, not unlike a financial transaction statement, and (2) support the specification of disclosure preferences, such as *who* can obtain *what* information *when*. Users would employ feedback in the log to iteratively refine their disclosure preferences over time.

As we will show below, the design of Faces involved some crucial missteps, which, as we discovered, are also present in other systems. What clued us in to the fundamental nature of these missteps is that we made them despite a substantive requirements gathering effort (details in [28]). We reviewed the literature. We interviewed twelve local residents solicited from a public community website, walking them through a series of scenarios to elicit how they might think about privacy in ubicomp. We surveyed 130 people on the web to investigate factors that determine

privacy preferences in ubicomp [27]. And we iterated through a series of low-fidelity designs. The upshot of our findings was that the identity of the inquirer is a primary determinant of users' privacy preferences, but the situation in which the information is disclosed is also important.

Accordingly, we designed Faces to let users assign different disclosure preferences to different *inquirers*, optionally parameterized by *situation* (a conjunction of location, activity, time, and nearby people). We employed the metaphor of *faces* to represent disclosure preferences. This is a fairly direct translation of Goffman, who posited that a person works to present himself to an audience in such a way as to maintain a consistent impression of his role in relation to that audience [17]. Users specify their preferences by creating 3-tuples of *inquirers*, *situations*, and *faces*, with each 3-tuple meaning "if *this* inquirer wants information about me when I'm in *this* situation, show her *this* face" (Figure 1). Wildcards are allowed in the inquirer and situation slots to handle requests involving inquirers or situations that the user has not specified.

Each face alters the information disclosed to the inquirer by specifying the *precision* at which to disclose it. Faces supports four levels of precision, from Undisclosed (disclose nothing) to Precise (disclose everything). Each face contains a precision preference for each of the following information dimensions: identity, location, activity, and information about nearby people. Adjusting the precision of information—in effect, blurring it—can desensitize it, allowing for different versions of the same information to reach different inquirers, depending on the situation [27]. In doing so, Faces operationalizes three of Adams and Sasse's four factors that determine the perception of privacy in sensed environments: recipient, context, and sensitivity [3]. We did not directly address the fourth factor, usage, because it is often impractical to predict an observer's information usage [7].

A formative evaluation revealed fundamental problems with our design. We asked five participants to use the system to configure their privacy preferences regarding two inquirers and two situations of their choice. We then described a series of hypothetical but realistic scenarios involving those same inquirers and situations and asked the participants what information, if any, they would prefer to disclose in those scenarios. It turned out that the participants' configured preferences often differed from their stated preferences during the scenarios. Further, they had trouble remembering the precision preferences inside their faces, clouding their ability to predict the characteristics of any given disclosure. Finally, they expressed discomfort with the indirection between faces and the situations in which they apply. In their minds, a situation and the face one "wears" in it are inseparable. These results together illustrate the misstep of separating privacy management from the contexts in which it applies. In sum, while Faces modeled Goffman's theory *in* the interface, it inhibited users from *practicing* identity management *through* the interface. Users had to think explicitly about privacy in the abstract—and instruct the system how to shape it—instead of managing it intuitively through their actions *in situ* [34].

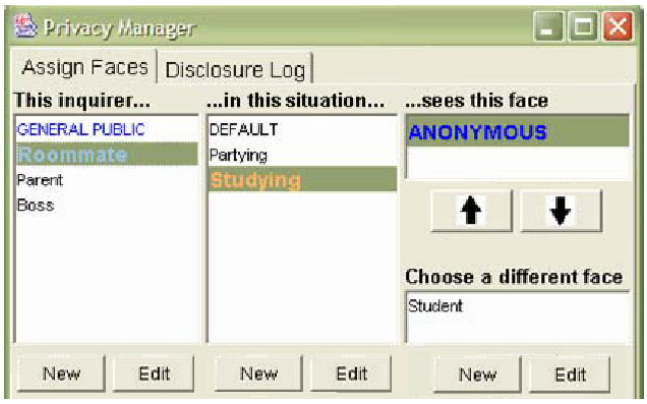

Figure 1. UI for creating and assigning faces. Each face holds precision preferences for blurring information disclosed to a given inquirer when the user is in a given situation.

Having identified these design flaws despite a reasonable design process, we reviewed other privacy-affecting systems in search of similar mistakes. The practicable outcome of this analysis is our five pitfalls to avoid when designing for personal privacy, presented below with evidence of designs both falling into and avoiding them. After articulating them, we will analyze the Faces system with respect to the five pitfalls.

FIVE PITFALLS IN DESIGNING FOR PRIVACY

Our pitfalls encode an analysis of common problems in interaction design across several systems, constituting a preventative guide to help designers avoid mistakes that may appear obvious but are still being made. Designers should carefully avoid them throughout the design cycle as appropriate. Naturally, not all of the pitfalls will apply to every system; they should be interpreted within the context of the system being designed

The pitfalls fit into a history of analyses and guidelines on developing privacy-sensitive systems. They are, in part, an effort to reconcile Palen and Dourish's theoretical insights about how people maintain privacy with Bellotti and Sellen's practical guidelines for designing feedback and control to support it. In reaching for this middle ground, we have tried to honor the fair information practices, as developed by Westin [42] and more recently promoted by Langheinrich [26], and to minimize information asymmetry between users and observers, as argued by Jiang *et al*. [24].

Concerning Understanding: Two Pitfalls

Our first two pitfalls primarily involve the user's *understanding* of the system's privacy implications. Designs can enable this understanding by illuminating (1)

the system's potential for information disclosure and (2) the actual disclosures made through it.

Pitfall 1: Obscuring Potential Information Flow

To whatever degree is reasonable, systems should make clear the nature and extent of their *potential* for disclosure, lest they give false impressions about their implications for personal privacy. Users will have difficulty appropriating a system if the scope of its privacy implications is unclear. This scope includes the types of information the system conveys, the kinds of observers it conveys to, the potential for unintentional disclosure, the presence of third parties, and the collection of meta-information like traffic analysis. Clarifying a system's potential for conveying personal information is vital to users' ability to predict the social consequences of using the system.

Among the conveyable information types that should be exposed are identifiable personae (*e.g.*, true name, email addresses, credit card numbers, social security number) and monitorable activities (*e.g.*, locations, purchases, web browsing histories, communications, A/V records, social networks). People cannot maintain consistent identities without knowing which of their activities can be associated with which of their personae [35].

Privacy-affecting systems tend to involve both interpersonal disclosure (revealing sensitive information to another person) and organizational disclosure (companies or governments). Designs should clarify the potential involvement of each, making clear the extent to which primarily interpersonal disclosures (*e.g.*, chat) involve incidental organizational disclosures (*e.g.*, workplace chat monitoring) and, conversely, the extent to which primarily organizational disclosures (*e.g.*, workplace cameras) involve secondary interpersonal disclosures (*e.g.*, mediaspaces).

"Privacy" is a broad term whose unqualified use as a label can mislead users into thinking a system protects or erodes privacy in ways it does not. Making the scope of a system's privacy implications clear will help users understand its capabilities and limits. This in turn provides grounding for comprehending the actual flow of information through the system, addressed in the next pitfall.

Evidence: Falling into the Pitfall

An easy way to obscure a system's privacy scope is to present its functionality ambiguously. One example is Microsoft's Windows operating systems. The Windows Internet control panel offers ordinal degrees of privacy protection (from Low to High) for Internet use. The functional meaning of this scale is unclear to average users and, as it turns out, this mechanism does not affect general Internet use through the operating system; its scope is limited to a particular web browser's cookie management heuristics. Similarly, Anonymizer.com's free anonymizing software can give the impression that all Internet activity is anonymous when the service is active, but in actuality it only affects web browsing, not email, chat, or other services. A for-pay version covers those services.

Another example is found in Beckwith's report of an eldercare facility using worn transponder badges to monitor the locations of residents and staff [5]. Many residents perceived the badge only as a call-button (which it was) but not as a persistent location tracker (which it also was). They did not understand the scope of its privacy implications.

Similarly, some hospitals use badges to track the location of nurses for efficiency and accountability purposes, but they can neglect to clarify what kind of information the system conveys. One concerned nurse wrote, erroneously, "They've placed it in the nurses' lounge and kitchen. Somebody can click it on and listen to the conversation. You don't need a Big Brother overlooking your shoulder" [36].

Evidence: Avoiding the Pitfall

Many web sites that require an email address for creating an account give clear notice on their sign-up forms that they do not share email addresses with third parties or use them for extraneous communication with the user. Clear, concise statements like these help clarify scope.

Another successful design is Tribe.net, a social networking service that carefully conveys that members' information will be made available only to other members within a certain number of degrees of social separation.

Pitfall 2: Obscuring Actual Information Flow

Having addressed the user's need to understand a system's *potential* privacy implications, we move now to the issue of *actual* instances of disclosure. To whatever degree is reasonable, designs should make clear the actual disclosure of information through the system. Users should understand *what* information is being conveyed to *whom*. The disclosure should be obvious to the user as it occurs; if this is impractical, notice should be provided within a reasonable delay. There should be just enough feedback to inform but not overwhelm the user.

We will not dwell on this point, for it is perhaps the most obvious of the five pitfalls. We suggest Bellotti and Sellen [7] as a useful guide to exposing actual information disclosure.

By avoiding both this and the prior pitfall, designs can clarify the extent to which users' actions engage the system's range of privacy implications. This enables users to understand the consequences of their use of the system thus far, and it empowers them to predict the consequences of future use. In the Discussion section, we will elaborate on how avoiding both of these pitfalls can support the user's mental model of his personal information flow.

Evidence: Falling into the Pitfall

Web browser support for cookies is a persistent example of obscuring information flow [30]. Most browsers do not, by default, indicate when a site sets a cookie or what information is disclosed through its use. The prevalence of third-party cookies and web bugs (tiny web page images that monitor who is reading the page) exacerbates users' ignorance of who is observing their browsing activities.

Another example of concealed information flow is in the Kazaa P2P file-sharing application, which has been shown to facilitate the concealed disclosure of highly sensitive personal information to unknown parties [18].

Another simple example is locator badges like those described in [5, 20], which generally do not inform their wearers about who is locating them.

Evidence: Avoiding the Pitfall

Friedman *et al's.* redesign of cookie management improves browsers' ability to show what information is being disclosed to what web sites [15].

Instant messaging systems often employ a symmetric design that informs the user when someone else wants to add her to his contact list, allowing her to do the same. By then letting users see and adjust their own status (*e.g.*, "Busy" or "Out to Lunch"), they inform users *who* can see *what* about them. This gives individuals a better understanding of how they are presenting themselves.

AT&T's mMode Find Friends service, which lets mobile phone users locate other users of the service, informs the user when someone else is locating them. They learn *who* is obtaining *what* (their location).

Concerning Action: Three Pitfalls

Our last three pitfalls primarily involve the user's socially meaningful *actions* involving the system. These three pitfalls support the recognition that privacy regulation occurs not within technical parameters but in the social consequences of discernable actions involving technical systems.

Pitfall 3: Emphasizing Configuration over Action

Designs should not require excessive configuration to create and maintain privacy. They should enable users to practice privacy management as a natural consequence of their ordinary use of the system.

Palen and Dourish write, "setting explicit parameters and then requiring people to live by them simply does not work, and yet this is often what information technology requires… Instead, a fine and shifting line between privacy and publicity exists, and is dependent on social context, intention, and the fine-grained coordination between action and the disclosure of that action" [34]. But because configuration has become a universal UI design pattern, many systems fall into the pitfall of configuration.

Configured privacy breaks down for at least two reasons. First, in real settings users manage privacy semi-intuitively; they do not spell out their privacy needs in an auxiliary, focused effort [44]. Configuration imposes an awkward requirement on users, one they will often forsake in favor of default settings [29, 33]. If users are to manage their privacy at all, it needs to be done in an intuitive fashion, as a predictable outcome of their situated actions involving the system.

Second, the act of configuring preferences is too easily desituated from the contexts in which those preferences apply. Users are challenged to predict their needs under hypothetical circumstances, and they can forget their preferences over time. If they predict wrongly, or remember incorrectly, their configured preferences will differ from their *in situ* needs, creating the conditions for an invasion of privacy.

People generally do not set out to explicitly protect their privacy. Rather, they participate in some activity, with privacy regulation being an embedded component of that activity. Designs should take care not to extract the privacy regulation process from the activity within which it is normally conducted.

Evidence: Falling into the Pitfall

Many systems emphasize explicit configuration of privacy, including experimental online identity managers [8, 23], P2P file-sharing software [18], web browsers [30], email encryption software [44], and our Faces prototype.

Evidence: Avoiding the Pitfall

Successful solutions can involve some measure of configuration, but tend to embed it into the actions necessary to use the system. Web sites like Friendster.com and Tribe.net allow users to regulate information flow by modifying their social networks—a process that is embedded into the use of these applications.

Georgia Tech's In/Out Board [13] lets users reveal or conceal their presence in a workspace by badging into an entryway device. Its purpose is to convey this information, but it can be intuitively used to withhold information as well, by falsely signaling your in/out status.

Ignoring the moral implications, another example involves camera surveillance. When someone is aware of a camera's presence, she tends to intuitively adjust her behavior to present herself as she wants to be perceived [14].

Cadiz and Gupta propose a smart card that one could hand to a receptionist to grant limited access to her calendar to schedule an appointment; he would hand it back right afterwards. No one would have to fumble with setting permissions. They also suggest extending scheduling systems to automatically grant meeting partners access to a user's location in the minutes leading up to a meeting, so they can infer his arrival time. The action of scheduling a

meeting implies limited approval of location disclosure [11].

Pitfall 4: Lacking Coarse-Grained Control

Designs should offer an obvious, top-level mechanism for halting and resuming the disclosure of personal information. Often a power button or exit button will do the trick. Users are accustomed to turning a thing off when they want its operation to stop. Turning off information flow is an instinctive behavior that affects personal privacy.

Beyond binary control, a simple linear control may also be appropriate in some cases (*cf.*, audio devices' mute and volume controls). Ubicomp systems that convey location or other context could incorporate both a *precision dial* and a *hide button*, so users can either adjust the precision at which their context is disclosed or decidedly halt disclosure.

In the general case, users can become remarkably adept at wielding coarse-grained controls to yield nuanced results (*e.g.*, driving a car). Coarse-grained controls tend to reflect their state, providing direct feedback and freeing the user from having to remember whether she set a preference properly. This helps users accommodate the controls and even co-opt them in ways the designer may not have intended. Examples specific to privacy include: setting a door ajar, covering up or repositioning cameras [7, 22], turning off a phone or using its invisible mode rather than navigating its privacy-related options, and removing a locator badge.

While some fine-grained controls may be unavoidable, the flexibility that fine-grained controls are intended to provide is often neglected by users (see Pitfall #3). Flexibility in the control of privacy often comes not from within the system, but from the user's nuanced manipulation of coarse-grained controls.

Evidence: Falling into the Pitfall

Many e-commerce web sites recommend to shoppers items that were purchased by other shoppers with similar shopping histories. While this is a useful service, there are times when a shopper does not want the item at hand to be included in his profile; he effectively wants to shop anonymously during the current session. Even though the merchant will know about the purchase, the shopper may not want his personalized shopping environment—which others can see—to reflect this private purchase. We have encountered no web sites that provide a simple mechanism for excluding the current purchase from our profiles.

Similarly, most web browsers still bury their privacy controls under two or three layers of configuration panels [30]. Third-party applications that expose cookie control have begun to appear (*e.g.*, GuideScope.com).

Further, wearable locator-badges like those described in [20] and [5] do not have power buttons. One could remove the badge and leave it somewhere else, but simply turning it off would at times be more practical or preferable.

Evidence: Avoiding the Pitfall

Systems that expose simple, obvious ways of halting and resuming disclosure include easily coverable cameras [7], mobile phone power buttons, chat systems with invisible modes, the In/Out Board [13], and our Faces prototype, with a button on a handheld application that overrides current settings.

Pitfall 5: Inhibiting Established Practice

Designs should beware inhibiting existing social practice. People manage privacy through a range of nuanced practices. For simplicity's sake, we might divide such practices into those that are already established and those that will evolve as new disclosure technologies emerge. While early designs might lack elegant support for emergent practices, they can at least take care to *avoid inhibiting established ones*.

Nuanced social practices cannot evolve around a system until the system is deployed. Designers might take care to co-evolve their systems along with the practices that develop around them. Interestingly, despite being notoriously awkward at supporting social nuance [1], technical systems that survive long enough in the field will often contribute to the emergence of nuanced practice regardless of whether they suffered from socially awkward design in the first place (*e.g.*, [9, 19]). In other words, nuance happens. Nonetheless, emergent practices are intrinsically difficult to predict and design for.

To facilitate adoption, designs should accommodate users' natural efforts to transfer existing practices to them. Designers can identify and assess the relevant existing genres of disclosure into which their systems will be introduced. From there, they can identify, support, and possibly enhance the technologies, roles, relations, and practices already at play in those genres.

Beyond genre-specific practices, certain meta-practices are worth noting. In particular, we emphasize the broad applicability of plausible deniability (whereby the observer cannot determine whether a lack of disclosure was intentional) [31, 45] and disclosing ambiguous information (*e.g.*, pseudonyms, imprecise location). These common techniques allow people to finesse disclosure through technical systems to achieve nuanced social ends. Systems that rigidly belie meta-practices like plausible deniability and ambiguous disclosure may likely encounter significant resistance during deployment [38].

Evidence: Falling into the Pitfall

Some researchers envision context-aware mobile phones that can inform the caller of the user's activity, to help explain why their call was not answered [37]. But this can prohibit users from exploiting plausible deniability. There

can be value in keeping the caller ignorant of the reason for not answering.

Location-tracking systems like those described in [20] and [5] constrain users' ability to incorporate ambiguity into their location disclosures. Users can only convey a single precision of location or, at times, nothing at all.

Evidence: Avoiding the Pitfall
Mobile phones, push-to-talk phones [45], and instant messaging let users exploit plausible deniability by not responding to hails and not having to explain why.

Although privacy on the web is a common concern, a basic function of HTML allows users to practice ambiguous disclosure. Forms that let users enter false data facilitate anonymous account creation and service provision.

Tribe.net supports another subtle real-world practice. Tribe allows users to partition their social networks into "tribes," thereby letting pre-existing groups represent themselves online, situated within the greater networks to which they are connected. In contrast, Friendster.com users each have a single set of friends that cannot be functionally partitioned.

DISCUSSION

Having described the five pitfalls and provided evidence of systems that fall into and avoid them, we now examine some of the deeper implications they have for design. We begin by elaborating on the influence of our first two pitfalls on the user's mental model of his information disclosures. This leads to the introduction of a new conceptual tool to help the design process. Then we present an analytical argument for why designs that avoid our five pitfalls can support the human processes of understanding and action necessary for personal privacy maintenance. Using our Faces prototype as a case study, we then show how falling into these pitfalls can undermine an otherwise ordinary design process. Finally we discuss some successful systems that have largely avoided the pitfalls.

Mental Models of Information Flow

As we said earlier, avoiding our first two pitfalls—obscuring potential *and* actual information flow—can clarify the extent to which users' actions engage the system's range of privacy implications. Users can understand the consequences of their use of the system thus far, and they can predict the consequences of future use.

Illuminating disclosure contributes constructively to the user's mental model of the portrayal of her identity in the context of the system. If she has a reasonable understanding of what observers already know about her (Pitfall 2) and of what they can learn about her (Pitfall 1), she can maintain and exploit this mental model to inform the ongoing portrayal of her identity through the system.

In the context of interactive systems, the personal information a user conveys is often tightly integrated with her interaction with the system. For example, by simply browsing the web, a user generates a wealth of information that can be used in ways that directly impact her life. When interaction and disclosure are integrated thusly, an informed user's mental model of the system's operation and her mental model of her disclosures are interdependent.

This suggests an extension to Norman's canonical elucidation of the role of mental models in the design process. According to Norman, the designer's goal is to design the system image (*i.e.*, those aspects of the implementation with which the user interacts) such that the user's mental model of the system's operation coincides with the designer's mental model of the same [32].

When we take into account the coupling of interaction and disclosure, we see that the designer's goal has expanded. She now strives to design the system image such that the user's mental models of the system's operation *and* of the portrayal of his identity through it are both accurate. As with Norman's original notion, ideally the designer's and the user's models of the system's operation will coincide. But the designer generally cannot have a model of the user's identity; that depends on the user and the context of use. Indeed, here the designer's task is not to harmonize the user's model of his information flow with her own (she likely has none), but to harmonize the user's information model with the *observer's* (Figure 2). In other words, she wants to design the system image to accurately convey a model not only of how other parties *can* observe the user's behavior through the system, but also what they *do* observe.

Generalizing this notion beyond privacy, to cooperative information flow in general, may be of further use to the CSCW community but is beyond the scope of this paper.

Opportunities for Understanding and Action

We have argued that people maintain personal privacy by *understanding* the privacy implications of their socio-technical contexts and influencing them through socially meaningful *action*. When a technical system is embedded into a social process, the primary means that designers have to engender understanding and action are feedback and

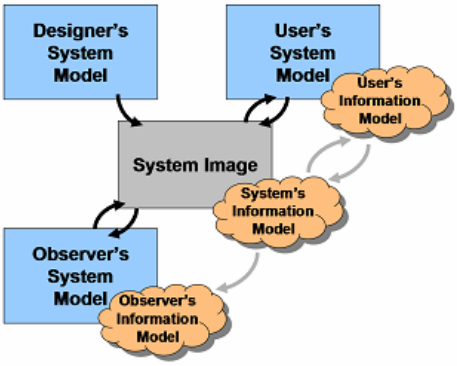

Figure 2. Building on Norman [32], designers should strive to harmonize the user's and the observer's understandings of the user's personal information disclosures.

control mechanisms. We encourage designers of privacy-affecting systems to think of feedback and control mechanisms as *opportunities* for understanding and action. They are the designer's opportunity to empower those processes, and they are the user's opportunity to practice them.

Thinking thusly can help designers reach across what Ackerman calls the *socio-technical gap*—the difference between systems' technical capabilities and their social requirements [1]—just enough to empower informed social action. The challenge is to find that intermediate point where carefully designed technical feedback and control translates into social understanding and action. Reaching too far can overwhelm the user. Reaching not far enough can disempower him.

We believe that avoiding our pitfalls can help designers reach that intermediate point. Carefully designed feedback about potential (#1) and actual (#2) information flow can help users understand the representation and conveyance of their behavior through the system. Curtailing configuration (#3), providing coarse-grained control (#4), and supporting established practices (#5) can help people make productive, intuitive use of a privacy-affecting system. Designs that heed these suggestions make their consequences known and do not require great effort to use, helping people incorporate them meaningfully into the lexicon of personal privacy practices by which they engage everyday life's genres of disclosure.

Negative Case Study: Faces

We return now to Faces—our prototypical ubicomp privacy UI—as a case study in how to fall into the pitfalls.

Pitfall 1: Obscuring Potential Flow. In trying to be a UI for managing privacy across any ubicomp system, Faces abstracted away the true capabilities of any underlying system. Users could not gauge its potential information flow because it aimed to address *all* information flow. Its scope was impractically broad and, hence, obscure.

Pitfall 2: Obscuring Actual Flow. Faces conveyed actual information flow through the user's disclosure log. The record was accessible after the relevant disclosure. While this design intends to illuminate information flow, it is unclear whether postponing notice is optimal. Embedding notice directly into the real-time experience of disclosure might foster a stronger understanding of information flow.

Pitfall 3: Configuration over Action. Faces required a considerable amount of configuration. Once configuration was done, and assuming it was done correctly (which our evaluation brings into doubt), the system required little *ad-hoc* configuration. The user simply goes about his business. Nonetheless, the sheer amount and desituated nature of configuration positions Faces squarely in this pitfall.

Pitfall 4: Lacking Coarse-grained Control. Faces avoided this pitfall somewhat by including an Override function that afforded quick transitions to alternate faces. Notably, this was not considered a central design feature.

Pitfall 5: Inhibiting Established Practice. While Faces modeled the nuance of Goffman's identity management theory, it appeared to hinder the actual identity management practice by requiring the user to maintain virtual representations of his fragmented identities *in addition to* manifesting them naturally through intuitive, socially meaningful behavior. In this sense, Faces disrupts privacy management practice at a fundamental level.

Our evaluation of Faces revealed a complex, abstract configuration requirement that belies the intuitive situatedness of privacy as practiced in real settings. Faces also futilely aimed to address privacy needs across an arbitrary range of information types—both static (*e.g.*, contact information) and dynamic (*e.g.*, location). In reality, privacy management employs critically different techniques for different information types. The upshot is that, rather than attempt to revise Faces to address our evaluation findings, we found it more appropriate to retire the Faces concept and scale our design focus down to a more isolable point in the ubicomp privacy space. In the following section, we assess a interaction concept that recently emerged from that process.

(Potentially) Positive Case Study: Precision Dial

One of Faces' core features—adjustable information precision—is a common privacy management technique in research (*e.g.*, [10, 21]) and could serve as the basis for a more streamlined ubicomp privacy tool. Here we briefly propose such a tool and suggest how its design might steer around the pitfalls better than Faces did. We will call this tool the *precision dial*.

The precision dial would be an easily accessible dial or rocker switch on a mobile phone that lets the user quickly adjust the precision of any contextual information—often referred to as *presence*—disclosed to his personal contacts on-the-fly. When an observer requests the user's presence information, it is blurred according to his current precision setting. He could quickly change precision settings as needed, similar to the practice of adjusting ringer volume when entering meetings and theaters. Pre-configuring privacy preferences would not be required, as it was in Faces.

Rather than a continuous precision scale (which seems rather implausible), we will assume the same four-point precision scale used in Faces (undisclosed > vague > approximate > precise). The dial would allow quick selection of one of these four points. In contrast to Faces' encapsulation of separate precision settings for each dimension of information (location, nearby people, *etc.*), the dial would apply a single precision across all

dimensions. The rationale here is that, rather than being a separable dimension of context, the user's *activity* is effectively constituted and represented by the sum of his context. Disclosing, say, where someone is and whom he is with could be tantamount to disclosing his activity, since observers can exploit personal or normative knowledge to infer activity from context. Hence if the user intends to blur the representation of his activity in a system that intentionally conveys presence, the easiest way to do so might be to apply a single transformation command to all disclosable information.

We envision the option to create groups of known observers (like friends/family/colleagues groupings in instant messaging clients) and to specify a default precision for each group. When adjusting precision *in situ*, the user could adjust for a specific group or for all observers.

To be clear, we do not intend the precision dial as a general user interface for ubicomp privacy. In fact, we hope this article makes clear the futility of such an idea, given the multidimensional, situated nature of personal privacy. We envision the dial as a tool for managing the representation of one's activity as conveyed through real-time presence awareness systems.

Reminding the reader of the speculative nature of this assessment, since the precision dial is merely a proposal, we suggest that, in comparison to Faces, the precision dial can largely avoid the five pitfalls in the following ways.

Pitfall 1: Obscuring Potential Flow. Unlike Faces, this tool is deliberately scoped to a specific subspace of the privacy space: intentional interpersonal disclosure of activity—as presence—to familiar observers. In other words, it lets your friends find out what you are doing, with your permission. A system employing this tool should clarify its operational definition of presence. And it should clarify that information is conveyable only to people on the user's contact list. By letting users collect observers into groups, they can know who has the potential to obtain what information about them at which precisions.

Pitfall 2: Obscuring Actual Flow. Disclosures can be exposed by real-time alerts, a disclosure log, or both.

Pitfall 3: Configuration over Action. The notion of blurring precision arguably aligns with the mental model of "I don't want to reveal too much about my activity right now." A readily accessible dial would allow quick assertion of such a preference and would achieve socially meaningful results. Managing groups might present a configuration a burden, but good design practices can minimize it. For instance, the user could have the option to quickly choose a group for each observer at the time he adds her to his contact list.

Pitfall 4: Lacking Coarse-grained Control. One cannot get much coarser than an ambiguous four-point ordinal precision scale. Nonetheless, we have chosen the number of points rather arbitrarily. A three-point scale might be better. Any coarser would result in a binary button, but we suspect people would prefer to leverage some gray area between the extremes of disclosing everything and disclosing nothing.

Pitfall 5: Inhibiting Established Practice. The precision dial supports both ambiguous disclosure and plausible deniability. The former is a consequence of the intrinsic ambiguity of the precision scale. The latter is supported by the observer's ignorance of the reasons why the user employed any given precision level; it may have been due to social expectations (*i.e.*, the user may have simply been keeping inline with the relevant genre of disclosure), or due to technical factors (*e.g.*, signal loss), or simply the desire to be left alone.

Positive Case Study: Instant Messaging and Mobile Telephony

Interestingly, two systems that largely avoid our pitfalls—mobile phones and instant messaging (IM)—are primarily *communication* media. Disclosure is one of their central functions. We will briefly assess these services against the pitfalls, focusing on their primary functions—textual and vocal communication—and on some of their secondary features that support these functions. We will not address orthogonal, controversial features like the location-tracking capabilities of some mobile phones and the capture of IM sessions, which would have to be addressed by a more robust assessment of the privacy implications of these technologies.

IM and mobile telephony each make clear the potential and actual flow of disclosed information, making for a robust, shared mental model of information flow through these cooperative interactive systems. *Potential flow* is scoped by features like Caller ID (telephony), Buddy Lists (IM), and feedback about the user's own online presence (IM). *Actual flow* is self-evident in the contents of the communications. Each technology requires minimal *configuration* for maintaining privacy (though other features often require excessive configuration), largely due to *coarse-grained controls* for halting and resuming information flow—power button (telephony), application exit (IM), invisible mode (IM), and ringer volume (telephony). Lastly, each supports *existing practices* of plausible deniability—people can choose to ignore incoming messages and calls without having to explain why—and ambiguous disclosure—the linguistic nature of each medium allows for arbitrary customization of disclosed information [31, 45].

Indeed, communication media could serve as a model for designing other privacy-affecting systems not conventionally categorized under as communication technologies. Disclosure *is* essentially communication, whether it results from the use of a symmetric linguistic medium—*e.g.*, telephony—or an asymmetric event-based medium—*e.g.*, e-commerce, context-aware systems. Systems that affect privacy but are not positioned as

communication media do nonetheless communicate personal information to observers. Exposing and addressing these disclosure media as communication media might liberate designs to leverage users' intuitive privacy maintenance skills.

CONCLUSION

In this paper we described five common pitfalls to which designs of privacy-affecting systems often succumb. These pitfalls include obscuring potential information flow, obscuring actual flow, emphasizing configuration over action, lacking coarse-grained control, and inhibiting established practice. We analyzed these pitfalls and provided several examples of systems that fall into or manage to avoid them, including Faces, our UI prototype for managing ubicomp privacy.

We encourage designers to identify the genres of disclosure to which their systems will contribute and—with the help of our guidelines—to design opportunities for the user to (1) understand the extent of the system's alignment with those genres and (2) conduct socially meaningfully action that supports them (or disrupts them, as the case may be).

REFERENCES

1. Ackerman, M.S. The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility. *Human-Computer Interaction*, *15* (2/3). 181-203.
2. Adams, A., Multimedia Information Changes the Whole Privacy Ballgame. in *Conference on Computers, Freedom, and Privacy*, (Toronto, Ontario, CA, 2000), ACM Press, 25-32.
3. Adams, A. and Sasse, M.A., Taming the Wolf in Sheep's Clothing: Privacy in Multimedia Communications. in *Proceedings of ACM Multimedia*, (Orlando, FL, USA, 1999), 101-107.
4. Altman, I. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Brooks/Cole Publishing Co., Monterey, CA, 1975.
5. Beckwith, R. Designing for Ubiquity: The Perception of Privacy *IEEE Pervasive*, 2003, 40-46.
6. Bellotti, V., Back, M., Edwards, W.K., Grinter, R.E., Henderson, A. and Lopes, C., Making sense of sensing systems: five questions for designers and researchers. in *Proceedings of the SIGCHI conference on Human factors in computing systems*, (Minneapolis, Minnesota, USA, 2002), ACM Press, 415-422.
7. Bellotti, V. and Sellen, A., Design for Privacy in Ubiquitous Computing Environments. in *Proceedings of the Third European Conference on Computer Supported Cooperative Work (ECSCW'93)*, (1993), 77-92.
8. boyd, d. Faceted Id/Entity: Managing representation in a digital world, MS Thesis *Program in Media Arts and Sciences, School of Architecture and Planning*, Massachusetts Institute of Technology, Cambridge, MA, 2002.
9. boyd, d., Reflections on Friendster, Trust and Intimacy. in *Workshop on Intimate Ubiquitous Computing, Ubicomp 2003*, (Seattle, WA, USA, 2003).
10. Boyle, M., Edwards, C. and Greenberg, S., The effects of filtered video on awareness and privacy. in *Proceedings of the 2000 ACM conference on Computer-Supported Cooperative Work*, (Philadelphia, PA, USA, 2000), ACM Press, 1-10.
11. Cadiz, J. and Gupta, A. Privacy Interfaces for Collaboration, Technical Report MSR-TR-2001-82, Microsoft Corp., Redmond, WA, 2001.
12. Cranor, L., Reagle, J. and Ackerman, M.S. Beyond Concern: Understanding Net Users' Attitudes About Online Privacy. in Vogelsang, I. and Compaine, B.M. eds. *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy*, MIT Press, 2000, 47-70.
13. Dey, A.K., Salber, D. and Abowd, G.D. A Conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications. *Human-Computer Interaction*, *16* (2-4). 97-166.
14. Foucault, M. *Discipline and Punish*. Vintage Books, New York, 1977.
15. Friedman, B., Howe, D.C. and Felten, E.W., Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design. in *Proc. of 35th Annual Hawaii International Conference on System Sciences*, (2002).
16. Gellman, R. Does Privacy Law Work? in Agre, P.E. and Rotenberg, M. eds. *Technology and Privacy: The New Landscape*, MIT Press, Cambridge, MA, 1998, 193-218.
17. Goffman, E. *The Presentation of Self in Everyday Life*. Doubleday, New York, NY, 1956.
18. Good, N.S. and Krekelberg, A., Usability and privacy: a study of Kazaa P2P file-sharing. in *Proceedings of the conference on Human factors in computing systems*, (Ft. Lauderdale, FL, USA, 2003), ACM Press, 137-144.
19. Green, N., Lachoee, H. and Wakeford, N., Rethinking Queer Communications: Mobile Phones and beyond. in *Sexualities, Medias and Technologies Conference*, (University of Surrey, 2001).
20. Harper, R.H.R., Lamming, M.G. and Newman, W.H. Locating Systems at Work: Implications for the Development of Active Badge Applications. *Interacting with Computers*, *4* (3). 343-363.
21. Hudson, S.E. and Smith, I., Techniques for addressing fundamental privacy and disruption tradeoffs in awareness support systems. in *Proceedings of the 1996 ACM conference on Computer-Supported Cooperative Work*, (Boston, MA, USA, 1996), ACM Press, 248-257.
22. Jancke, G., Venolia, G.D., Grudin, J., Cadiz, J.J. and Gupta, A., Linking public spaces: technical and social

issues. in *Proceedings of the SIGCHI conference on Human factors in computing systems*, (Seattle, WA, USA, 2001), ACM Press, 530-537.
23. Jendricke, U. and Gerd tom Markotten, D., Usability meets Security – The Identity-Manager as your Personal Security Assistant for the Internet. in *16th Annual Computer Security Applications Conference*, (2000).
24. Jiang, X., Hong, J.I. and Landay, J.A., Approximate Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing. in *The Fourth International Conference on Ubiquitous Computing*, (2002), Springer-Verlag LNCS.
25. Kaasinen, E. User needs for location-aware mobile services. *Personal and Ubiquitous Computing*, *7* (1). 70-79.
26. Langheinrich, M., Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. in *The Third International Conference on Ubiquitous Computing*, (2001), Springer-Verlag LNCS, 273-291.
27. Lederer, S., Mankoff, J. and Dey, A.K., Who wants to know what when? Privacy preference determinants in ubiquitous computing. in *CHI '03 extended abstracts on Human factors in computer systems*, (Ft. Lauderdale, FL, USA, 2003), ACM Press, 724-725.
28. Lederer, S., Mankoff, J., Dey, A.K. and Beckmann, C. Managing Personal Information Disclosure in Ubiquitous Computing Environments, Technical Report CSD-03-1257, UC Berkeley, Berkeley, CA, 2003.
29. Mackay, W.E., Triggers and barriers to customizing software. in *Proceedings of the SIGCHI conference on Human factors in computing systems*, (New Orleans, LA, USA, 1991), ACM Press, 153-160.
30. Millett, L.I., Friedman, B. and Felten, E., Cookies and Web browser design: toward realizing informed consent online. in *Proceedings of the SIGCHI conference on Human factors in computing systems*, (Seattle, WA, USA, 2001), ACM Press, 46-52.
31. Nardi, B.A., Whittaker, S. and Bradner, E., Interaction and Outeraction: Instant Messaging in Action. in *Proc. ACM CSCW Conf.*, (New York, NY, 2000), ACM, 79-88.
32. Norman, D.A. *The Design of Everyday Things*. Basic Books, New York, NY, 1988.
33. Palen, L., Social, Individual & Technological Issues for Groupware Calendar Systems. in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 99)*, (Pittsburgh, PA, 1999), ACM, 17-24.
34. Palen, L. and Dourish, P., Unpacking "privacy" for a networked world. in *Proceedings of the conference on Human factors in computing systems*, (Fort Lauderdale, FL, 2003), ACM Press, 129-136.
35. Phillips, D.J., Context, Identity, and Privacy in Ubiquitous Computing Environments. in *Ubicomp 2002 (Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing)*, (Göteborg, Sweden, 2002).
36. Reang, P. Dozens of nurses in Castro Valley balk at wearing locators *Mercury News*, San Jose, CA, 2002.
37. Siewiorek, D., Smailagic, A., Furukawa, J., Krause, A., Moraveji, N., Reiger, K., Shaffer, J. and Wong, F., SenSay: A Context-Aware Mobile Phone. in *IEEE International Symposium on Wearable Computers*, (White Plains, NY, USA, 2003).
38. Suchman, L. Do Categories have Politics? The language/action perspective reconsidered. *Computer-Supported Cooperative Work*, *2*. 177-190.
39. Taylor, H. Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits, The Harris Poll, 2003.
40. Turow, J. Americans and Online Privacy: The System is Broken, Annenberg Public Policy Center, University of Pennsylvania, 2003.
41. Weiser, M. The Computer for the Twenty-First Century *Scientific American*, 1991, 94-104.
42. Westin, A. *Privacy and Freedom*. Atheneum, New York, NY, 1967.
43. Westin, A., Privacy in America: An Historical and Socio-Political Analysis. in *National Privacy and Public Policy Symposium, Hartford, CT*, (1995).
44. Whitten, A. and Tygar, J.D., Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. in *8th USENIX Security Symposium*, (1999).
45. Woodruff, A. and Aoki, P.M., How Push-to-Talk Makes Talk Less Pushy. in *Proc. ACM SIGGROUP Conf. on Supporting Group Work (GROUP '03)*, (Sanibel Island, FL, 2003), ACM Press, 170-179.