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@cs.berkeley.edu

Abstract. We present a conceptual model of everyday privacy in ubiquitous computing environments, based on the works of Lessig and Adams. By *everyday privacy*, we mean the end-user's ongoing exposure to and control over personal information collection. 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 *faces*, designed to mitigate the complexity of privacy for the end-user. Users vary the *face* they wear depending on the recipient and/or situation, where a face is a meaningful encapsulation of privacy preferences.

1 Introduction

Ubiquitous computing, or ubicomp, presents significant challenges for technologists (e.g., [16]), 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 [9]. 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 beginning 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., [6]) 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 proposes a conceptual model of everyday privacy in ubicomp and an interactional metaphor to simplify its management. By *everyday* privacy in ubicomp, we mean individual end-users' ongoing exposure to and control 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 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 and Ackerman, we extend our model into an interactional metaphor for the end-user. The *faces* metaphor tames the complexity of everyday ubicomp privacy with a high-level metaphor 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 assigns a *face*, which is an abstraction of a permutation of *privacy preferences,* to a given recipient or 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 [13] with Adams's user perceptual model [2].

Lessig, a legal scholar, describes the shape of privacy in a given place and time as contingent on the convergence of four forces: *Law (L)*, *Market (M)*, *Norms (N)*, and *Architecture (A)*. 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 [14]. 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 model of privacy on the scale of a single PI collection event is necessary to complement Lessig's broad model.

Adams [3] has shown that, in a given audio/video-captured environment, four interdependent factors determine an individual's *perception* of privacy: the information *recipient*, the intended *usage* of the information, the information *sensitivity*, and the *context* in which the disclosure occurs. 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.

2.1 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.) [8]. 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 (see Figure 1).

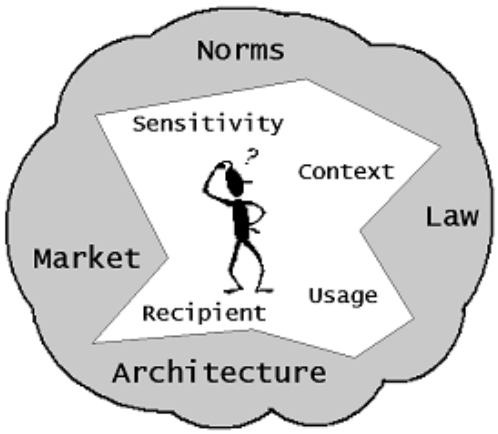

Figure 1. Macro and micro factors shaping an individual's preferred level of privacy in a given situation.

3 Faces: A Metaphor for End-User Management of Privacy

The model presented above can assist system designers and administrators in conceptualizing everyday privacy in ubicomp, but it remains too complex to serve 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 [11] and Ackerman [1]. The *faces* metaphor affords interactional mechanisms for taming the deluge of PI collection events [12] 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., [6]). 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 [15]. 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 [5]. 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 [10].

In the remainder of this section we explain how notice and consent in ubicomp can be supported on the interactional level by using PI disclosure logs incorporating interactional mechanisms for exercising access and redress, and by extending our model of everyday ubicomp privacy into the *faces* metaphor.

3.2 Supporting Notice with Logs

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. We believe that notice should be logged by the user-agent for subsequent review. All PI collection attempts, whether successful or not, would be logged. Users can review recent PI collection events after the fact. At first thought, this may sound counterproductive; after all, we want to prevent unwanted PI collection, not simply complain about it afterwards. Opt-in is generally preferred to opt-out amongst privacy advocates. However, two factors can contribute to the feasibility of this approach:

1. Fair Information Practices require that PI collectors provide appropriate means of access and redress. If a user reviews her PI disclosure logs and disapproves of a certain collection, she can click through to retract or edit her information. Naturally, this requires broad and faithful adherence to fair information practices, but market pressures in the PI economy may ensure adherence to this model.
2. Users can designate a default setting to not disclose PI to collectors with which they are unfamiliar. This way, they would subsequently review notice of the PI they *would have* disclosed had their user-agent allowed it. They can then, if desired, program their user-agent to disclose appropriate PI on subsequent exposure to that collector. Or perhaps the notice will come embedded with have a valid service offer.

3.3 Supporting Consent with Faces

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 [17], 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 [7]. 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 [11] 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.

After reviewing notices in her PI disclosure log, a user could assign the appropriate face to handle future PI collection by a given recipient, or class of recipient. Such recipients would always receive information filtered by the assigned face, regardless of the situation, or the assigned face could be parameterized to

vary by situation. Users might also assign faces to activate in certain situations, to handle PI collectors to whom they user has not assigned a face. Users could also activate faces on the fly for this same purpose.

4 Conclusion and Future Work

We have presented a conceptual model of everyday privacy in ubiquitous computing environments. The model accounts for the influence of societal-scale forces, contextual factors, and subjective perception on the shape of privacy. The *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 assigns *faces, i.e.*, permutations of *privacy preferences,* to recipients and/or situations. 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.

We are presently designing a ubicomp user interface to support creation and management of faces, and dynamic assignment of faces to recipients and situations.

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. Victoria Bellotti and A. Sellen. Design for privacy in ubiquitous computing environments. In *Proc. of the European Conference on Computer-Supported Cooperative Work*, 1993.
6. Center for Democracy and Technology. Generic Principles of Fair Information Practices. http://www.cdt.org/privacy/guide/basic/generic.html.
7. 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.
8. Anind K. Dey and Gregory D. Abowd. *Towards a Better Understanding of Context and Context-Awareness.*In the Workshop on The What, Who, Where, When, and How of Context-Awareness, as part of the 2000 Conference on Human Factors in Computing Systems (CHI 2000), The Hague, The Netherlands, April 3, 2000.
9. Paul Dourish. *Where the Action Is*. MIT Press, Cambridge, MA, 2001.
10. Simson Garfinkel. *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly and Associates, Cambridge, MA, 2001.
11. Erving Goffman, *The Presentation of Self in Everyday Life*. Anchor-Doubleday, New York, NY, 1961.
12. Mark Langheinrich. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In *Proc. Of Ubicomp 2001*.
13. 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.
14. Lawrence Lessig. *Code and Other Laws of Cyberspace*. Basic Books, New York, NY, 1999.
15. Donald A. Norman. *The Psychology of Everyday Things*. Basic Books, New York, NY, 1988.
16. Mark Weiser. Some Computer Science Issues in Ubiquitous Computing. In *Communications of the ACM*, 36(7), 75-83, 1993.
17. World Wide Web Consortium. Platform for Privacy Preferences Project. http://www.w3c.org/P3P.