Information School

Reflections on Usable Privacy for Location-Awareness Systems

Batya Friedman

Technical Report IS-TR-2005-06-02

June 29, 2005

Information School
University of Washington
Suite 370 Mary Gates Hall, Box 352840
Seattle, WA 98195-2840

Phone: (206) 616-7490
Fax: (206) 616-3152
Email: batya@u.washington.edu
Web: www.ischool.washington.edu/vsd

Reflections on Usable Privacy for Location-Awareness Systems

Abstract. For the past decade, the Value Sensitive Design Research Lab now at the University of Washington has been investigating privacy in public in relation to information technologies. More recently, we have begun collaborations with the Intel Research Seattle lab to extend those investigations to location-awareness technologies. In this brief workshop paper, I offer ten propositions for privacy in the context of location-awareness technologies that have emerged from our work and continue to guide it. Finally, I end with a "deign to think with" for usable privacy.

Introduction

Community, at times, requires a sense of presence among its members and, at times, the ability for members to withdraw. Different moments, different roles, different community members, lend themselves to different balances among how individuals want to be known and in what ways and by whom. A long history of research and experience with deployed community, groupware, and collaborative technologies points to the tensions between supporting group awareness and privacy (see, for example, Boyle, Edwards, & Greenberg, 2000; Consolvo, Roessler, & Shelton, 2004; Fuchs , 1999; Hudson & Smith, 1996; Jancke, Venolia, Grudin, Cadiz, & Gupta, 2001; Svensson, Höök, Laaksolahti, & Waern, 2001; Tan & Czerwinski, 2003). Moreover, studies like Jancke et al. (2001), that introduced real-time video links between the semi-public kitchen spaces at Microsoft Research, highlight how lack of attention to privacy can undermine system adoption despite the potential benefits to community through awareness. Furthermore, as awareness systems provide access not only to people but also people's locations (in the semi-public arenas of the workplace, the more private arena of the home, and into public places at large), we can expect the tensions between awareness and privacy to intensify.

For the past decade, the Value Sensitive Design Research Lab now at the University of Washington has been investigating privacy in public (or semi-public) in relation to information technologies. Our work is grounded in the approach of Value Sensitive Design (Friedman, 1997, 2004: Friedman, Kahn, & Borning, in press), drawing on its interactional theory, integrative tripartite methodology of conceptual, technical and empirical investigations, and systematic analysis of direct and indirect stakeholders. More recently, we have begun collaborations with the Intel Research Seattle lab to extend those investigations to location-awareness technologies. With the hope that our work

might offer some useful insight into how the field might move forward, in this brief workshop paper I offer ten propositions for privacy in the context of location-awareness technologies that have emerged from our work and continue to guide it. I end with a "design to think with" for usable privacy of location-awareness technologies.

Privacy Propositions

Each of the propositions that follow has guided our work on usable privacy. Propositions I and II are more general observations about privacy and the integration of systems into society; hence the design implications that follow from those propositions are broad. The remaining eight propositions derive from our research and design endeavors and those of others working on usable privacy.

Proposition I: We can't anticipate all the value consequences of designing and deploying a particular information technology

A large body of literature points to unintended consequences from the introduction of technology, many of which affect important human values (see, for example, Houston, 1995 for a discussion of the impact of the introduction of snow mobiles to the Intuit on issues of status and autonomy; Sharp, 1952/1980 for a discussion of the introduction of steel axe heads to the Yir Yoront on issues of ownership; and Sproull & Kiesler, 1991 for a discussion of the introduction of email into western organizations on issues of hierarchy).

Two design implications follow. First, since we cannot anticipate all of the consequences, we cannot demand perfect designs – they are simply beyond our grasp. That said we can use and expect others to use "best practices". To the extent that the field has developed design practices responsive to privacy issues and at least partial design solutions, they should be employed and incorporated into our technologies. Second, having recognized that unanticipated value consequences are likely to emerge, we should design systems with the expectation that they will need to be adapted over time. For example, underlying system architectures should provide mechanisms for applications to be able to control the flow of information. Any given application may or may not take advantage of these mechanisms, but should the need arise those mechanisms will be in place within the deployed infrastructure. In our work on informed consent for cookies in web browsers (Friedman, Howe, & Felten, 2002), we observed this problem first hand. Specifically, users would like the opportunity to accept or decline a particular use of a particular cookie at a particular moment in time. However, the HTTP protocol automatically volunteers cookies once they have been set, thus precluding the possibility for users to intervene at the time of use.

Proposition II: Historically the bulk of our privacy protections have come from the difficulty and cost of accessing and manipulating information

Historically privacy protections have come less from regulation and more from the difficulty of collecting, accessing, manipulating, and analyzing information. For example, in the United States the public in principle has access to court records. However, until recently anyone who wanted to view a court record would need to travel physically to the court that housed that particular record, submit a request for the record, wait for the record to be located and retrieved, and then view a paper copy. Thus, only those individuals with the resources of time and funds for travel as well as significant incentive would incur the costs to access these public records. In recent years, courts have begun to put court records online and, in some cases, provide web access. In many of those jurisdictions, anyone with access to a computer and the Internet can with relative ease access these records in a matter of minutes from wherever they are connected. For example, while a high school student out of curiosity might be reluctant to walk into a court house to request the court records for a teacher under-going a divorce, that same student might have no qualms about accessing that same court record on the web from the comfort of home. Within Washington State, just such concerns prompted the Washington State Supreme Court to set a one-year review date for a court rule it had adopted that allows such online access to court records. Of note, our work that investigated people's social judgments about privacy in public (Friedman, Kahn, & Hagman, 2004) was instrumental (along with other research findings) in stimulating attention to and discussion about these concerns among many different groups; in turn, these groups actively brought these concerns to the attention of the Washington State Supreme Court with the above result (Honorable Donald Horowitz[1], personal communication, June 21, 2005).

More generally, when technology is introduced that enhances access to information we can expect it to unbalance privacy checks within the social fabric. Alongside of designing the technology, we will likely need to design social conventions, policies and laws to help re-establish a reasonable balance.

Proposition III: Privacy does not exist in isolation

The value of privacy is intricately connected to other key values such as security, trust, autonomy, and informed consent. For example, in our work on people's social judgments about privacy in a public place in which we surveyed 750 participants and interviewed an additional 120 participants (Friedman, Kahn, &

[1] The Honorable Donald Horowitz is a former Superior Court Justice and currently Chair, Access to Justice Technology Bill of Rights Committee of the Washington States Access to Justice Board.

Hagman, 2004), interview participants not only spoke about privacy, but connected their privacy judgments with other values. For example, when asked about a camera pointed toward a public plaza that displayed a video image in real-time in a nearby office, one participant said, "it's perfectly fine [to have the camera and display] as long as we're not capturing people, individual people. If it's just the scene then it's okay … cause hopefully no one's um privacy is being violated, uh that makes it you know okay I mean it's, it's a beautiful scene, if it adds to your ambience then go for it, yeah. If it's, if it's not hurting anybody". For this participant, the considerations of privacy are interwoven with considerations of *aesthetics* ("it's a beautiful scene") and *welfare* ("it's not hurting anybody"). In reflecting on similar questions, other participants responded with considerations of *physical welfare* (e.g., "for security reasons it would probably be helpful"), *psychological welfare* (e.g., "that's creepy", "that might make some people feel uncomfortable"), *property* (e.g., "Because of um property rights. My image, if I'm being looked at is a different, I feel a different property right even then if I'm being recorded…Because if I'm being recorded it's like any recording, a song or um a book you know how you have um copyright laws and intellectual property laws and those kinds of things"), and *informed consent* (e.g., "I think that that's um without my consent it, it violates my privacy").

Thus, designing for privacy requires engaging other fundamental values of import to stakeholders. Our research suggests that the values of trust, security, informed consent, autonomy, property, and welfare will be central here.

Proposition IV: Informed consent can be a useful tool for creating the conditions in which a balance between privacy and access can flourish

Informed consent provides a partial means to resolve the tension between privacy and access by turning some control for this trade-off over to the stakeholder about whom information will be collected and disseminated. We offer a model for informed consent of information systems (derived in large part from the Belmont Report) based on six components: *disclosure*, *comprehension*, *voluntariness*, *competence*, *agreement*, and *minimal distraction*. The word "informed" encompasses the first two components, disclosure and comprehension. The word "consent" encompasses the following three components, voluntariness, competence, and agreement. In addition, the activities of being informed and giving consent should happen with minimal distraction, without diverting users from their primary task or overwhelming them with intolerable nuisance. We have used this model to good success in examining cookies and web browser security, usable security of web browsing, and Google's web-based email system Gmail. Taken together, this work has investigated the possibilities and limitations for informed consent, informing through interaction design, and the

scope of informed consent (see Friedman, Howe, & Felten, 2002; Friedman, Lin, & Miller, in press).

Proposition V: Inference

When considering privacy, what must be taken into account is not just what is specifically known about an individual but what can be inferred about that individual from what is known. A significant body of literature from the data-mining and security communities had demonstrated that (a) a small number of pieces of information about a particular individual can be used to link an individual from one system to another, and (b) statistical behavior patterns from large samples can be used with good reliability to predict the behavior of a particular individual or individuals with particular profiles (again based on a small amount of information about that individual). Of importance for location-awareness technologies are the vulnerabilities that can come from exposure of one's location or location patterns over time. For example, based on statistical models derived from location information, a mugger may be able determine that someone usually walks on a particular dark side street between the hours of 5 – 8 PM every evening.

Informing users of the risks from inference is extremely challenging. After all, it is not obvious to most people how half a dozen seemingly unimportant pieces of information about a person's behavior provide exposure of the sort alluded to above. This is a hard problem for the field and one our Lab has just begun to engage. We suspect aspects of our informed consent work may be relevant here. In particular, we hope to be able to leverage some of the design analyses we developed in our investigation of informing through interaction design.

Proposition VI: At-risk populations

Ubiquitous information systems (and especially those focused on location) may increase the vulnerabilities for some groups (e.g., women, victims of domestic violence). Given this possibility, attention in the design needs to be paid these populations, perhaps in the form of warnings, usage models, user control, and so forth. In our work, we have begun to explore the use of warning labels similar to those that appear on containers of alcohol in the United States to warn pregnant women of the increased risk of birth defects associated with alcohol (e.g., "GOVERNMENT WARNING**:** ACCORDING TO THE SURGEON GENERAL, WOMEN SHOULD NOT DRINK ALCOHOLIC BERVERAGES DURING PREGNANCY BECAUSE OF THE RISK OF BIRTH DEFECTS".) An example of the sort of warning label that might appear on location-awareness systems is as follows: *Individuals who consider themselves "at-risk" for stalking (e.g., victims of domestic violence) should use caution when using [name of system] because*

exposing location information may increase the risk to their physical safety. Granted, this sort of warning label is just a beginning.

Proposition VII: Defaults matter

A well-established body of literature in human-computer interaction, computer-supported cooperative work, and related fields indicates that most people don't change the default settings on their machines (though some may relegate this job to trusted others in their organization or community). Here, we call attention to the importance of accounting for this user behavior in the design of location-awareness systems: Careful attention should be paid to privacy considerations when determining default settings.

Proposition VIII: Opt in or opt out?

For awareness systems, one basic default consideration is: Opt-in or opt out? From the perspective on community participation, an "opt-out" default is attractive because participants' systems are configured for participation unless the participant takes an explicit action otherwise. The reverse is the case with respect to privacy: an "opt-in" default is attractive because participants must take an explicit action if they want to share their information and hence benefit from the community interactions.

However, most of us live lives that are more fluid than a simple "opt-in" or "opt-out" strategy can accommodate. In some physical contexts with some people at some times, we are willing to share our location information. But, let another person walk into the room or our relationship with the original person change or we walk from inside an office into a hallway, and what we are willing to share may change in an instant (see Palen and Dourish, 2003). The more rigid conception of a "opt-in/opt-out" preference setting may not have the agility to respond to the nuanced and on-going negotiations of privacy and awareness in the human condition. Thus, in our current work we are exploring a new type of mechanism for allowing users to control their participation in location-awareness systems: "On-the-fly" opt in/opt out. The idea here is a simple ready-to-hand toggle switch that allows the user to rapidly toggle between an opt-in and opt-out participation in the system (see also the "design to think with" described below).

Proposition IX: Visible or invisible?

To realize the design implications that follow from Proposition IV (Informed consent) and Proposition VIII (Opt-in or opt-out?) users will need to know what information about them is being made available to others and when it is being made available. Otherwise, users are not positioned through an on-the-fly opt-in/opt-out mechanism (Proposition VIII) to participate in informed consent

(Proposition IV) in the nuanced way that is meaningful for social interaction. Hence, visibility of the right information at the right time is essential. Our work with cookies and web browsers (Friedman, Howe, & Felten, 2002) suggests that coupling peripheral awareness mechanisms with ready-to-hand information management may be a productive approach here.

Proposition X: Simplicity

As with defaults, there is a long standing body of research in human-computer interaction, computer-supported cooperative work, and interaction design that points to the desirability of simplicity (perhaps with successive levels of disclosure or complexity) (see Norman, 1998; Simon, 1969/1996). We suspect that the successful designs here will be simple ones.

A Device to Think With

In our lab, we have begun to think about how to integrate the implications of the above ten privacy propositions into interaction design for location-awareness systems. In the spirit of providing a "design to think with", we offer the sketch below. The sketch shows a simple hand-held device for helping users manage the privacy aspects of location-awareness applications. The orange (right-hand) side of the device is the "cell-phone" like interface for inbound-only information applications, such as GPS. When receiving such information, it would be virtually impossible to be tracked. The orange side is "privacy" strong. In contrast, the yellow (left-hand) side of the device is the "cell-phone" like interface for in-and-outbound information applications, such as talking or instant messaging. The yellow side provides additional capabilities, but with greater privacy risks. Any application that supports bi-directional communication (i.e., message passing of any sort) between two devices would reside on the yellow side. The yellow side of the device contains two additional features: (1) a notification method (e.g., red light, vibration) that signals the user a brief amount of time (on the order of tens of seconds) before the device sends information out, and (2) an on-the-fly opt-in/opt-out button that allows the user to easily toggle in real-time between (a) the device being on and potentially sending out data and (b) the device being off and not sending out (releasing) any data. Thus, users are positioned to know when information is about to be transmitted and have a simple ready-to-hand mechanism to control such information flow. Similarly, as users move fluidly in and out of physical environments and social interactions in which their desire to share or not share information changes, they can readily toggle information sharing applications "on" and "off".

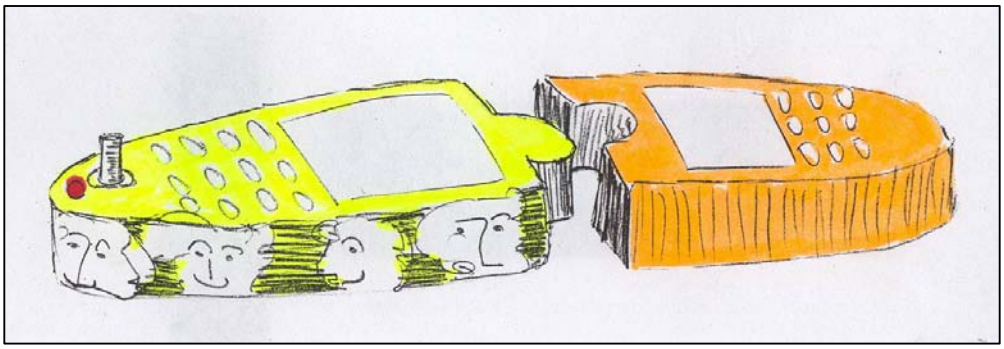

Figure 1. The sketch above shows a simple hand-held device for helping users manage the privacy aspects of location-enhanced applications. The orange (right-hand) side of the device is the "cell-phone" like interface for inbound-only information applications (such as GPS); the yellow (left-hand) side of the device is the "cell-phone" like interface for in-and-outbound information applications (such as IM).

Conclusion

We hope the privacy propositions offered here and the "design to think with" will provide useful material for others to build from and react against, as a means to stimulate positive designs that will move the field forward in addressing usable privacy for location-awareness systems.

Acknowledgments

Thanks to Sunny Consolvo, Nathan G. Freier, Peter H. Kahn, Jr., and Ian Smith for many thought provoking discussions about location-awareness computing and the related privacy implications. Aspects of this paper were presented by the author in the following talks. (2004, January 16 - 17): 'Human values in information system design', Keynote address at the *Technology, Values and the Justice System Conference*, Seattle, WA; (2004, January 30 - 31): 'Privacy in a public place', Keynote address at the *WHOLES Conference on A Multiple View of Individual Privacy in a Networked World*, Sigtuna, Sweden; and (2005, March 3): 'Privacy by design', Invited talk presented at the *Forum on Usable Privacy when Privacy is Ubiquitous*, Intel Corporation. Hillsboro, OR. This material is based, in part, upon work supported by the National Science Foundation under Grant Nos. IIS-0325035, IIS-0102558, IIS-9911185 and, in part, by a gift from Intel Corporation. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation or of Intel Corporation.

References

Boyle, M., Edwards, C., and Greenberg, S. (2000): 'The effects of filtered video on awareness and privacy', in *Proceedings of CSCW 2000.*

Consolvo, S., Roessler, P., and Shelton, B. E. (2004): 'The CareNet display: Lessons learned from an in home evaluation of an ambient display', in *Proceedings of Ubicomp 2004.*

Friedman, B. (ed.) (1997): *Human Values and the Design of Computer Technology*, Cambridge University Press and CSLI: New York, NY and Stanford, CA.

Friedman, B. (2004): 'Value Sensitive Design', in W. S. Bainbridge (ed.), *Berkshire Encyclopedia of Human-Computer Interaction* (769-774): Berkshire Publishing Group, LLC, Great Barrington, MA.

Friedman B., Howe, D. C., and Felten, E. W. (2002): 'Informed Consent in the Mozilla Browser: Implementing Value Sensitive Design', in *Proceedings of the 35th Hawaii International Conference on System Science.*

Friedman, B., Kahn, P. and Borning, A. (in press): 'Value Sensitive Design and Information Systems', to appear in P. Zhang & D. Galletta (eds.): *Human-Computer Interaction in Management Information Systems: Foundations*, M.E. Sharpe, New York.

Friedman, B., Kahn, P. H., Jr., and Hagman, J. (2004): 'The watcher and the watched: Social judgments about privacy in a public place', in *Online Proceedings of. CHI Fringe 2004*, Vienna, Austria.

Friedman, B., Lin, P., and Miller, J. K. (in press): 'Informed consent by design', in L. Cranor and S. Garfinkel (eds.): *Designing Secure Systems that People Can Use*, O'Reilly and Associates, Cambridge, MA:

Fuchs, L. (1999): 'AREA: A cross-application notification service for groupware', in *Proceedings of ECSCW 1999.*

Houston, J. (1995): *Confessions of an Igloo Dweller*, Houghton Mifflin, New York, NY.

Hudson, S. E., and Smith, I. (1996): 'Techniques for addressing fundamental privacy and disruption tradeoffs in awareness support systems', in *Proceedings of CSCW 1996*.

Jancke, G., Venolia, G. D., Grudin, J., Cadiz, J. J., and Gupta, A. (2001): 'Linking public spaces: Technical and social issues', in *Proceeding of CHI 2001*.

Norman, D. A. (1988): *The Design of Everyday Things*, Doubleday Press, New York NY.

Palen, L. and Dourish, P. (2003): 'Unpacking "privacy" for a networked world', in *Proceeding of CHI 2003.*

Sharp, L. (1980): 'Steel axes for stone-age Australians', in J. P. Spradley & D. W. McCurdy (eds.), *Conformity and conflict* (pp. 345-359): Little, Brown, & Company, Boston. (Reprinted from Human Organization, 1952, 11, 17-22)

Simon, H. A. (1969/1996): *The Sciences of the Artificial (third edition*), The MIT Press, Cambridge, MA.

Sproull, L., & Kiesler, S. (1991): *Connections: New ways of Working in the Networked Organization*, The MIT Press, Cambridge, MA..

Svensson, M., Höök, K., Laaksolahti, J., and Waern, A. (2001): 'Social navigation of food recipes', in *Proceedings of CHI 2001*.

Tan, D. S. and Czerwinski, M. (2003): 'Information voyeurism: Social impact of physically large displays on information privacy', in *Extended abstracts of CHI 2003.*