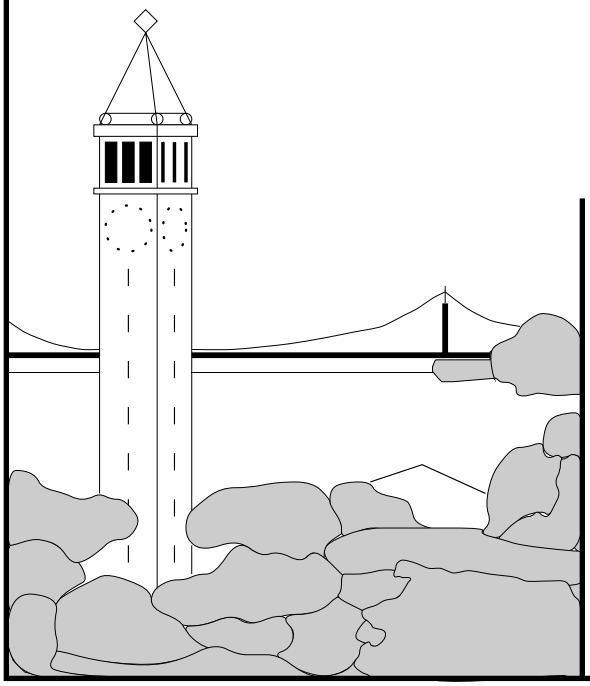
A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous Computing Environments

Scott Lederer, Anind K. Dey, Jennifer Mankoff



Report No. UCB/CSD-2-1188

June 2002

Computer Science Division (EECS)
University of California
Berkeley, California 94720

A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous Computing Environments

Scott Lederer, Anind K. Dey, Jennifer Mankoff

Group for User Interface Research
University of California, Berkeley
Berkeley, CA, 94720, USA
{lederer, dey, jmankoff}@cs.berkeley.edu

Abstract. We present a unified model of everyday privacy in ubiquitous computing environments, designed to aid system designers and administrators in conceptualizing the end-user privacy experience. The model accounts for the influence of societal-scale forces, contextual factors, and subjective perception on end-user privacy. We identify *notice* and *consent* as the *fair information practices* of greatest everyday utility to users, as they gradually engender the user's conceptual model of ubicomp privacy. Navigating the regular deluge of personal information collection events in ubicomp requires that notice be minimally intrusive and consent be implicitly granted by a persistent, situation-specific set of user preferences. We extend our model into an interactional metaphor called *situational faces*, designed to mitigate the complexity of privacy for the end-user. When encountering a *situation*, a user engages the appropriate *face*, a metaphorical abstraction of a set of privacy preferences.

1 Introduction

Ubiquitous computing (ubicomp) presents significant challenges for technologists (e.g., [23]), but is far more than just a grand engineering effort. It is the potentially inextricable embedding of networked computation into the fabric of society, into the everyday lives of people [10]. As society begins to incorporate into itself not just technology per se, but the intricately networked, computationally rich tapestry of ubicomp, technologists must double as social scientists and make their best efforts to design systems responsive to the nuanced, evolving needs of society [1]. This paper represents the state of our efforts to do just that with regard to end-user understanding and management of privacy in ubiquitous computing.

The emergence of ubiquitous sensor networks and robust data mining techniques will amplify the tracking and profiling capabilities of *personal information* (PI) collectors. Adherence to *fair information practices* (e.g., [7]) requires PI collectors to provide suitable means of notice and consent to users, but the sheer volume of collection events would arguably overwhelm the general public if expected to acknowledge and (possibly) consent to every collection event. A simpler means of managing everyday privacy is necessary.

This paper aims to elucidate a conceptual model of everyday privacy in ubiquitous computing environments by which system designers and administrators can conceptualize the end-user privacy experience. By *everyday* privacy in ubicomp, we mean *individual* end-users' ongoing exposure to and influence over the collection of their personal information in ubicomp environments. Ubicomp system designers have a responsibility to support users' daily exposure to the privacy-sensitive aspects of such systems. We consider a cogent conceptual model requisite for the design of viable tools for empowering end-user management of privacy in ubicomp. We are concerned herein not with underlying infrastructural issues like trust modeling and encryption, but with the end-user experience itself, which we consider of paramount importance in the design of ubicomp systems.

Building on the insights of Goffman [12] and Ackerman [1], we extend our model into an interactional metaphor for the end-user. The *situational faces* metaphor encapsulates the complexity of everyday ubicomp privacy and provides interactional guidance for supporting *notice* and *consent*, which effectively comprise the everyday user interface of the privacy-sensitive aspects of a ubicomp system. According to our model, a user achieves understanding of the privacy implications of a given *situation* both intuitively and through adequate *notice*. In response, the user selects his preferred *face*, which is an abstraction of a permutation of *privacy preferences* applicable to the situation. These preferences are accessed by the ubicomp system and codify the user's conditional *consent* to disclose certain personal information in exchange for ubicomp services.

2 A Conceptual Model of Everyday Privacy in Ubicomp

A cohesive model of everyday ubicomp privacy must account for both large- and small-scale factors. In this section we develop a unified model of everyday ubicomp privacy by synthesizing Lessig's societal-scale model [16] with Adams's user perceptual model [2].

Privacy does not consist of a universal benchmark against which a given PI collection event can be measured. Its shape and scope vary across jurisdiction, culture, economy, time, and individual. Accordingly, the emergence of ubiquitous computing, with its attendant legal, cultural, economic, and personal adjustments, calls for a reevaluation of the shape of privacy [16]. In particular, ubicomp technologists need a simple yet cogent conceptual model of the workings of everyday privacy to support their efforts to incorporate privacy-sensitivity into their systems from design-time [15].

2.1 Societal-Scale Model of Privacy

Lessig, a legal scholar, describes the shape of privacy in a given place and time as contingent on four forces: *Law (L)*, *Market (M)*, *Norms (N)*, and *Architecture (A)* [16]. Briefly, *architecture* refers to technological context; what can and cannot be private is partially contingent on technological capability, and technology varies across temporal and spatial contexts [17].

The recognition that these four forces operate interdependently is crucial. Any significant shift in one force requires a compensatory adjustment in one or more of the others. Ubicomp is just such a shift in the realm of architecture, and corresponding shifts can already be noted in law (e.g., [8]), norms (e.g., [13]), and markets (e.g., [18, 19]).

The Lessig model is a convenient means of conceptualizing the influence of societal-scale forces on the shape of privacy, but these forces operate primarily beyond the reach of the individual. When an individual decides whether to disclose a set of PI in a given situation, he may have some awareness of the applicable laws, market forces, norms, and architecture, but the decision is still greatly influenced by subjective factors. A framework for conceptualizing ubicomp privacy must account for variations in the shape of privacy across individuals.

2.2 User Perceptual Model of Privacy

A model of privacy on the scale of a single PI collection event is necessary to complement Lessig's broad model. Adams has conducted empirical investigations into individual users' perceptions of privacy in multimedia environments [3], i.e., environments outfitted with audio/video capture equipment. Individuals are comfortable revealing certain PI in certain situations based in part on how private they *perceive* the situation to be. Note that, through the use of inconspicuous sensors, the situation can be less private than the user thinks [2]. Adams's analysis has identified three interdependent factors determining users' perception of privacy in such environments:

Information Sensitivity (IS): The user performs a subjective *judgment* of the sensitivity of the information she (perhaps inaccurately) perceives as being disclosed.

Information Receiver (IR): The user evaluates the level of *trust* she has in the perceived (not always actual) recipient(s) of the information.

Information Usage (IU): The user assesses the expected *costs and benefits* of the perceived current and future usages the recipient will make of the information.

In the *context* of a given situation, these factors largely determine the user's perception of privacy. This model describes the process the user undergoes in determining whether, and to what degree, her privacy has been or would be invaded by a PI collection event that has occurred or may occur.

The Adams model is useful for conceptualizing the influence of perceptual and contextual factors on the shape of privacy in multimedia and, we believe, ubicomp environments, but it does not directly address the influence of societal-scale forces, abstracting them and other situational factors into the nebulous category of *context*. A framework for conceptualizing ubicomp privacy must account for the forces that determine the context of a PI collection event and the range of possible information receivers and usages.

2.3 Everyday Ubicomp Privacy: A Synthesis

We propose a direct synthesis of the Lessig and Adams models as a framework for conceptualizing privacy in ubiquitous computing environments, in which the *context* referred to in the Adams model is the confluence of (1) the societal-scale forces of the Lessig model, and (2) traditional contextual factors (e.g., activity, time, location, companions, user's role, etc.). Legal, market, normative, and architectural forces, in conjunction with contextual factors, constrain the possible levels of privacy of a given set of PI in a given situation. Within this constrained range, the user's subjective values, informed by the perceptual factors of the Adams model, determine the actual level of preferred privacy.

We present the following formula as a condensed representation of our conceptual model of everyday privacy in ubicomp:

$$preferred\_privacy\_level = user(L, M, N, A, C, PI, IS, IR, IU) \quad (1)$$

where *user* is the user's internalized value system; *L*, *M*, *N*, and *A* are the forces from the Lessig model; *C* is the set of contextual variables (e.g., activity, location, companions, etc.); *PI* is the personal information being disclosed; and *IS*, *IR*, and *IU* are perceptual factors from the Adams model. For those concerned with privacy management in organizational environments, we offer that, for the purposes of this general model, organizational policies are subsumed under Laws and Norms.

Given this model, for an individual to exhibit informed control over the release of his PI, he needs (1) to know the values, so to speak, of the aforementioned nine parameters, and (2) the ability to effect his preferred privacy level in a situation. We address these needs in the following section.

3 Situations and Faces

The model presented above can assist system designers and administrators in conceptualizing everyday privacy in ubicomp, but its explicit parameterization of real-life invalidates it as a general model for the consideration of end-users. In this section we encapsulate the inherent complexity of the model in a metaphor for end-users, building on the insights of Goffman [12] and Ackerman [1]. The *situational faces* metaphor affords interactional mechanisms for taming the deluge of notice and consent events [15] that promise to overwhelm users in a sensor-rich ubicomp environment.

3.1 Notice and Consent

Legislators, businesses, and advocates have identified a set of *Fair Information Practices* common to most privacy-protecting legislation (e.g., [7]). PI collectors subscribing to these practices are generally considered ethical in that capacity. Among these practices, *notice*, the notification of the individual of the collection and use of PI, and *consent*, the ability of the individual to selectively approve PI collection, are of greatest everyday utility to users concerned with the ongoing collection of PI in

ubicomp. While other fair information practices (e.g., access, security, redress) are critical components of ethical PI collection, notice and consent are the particular practices that individual end-users encounter on an ongoing basis.

As such, notice and consent are the means by which a user gains feedback from and exhibits control over the privacy-sensitive aspects of a ubicomp system. They effectively comprise the user interface of those aspects of the system, the recurrent interaction with which engenders the user's conceptual model of the system [20]. If users are to develop the ability to comfortably manage ubicomp privacy, they will arguably do so through their exposure to well designed feedback and control mechanisms [6]. Notice can also mitigate the disparity between the user's perception of privacy and the actual level of privacy in a situation, thereby addressing one of Adams's concerns [4]. Notice of information usage is particularly important when disclosure of PI is viewed as compensation for a service. People may not want to reveal certain information unless they know they are getting something of value in return [11].

In the remainder of this section we explain how notice and consent in ubicomp can be supported on the interactional level by extending our model of everyday ubicomp privacy into a metaphor we call *situational faces*.

3.2 Situations: Supporting Notice

We have thus far discussed privacy in the vague context of a "given situation". Here we define "situation" formally. A *situation* is a permutation of the nine parameters in (**1**). Given a specific permutation of these variables, an individual makes a subjective judgment of his preferred privacy level. Replacing *L, M, N, A, C, PI, IS, IR, IU* in (**1**) with *situation* leaves us with:

$$preferred\_privacy\_level = user(situation)\ . \qquad (\mathbf{2})$$

For an individual to make an informed ubicomp privacy decision, he needs adequate knowledge of the variables encapsulated by the situation variable. Arguably, much of this knowledge is implicit in a situation or internalized through the course of one's development (i.e., one learns to obey the law without learning every letter of it; one naturally subscribes to certain social norms; one grows accustomed to market and architectural forces) or through recurrent exposure to routines [21], and some of it is particularly subjective (e.g., information sensitivity). The values of the remaining situational variables, in particular but not necessarily limited to information receiver, information usage, and classes of PI, need to be communicated to the user to enable an informed privacy decision. That is, in accordance with fair information practices, *notice* must be given to the user.

In an environment rife with networked sensors attuned to human behavior, PI collection events are too numerous to expect users to reasonably put up with incessant beeping, blinking, or vibrating notifications. One solution we are investigating is the posting of visible signage in ubicomp environments, using standardized symbols and labels [22] to indicate the values of the notification variables, similar to roadway signs. In accordance with the Boundary Principle described by Kindberg and Fox [14], we expect signage can be strategically placed near the boundaries between

discrete ubicomp environments. We are also investigating the use of wireless beacons to broadcast notification to wearable and handheld computers for real-time feedback and to aid in end-user logging of PI collection events.

Adequate notification, in conjunction with the user's naturally honed ability to distinguish between situations, can clarify the situation enough for the user to make an informed decision about the disclosure of her PI. But once informed, the user needs a means of effecting consent, if she indeed consents.

3.3 Faces: Supporting Consent

Manually handling the considerable frequency of PI collection events in ubicomp would overwhelm any reasonable user. But the alternative to amortized consent is equally burdensome: the user is faced with the configuration of an exponentially complex space of *privacy preferences*, which we can operationally define as the situational codification of conditional consent. Examples of ubicomp privacy preferences might include *identify me only if…*, *track my location only if…*, *crawl my calendar and to-do list only if…*, *capture me visually only if….*, where "*only if…*" implies conditional approval contingent on situational factors. Existing technical standards, like P3P [24], may be applicable here. Presumably, preferences would be persistently stored either on a wearable or handheld computer, or in a network-accessible location.

Users are notoriously hesitant to configure a large set of highly descriptive preferences, but are comfortable managing a few simple, opinionative variables [9]. The challenge, then, is to represent descriptive permutations of privacy preferences with a high-level abstraction that affords the user a means of subjectively conceptualizing privacy in a given situation.

We offer the metaphor of *faces* to represent the set of permutations of ubicomp privacy preferences an individual engages in the course of her everyday life. As she encounters a new *situation*, the user dons the appropriate *face (*e.g., *secure shopper*, *cocktail party*, *hanging out with friends*, *anonymous*, *family outings*, *traveling abroad*, etc.). Users can concern themselves primarily with their collection of faces, and less so with the underlying preferences they abstract.

This abstraction is derived from Goffman [12] and Ackerman [1]. Offline, in the real world, people seamlessly switch "faces" between situations, but online this practice is impeded by the recurrence of mouse clicks, HTML forms, and menus that are the means by which a user actively constructs or selects a "profile". As the architectural convergence of the online and embodied worlds, ubicomp effectively mandates a more seamless way of switching digital faces.

Replacing *preferred_privacy_level* with *face* in (**2**) reveals our final formula:

$$face = user(situation)\ . \qquad (\mathbf{3})$$

(**3**) is many-to-one. A user may wear the same face in different situations. While conceivable that faces could be automatically selected based on automatic sensing and interpretation of situational variables, the AI challenge implicit in that task can be avoided by establishing the user himself as the primary executive of the process. If a user's set of faces is sufficiently small, it can be represented linearly, affording rapid

manual face selection in real-time using established or emerging [5] interaction techniques. Supporting the configuration and selection of faces presents significant challenges for interaction designers.

4 Conclusion and Future Work

We have presented a conceptual model of everyday privacy in ubiquitous computing environments that can assist system designers and administrators in understanding the factors contributing to the end-user privacy experience in a given situation. The model accounts for the influence of societal-scale forces, contextual factors, and subjective perception on the shape of privacy.

The *situational faces* metaphor, inspired by Goffman and Ackerman, encapsulates the complexity of the model and provides interactional guidance for supporting notice and consent, which effectively comprise the everyday user interface of the privacy-sensitive aspects of a ubicomp system. According to our model, a user achieves understanding of the privacy implications of a given *situation* both intuitively and through adequate *notice*. In response, the user selects his preferred *face*, which is an abstraction of a permutation of *privacy preferences* applicable to the situation. These preferences are accessed by the ubicomp system and codify the user's conditional *consent* to disclose certain personal information in exchange for ubicomp services.

This paper has focused on the experience of the individual in managing privacy in ubicomp. Further research is required to investigate techniques for accommodating the privacy needs of cooperative groups.

We are presently conducting research into empirical validation of the conceptual model presented in this paper and user interaction techniques supporting it. We are addressing the former through ethnography and user studies. Regarding the latter, we are exploring UI techniques for providing unobtrusive but adequate notice, methods for configuring and combining faces, and techniques for rapidly selecting faces.

Acknowledgements

We would like to thank Xiaodong Jiang, John Canny, Deirdre Mulligan, Jason Hong, and danah boyd for their contributory insights.

References

1. Mark S. Ackerman. The Intellectual Challenge of CSCW: The Gap between Social Requirements and Technical Feasibility. In John M. Carroll, editor, *Human-Computer Interaction in the New Millenium*. Addison-Wesley, Reading, MA, 2002.
2. Anne Adams. The Implications of Users' Privacy Perception on Communication and Information Privacy Policies. In *Proceedings of Telecommunications Policy Research Conference*, Washington DC, 1999.

3. Anne Adams. Multimedia information changes the whole privacy ballgame. In *Proceedings of Computers, Freedom, and Privacy*, 2000.
4. Anne Adams. & M. A. Sasse. Taming the wolf in sheep's clothing: privacy in multimedia communications. In *Proceedings of ACM Multimedia*, 1999.
5. Brian Amento, Will Hill, Loren Terveen. The Sound of One Hand: A Wrist-mounted Bio-acoustic Fingertip Gesture Interface. In *Proc. Of CHI 2002*.
6. Victoria Bellotti and A. Sellen. Design for privacy in ubiquitous computing environments. In *Proc. of the European Conference on Computer-Supported Cooperative Work*, 1993.
7. Center for Democracy and Technology. Generic Principles of Fair Information Practices. http://www.cdt.org/privacy/guide/basic/generic.html.
8. Center for Democracy and Technology. Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices. Before the Federal Communications Commission, Washington, D.C. See HTML version http://www.cdt.org/privacy/issues/location/010406fcc.shtml.
9. Lorrie Faith Cranor and Joseph Reagle, Jr. Designing a Social Protocol: Lessons Learned from the Platform for Privacy Preferences Project. In *Proc. Of the Telecommunications Policy research Conference*, Alexandria, VA, Sept. 27-29, 1997.
10. Paul Dourish. *Where the Action Is*. MIT Press, Cambridge, MA, 2001.
11. Simson Garfinkel. *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly and Associates, Cambridge, MA, 2001.
12. Erving Goffman, *The Presentation of Self in Everyday Life*. Anchor-Doubleday, New York, NY, 1961.
13. Rebecca E. Grinter & Margery A. Eldridge, "y do tngrs luv 2 txt msg?" In *Proceedings of the European Conference on Computer-Supported Cooperative Work*, 16-20 September 2001, Bonn, Germany.
14. Tim Kindberg and Armando Fox. System Software for Ubiquitous Computing. In *IEEE Pervasive Computing*, v.1 no. 1, 2002.
15. Mark Langheinrich. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In *Proc. Of Ubicomp 2001*.
16. Lawrence Lessig. The Architecture of Privacy. Paper presented at Taiwan Net Conference, Taipei, March 1998. See HMTL version http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf.
17. Lawrence Lessig. *Code and Other Laws of Cyberspace*. Basic Books, New York, NY, 1999.
18. The Liberty Alliance Project. http://www.projectliberty.org/.
19. Microsoft .NET Passport. http://www.passport.com/.
20. Donald A. Norman. *The Psychology of Everyday Things*. Basic Books, New York, NY, 1988.
21. Peter Tolmire, James Pycock, Tim Diggins, Allan MacLean, and Alain Karsenty. Unremarkable Computing. In *Proc. Of CHI 2002*.
22. TRUSTe. Privacy Symbols and Labels Initiative. http://www.truste.org/bus/symbols.html
23. Mark Weiser. Some Computer Science Issues in Ubiquitous Computing. In *Communications of the ACM*, 36(7), 75-83, 1993.
24. World Wide Web Consortium. Platform for Privacy Preferences Project. http://www.w3c.org/P3P.