A Value Sensitive Design Investigation of Privacy for Location-Enhanced Computing

Nathan G. Freier[1], Sunny Consolvo[2], Peter H. Kahn, Jr. [3], Ian Smith[2], Batya Friedman[1]

[1]The Information School
University of Washington
Seattle, WA 91895
{nfreier, batya}@u.washington.edu

[2]Intel Research Seattle
1100 NE 45th Street, 6th Floor
Seattle, WA 98105
{sunny.consolvo, ian.e.smith}@intel.com

[3]Department of Psychology
University of Washington
Seattle, WA 98195
pkahn@u.washington.edu

ABSTRACT

Building on principles of Value Sensitive Design, this paper presents a preliminary conceptual and technical investigation of privacy for location-enhanced computing. The following features are considered: directionality of information flow, information management, interpretability, awareness, control, scope of disclosure, and risk & recourse. Each feature is considered at three levels of system design: technology, infrastructure, and application. Our goal is to create an analytic tool that, when completed, will provide designers with the means to recognize the privacy implications of their designs, and through their designs to proactively enhance privacy along with other enduring human values.

Author Keywords

Privacy, location-enhanced computing, ubiquitous computing, values, value sensitive design.

INTRODUCTION

Identifying one's own location or the location of another person, entity, or object is a fundamental part of the human experience. We rely on location information to travel from here to there, find resources such as food and shelter, and maintain our personal awareness, privacy, and safety. Parents are often concerned with the location of their children; and, likewise, children with their parents. Retail businesses have an interest in informing potential customers of the location of their stores, and customers want to be able to find stores. Governments have an interest in knowing who is within their jurisdiction; the U.S. electoral system, for example, would not function without voters' residential location information. Ultimately, keeping track of one's own location and the location of others is foundational to both psychological and societal well-being.

The balance is precarious, however, between the necessary dissemination of our location and the potential for the widespread abuse of recorded, networked, and statistically analyzed personal information. Technologies that can be used to identify an individual, record location, infer activity, and track this information over time are infiltrating the fabric of society. Everyday city-goers in industrialized nations experience video surveillance cameras (e.g., cameras in USPS stamp machines), GPS navigation systems, EasyPass electronic toll systems, and security access swipe cards. These technologies lend support to healthy social functioning by increasing safety, reducing traffic congestion, and limiting access to those who have clearance. However, as more technologies are designed and used in our everyday lives, and as the information collected by these technologies becomes intertwined in networks and databases, the potential for abuse increases dramatically.

This paper presents a first iteration on an analytic tool that designers can use to evaluate location-enhanced computing designs with respect to privacy.

RECENT LITERATURE ON PRIVACY IN LOCATION-ENHANCED COMPUTING

There is an emerging literature on designing to support privacy in ubiquitous computing applications. Barkhuus and Dey [2], for example, investigated users' conceptions of privacy in position-aware and location-tracking applications on mobile telephones. Beckwith [3] presented a case-study of ubiquitous computing applications in an assisted living facility where both residents and staff were tracked by sensors and ID badges. Hong and Landay [14] utilize the mechanisms of data tagging and infospaces to construct a conceptual system for ubiquitous computing that helps protect privacy and ensure security. Hong, Ng, Lederer, and Landay [15] discuss the application of a risk model to direct two specific design projects. Beresford and Stajano [4, 5] present a technical system that helps protect user privacy while providing the utility of location-tracking by utilizing pseudonyms and "mix zones." Langheinrich [17] presents principles upon which ubiquitous computing systems should be designed if they are to protect user privacy. He applies these principles to a design project in later work [18]. Others [19, 20, 21] have focused on defining and deconstructing the privacy space.

VALUE SENSITIVE DESIGN

Value Sensitive Design emerged in the 1990's as an approach to the design of information and computer systems that accounts for human values in a principled and comprehensive manner throughout the design process [8, 10, 12]. Two overarching goals motivate Value Sensitive Design: (1) be proactive about human values in system

design, and (2) do so in a manner that is principled, comprehensive, and systematic.

Value Sensitive Design emphasizes values with ethical import, including privacy, trust, human dignity, respect for person, physical and psychological well-being, informed consent, intellectual property, access, universal usability, freedom from bias, moral responsibility, and moral accountability. While emphasizing the moral perspective, Value Sensitive Design also accounts for usability (e.g., ease of use), conventions (e.g., standardization of technical protocols), and personal predilections (e.g., color preferences in a graphical interface).

Key features of Value Sensitive Design involve its interactional perspective, emphasis on direct and indirect stakeholders, and tripartite methodology.

Interactional Perspective

Value Sensitive Design is an interactional theory [11]: values are viewed neither as inscribed into technology (an endogenous theory) nor as simply transmitted by social forces (an exogenous theory). Rather people and social systems affect technological development, and new technologies shape individual behavior and social systems.

Direct and Indirect Stakeholders

Direct stakeholders refer to parties who interact directly with the computer system or its output. *Indirect stakeholders* refer to all other parties who are otherwise affected by the use of the system. For example, computerized medical records systems impact not only the direct stakeholders, such as doctors, nurses, insurance companies, and hospitals, but an especially important group of indirect stakeholders, the patients.

Tripartite Methodology

Value Sensitive Design systematically integrates and iterates on three types of investigations: *conceptual*, *empirical*, and *technical*.

Conceptual investigations comprise philosophically informed analyses of the central constructs and issues under investigation. For example, how does the philosophical literature conceptualize certain values and provide criteria for their assessment and implementation? What values have standing? How should we engage in trade-offs among competing values in the design, implementation, and use of information systems (e.g., access vs. privacy)? *Empirical* investigations focus on the human response to the technical artifact, and on the larger social context in which the technology is situated. The range of quantitative and qualitative methods used in social science research may be applicable, including observations, interviews, surveys, focus groups, experimental manipulations, measurements of user behavior and human physiology, contextual inquiry, collection of relevant documents, and interaction logs. *Technical* investigations focus on the design and performance of the technology itself. It is assumed that technologies provide value suitabilities that follow from their properties. Technical investigations can involve either retrospective analyses of existing technologies or the design of new technical mechanisms and systems.

The three types of investigations – conceptual, empirical, and technical – are employed iteratively such that the results of one investigation are integrated with those of the others, which, in turn, influence additional investigations.

In what follows, we offer our initial start at a conceptual and then technical investigation of privacy in location-enhanced computing.

A CONCEPTUAL INVESTIGATION OF LOCATION-ENHANCED COMPUTING

Below we describe a set of identified features of location-enhanced computing that has direct implications for user privacy: *directionality of information flow*, *information management*, *interpretability*, *awareness*, *control*, *scope of disclosure*, and *risk & recourse*.

Directionality of Information Flow

The direction in which information flows in any location-enhanced computing technology is critical to understanding the privacy implications of the technology. There are two classes of directionality (as understood from the location of the user): in-bound and out-bound. Infrastructures or applications that utilize an *in-bound* directionality (sometimes referred to as a passive or anonymous model) to provide location information only to the target device are inherently more protected with respect to possible privacy intrusions. Place Lab is an example of a system that uses an in-bound directionality of information flow explicitly to protect the privacy of users [16]. Infrastructures or applications that utilize an *out-bound* directionality (sometimes referred to as an active model) require users to divulge their location to the environmental data collectors. Any system that requires a transmission from users to the environment has an out-bound directionality. Others have identified directionality of information flow as an essential indicator of potential privacy harms [6].

When designing location-enhanced computing systems, designers ought to consider first and foremost the directionality of information flow. If the functionality that is to be supported does not require an out-bound transmission of information (e.g., pedometer and location tracking device for fitness training), designers are much better off from a privacy perspective designing their system with an in-bound directionality only. However, there may be circumstances in which a service requires some out-bound transmission (e.g., E911 services). In these circumstances, designers ought to consider the implications of privacy along the dimensions discussed next.

Information Management

Once information about the location of the user is collected, either locally on the user's device or somewhere on the network, it becomes critical to understand how the information is managed. At least four approaches to data protection appear in the literature. The most problematic approach from a privacy perspective is the centralized, unified storage of information; what we call *unprotected* information management. The centralized storage of information that has a unified representation of users and their location information provides open opportunity for malicious activity. Splitting information into separate, unconnected representations, an approach we call *modularity*, is less problematic. Al-Muhtadi, Hill, & Campbell [1] present an argument for why such an approach is appropriate in the context of location-aware computing. The *encryption* of location and identity information is a third approach. Finally, the use of temporary *pseudonyms* and mix zones is an alternative approach that claims to have the benefits of anonymous systems while increasing the utility of location-enhanced applications [4, 5].

Considering how the user's information is managed is critical to respecting user privacy. Efforts can be made to encrypt data both during transmission and in storage. Data can be modularized, and pseudonymity can be an effective protection mechanism. In addition to these approaches to information management, it is important to be aware that the longer information about users is stored, the greater the risk of privacy intrusion.

Interpretability

Considering the amount of effort required to interpret the collected information is important to understanding the potential privacy risks of a technology. Data that is transmitted or stored using standardized protocols increases interoperability but also provides opportunity for machine-automated interpretation. Information that has a high fidelity (e.g., vision or audio feeds) is inherently interpretable by humans.

Consider, for example, systems that are currently being developed that use location information and RFID object tags in the user's environment to infer user activity [22]. Such systems obviously have a great potential for utility but are also increasingly intrusive. Storing comprehensive information about the inferred activities reduces the amount of effort required by third parties to interpret the data. Systems that reduce the general interpretability of the collected information while maintaining the usability of the information for the specific purposes of the application are more protective of privacy.

Awareness

Privacy observant technologies usually require the informed consent of the user. Therefore, it is important that location-enhanced computing technologies provide mechanisms for user awareness of what information is being collected, how that information will be stored, where that information will be stored, how long the information will be stored, and to whom the information might be transferred. Friedman, Howe, and Felten [9] conducted a conceptual analysis of informed consent in online interactions. In their analysis, the function of being 'informed' requires disclosure on the part of the system and comprehensibility on the part of information being disclosed. We assume a similar construct within the dimension of awareness. That is, awareness requires not only that the appropriate information is disclosed to the user but also that the disclosure is communicated in a comprehensible form.

We classify technologies into two classes within the dimension of awareness: invisible and transparent. Technologies are *invisible* if they provide no mechanism for enabling user awareness. Weiser, Gold, and Brown [26] may have considered ubiquitous computing to ultimately result in invisible functioning, but from a privacy perspective, invisibility results in an uninformed user, and ultimately puts privacy at risk. *Transparent* systems, however, are those that disclose the appropriate information to the user in a form that is comprehensible.

Control

As with awareness, control is critical to supporting informed consent. In their analysis of informed consent in online interactions, Friedman et al. [9] considered 'consent' to include: voluntariness, competence, and agreement. We consider the dimension of control to include these three requirements as well. Voluntariness requires that the user is not coerced into the use of the system. Competence requires that the user be cognitively capable of judging the risks and benefits of allowing the system to track their location. Of course, we recognize that pragmatically this is a difficult, if not impossible, condition for designers to ensure. However, designers can make attempts to ensure that users are cognitively capable. For example, a system might be marketed to a specific population of an age commiserate with the risks and benefits of that system. Finally, agreement requires that the user be given the opportunity to opt-in or out prior to the collection of any personal information and prior to the distribution of any personal information. A system provides control to the user if it fulfills each of these requirements.

Scope of Disclosure

The scope of disclosure refers to how and to whom information about the user is distributed. There are at least five classes of this feature: *personal*, *interpersonal*, *institutional*, *organizational*, and *societal*. (There are likely more classes such as governmental but for the purposes of this paper we consider the five listed.) A *personal* disclosure occurs when information about the user is collected by that user's own device but is not communicated to any person or system beyond the device itself. In this case, the user is disclosing information to a personal device for the purposes of current or future

personal use. An *interpersonal* disclosure occurs when information about the user is transmitted directly to members of that user's social network. Note that how the personal information is transmitted is important to consider. A secure, point-to-point transmission between the personal devices of two members of the same social network is an interpersonal disclosure, but if that same information is communicated using a digital cellular network, the disclosure is both social and institutional (e.g., mMode). An *institutional* disclosure is one in which any information goes to/through a service-provider's network (e.g., Cingular Wireless, Safeway Club Cards). An *organizational* disclosure occurs when information about the user is communicated to his or her employer or within some other organizational setting (e.g., an online calendaring system or PARC's Active Badge system). Finally, a *societal* disclosure occurs when personal information is made available to members of society (e.g., political campaign contribution information available through Fundrace.org).

Designers must recognize that an application like Cingular's (previously AT&T's) mMode is designed to function within the social domain but is by definition also disclosing information within an institutional domain. In such a context, users may not recognize the implications.

Risk & Recourse

The *risk & recourse* feature of system design refers to the balance between the amount of risk users take on when disclosing personal information and the degree to which those users have recourse against those to whom the information is disclosed. Risk is directly related to the content of the information. How sensitive is the information? What can be accomplished by a malicious agent who has access to the information? How easily can the information be associated with other seemingly benign information resulting in greater potential for harm? Recourse refers to the user's ability to hold the recipient of a disclosure accountable for inappropriate use of the user's personal information. Recourse likely differs for each form of disclosure and, related to risk, the actual inappropriate use of the information. For example, with respect to the inappropriate use of a social disclosure, a user's mechanisms for recourse might be as basic as discontinuing the social relationship or publicly announcing the inappropriate use, thereby harming reputation. Likewise, institutional disclosures result in greater potential for recourse within the financial domain.

Technology	Infrastructure	Application	Directionality	Interpretability	Scope of Disclosure
Ultrasound			Either	Med	Organizational
Vision			Out-Bound	High	Any Level
Ultrawideband Radio			Either	Med	Organizational
	UbiSense		Out-Bound	High	Organizational
GPS			In-Bound	Low	Personal
Infrared			Either	Med	Personal, Social or Organizational
	Cricket (also uses Ultrasound)		In-Bound	Low	Personal
Wi-Fi			Either	Med	Any Level
	Place Lab		In-Bound	Low	Personal
Wi-MAX			Either	Med	Any Level
Bluetooth			Out-Bound	Med	Social or Organizational
		IcyPole	Out-Bound	High	Social
RFID			Out-Bound	Med	Organizational
Cellular			Out-Bound	High	Institutional
		OnStar (with GPS)	Out-Bound	High	Institutional
		E911	Out-Bound	Med	Institutional
		mMode	Out-Bound	High	Institutional
TV-GPS			Out-Bound	Med	Organizational
	Rosum		Out-Bound	Med	Organizational

Table 1. Privacy-related features of technologies, infrastructures, and applications.

A TECHNICAL INVESTIGATION OF LOCATION-ENHANCED COMPUTING

Building on principles of Value Sensitive Design, the above conceptual investigation can now be employed to help structure the first iteration of a technical investigation. Specifically, we sought to analyze the privacy-related features of a handful of important and emerging technologies, infrastructures, and applications. The technologies are comprised of ultrasound, vision, ultrawideband radio, GPS, infrared, WiFi, WiMAX, Bluetooth, RFID, cellular, and TV-GPS. (See [13] for a brief review of location-enhanced technologies.) The infrastructures are comprised of UbiSense, Cricket, PlaceLab, and Rosum. The applications are comprised of IcyPole, OnStar, E911, and mMode.

Table 1 provides an overview of our technical investigation. Each row of the table represents a technology, infrastructure, or application within the area of location-enhanced computing. Each is evaluated along the dimensions of directionality, interpretability, and scope of disclosure. We have excluded information management, awareness, control, and accountability from the table, as they are primarily associated with the application layer of the system design, and as such, require a more complex technical analysis then we were able to conduct for the purposes of this paper. This table allows the reader to see which features of which technologies, infrastructures, or applications represent potential privacy risks to users.

Each feature relates differently to the three system design layers of technology, infrastructure, and application in location-enhanced computing. Applications ultimately reflect the features of the technologies and infrastructures upon which they are built in addition to those features associated specifically with the application layer; thus it is critical to consider all three layers in any investigation of an application.

DISCUSSION

There are a number of pragmatic reasons for designers to consider privacy in location-enhanced computing. From a market perspective, designers need to recognize that there are financial incentives to systematically account for privacy issues in design. For example, PARC's Active Badge Location System [25] was widely considered a powerful but ultimately unfriendly technology because it neglected to account adequately for privacy concerns in the design. Intel suffered a public relations setback when it announced that its Pentium III PC processors would ship equipped with embedded unique identifiers [7, 23]. Tang [24] investigated the economic and value implications for a company that neglected to install an on/off switch in the microphones of its PC products. Each of these examples illustrates the financial benefits for considering privacy, especially when designing systems that are as inherently intrusive as location-enhanced technologies.

Building on principles of Value Sensitive Design, we have offered our initial start at a conceptual and then technical investigation of privacy in location-enhanced computing. In future work, we expect to extend these investigations, and iterate on empirical investigations as well. Our goal is to create an analytic tool that, when completed, will provide designers with the means to recognize the privacy implications of their designs, and through their designs to proactively enhance privacy along with other enduring human values.

ACKNOWLEDGMENTS

This work was funded in part by National Science Foundation Award IIS-0325035.

REFERENCES

1. Al-Muhtadi, J., Hill, R., & Campbell, R. A privacy preserving overlay for active spaces. *UbiComp 2004 Privacy Workshop*, Nottingham, England, 2004.
2. Barkhuus, L., & Dey, A.K. Location-based services for mobile telephony: a study of users' privacy concerns. *INTERACT 2003, 9th IFIP TC13 Int'l Conference on Human-Computer Interaction*, 2003.
3. Beckwith, R. Designing for ubiquity: The perception of privacy. *Pervasive Computing, Apr-Jun*, 2003.
4. Beresford, A.R. & Stajano, F. Location privacy in pervasive computing. *Pervasive Computing,* Jan-Mar, 2003.
5. Beresford, A.R., & Stajano, F. Mix zones: User privacy in location-aware services. *IEEE Workshop on Pervasive Computing & Communication Security*, 2004.
6. Borriello, G. Privacy through broadcast and anonymous response. *UbiComp 2004 Privacy Workshop*. Nottingham, England, 2004.
7. Center for Democracy and Tech. Complaint and request for injunction, request for investigation, and for other relief. Federal Trade Commission, 1999. Online at http://www.cdt.org/privacy/issues/pentium3/990226intelcomplaint.shtml.
8. Friedman, B. (Ed.). *Human Values and the Design of Computer Technology*. NY: Cambridge Univ. Press, 1997.
9. Friedman, B., Howe, D. C., & Felten, E. Informed consent in the Mozilla browser: Implementing Value-Sensitive Design. *Proceedings of the 35th Annual Hawai'i Int'l Conference on System Sciences*, 2002.
10. Friedman, B. & Kahn, P. H., Jr. Human agency and responsible computing: Implications for computer system design. *Journal of Systems Software*, *17*: 7-14, 1992.
11. Friedman, B. & Kahn, P. H., Jr. Human values, ethics, and design. In J. A. Jacko and A. Sears (Eds.), *The Human-Computer Interaction Handbook*, 1177-1201. Mahwah, NJ: Erlbaum, 2003.

12. Friedman, B., Kahn, P. H., Jr., & Borning, A. Value sensitive design and information systems. To appear in D. Galletta & P. Zhang (Eds.), *Human-Computer Interaction in Management Information Systems*. Armonk, NY: Sharpe, in press.

13. Hazas, M., Scott, J., & Krumm, J. Location-aware computing comes of age. *Computer*, February, 2004.

14. Hong, J., & Landay, J.A. An architecture for privacy-sensitive ubiquitous computing. *MobiSYS '04*, 2004.

15. Hong, J., Ng, J.D., Lederer, S., & Landay, J. Privacy risk models for designing privacy-sensitive ubiquitous computing systems. *DIS2004*, 2004.

16. LaMarca, A., et al. Place Lab: Device positioning using radio beacons in the wild. *Proceedings of the 3rd Int'l Conference on Pervasive Computing, May 2005*, to appear.

17. Langheinrich, M. Privacy by design – principles of privacy-aware ubiquitous systems. *Proceedings of the 3rd Int'l Conference on Ubiquitous Computing*, 273 – 291. Atlanta, Georgia, USA, 2001.

18. Langheinrich, M. A privacy awareness system for ubiquitous computing environments. *Proceedings of the 4th Int'l Conference on Ubiquitous Computing*, 237 – 245. Göteborg, Sweden, 2002.

19. Lederer, S. Designing disclosure: Interactive personal privacy at the dawn of ubiquitous computing. *Master's Thesis Report*, Computer Science Division, University of California at Berkeley, 2003.

20. Lederer, S., Mankoff, J., & Dey, A.K. Towards a deconstruction of the privacy space. Presented at *UbiComp 2003 Privacy Workshop*, 20.

21. Palen, L. & Dourish, P. Unpacking "privacy" for a networked world. *CHI 2003*, Ft. Lauderdale, FL, 2003.

22. Philipose, M., Fishkin, K.P., Perkowitz, M., Patterson, D., & Hähnel, D. The probabilistic activity toolkit: Towards enabling activity-aware computer interfaces. *IRS-TR-03-013*, 2003. Online at http://www.intel-research.net/Publications/Seattle/012020041254_212.pdf.

23. Sprenger, P. Intel on privacy: 'Whoops!' *Wired News*, 10:45 AM, Jan. 25, 1999. Online at http://www.wired.com/news/politics/0,1283,17513,00.html.

24. Tang, J. Eliminating a hardware switch: Weighing economics and values in a design decision. In Friedman, B. (Ed.) *Human Values and the Design of Computer Technology*. Stanford, CA: Center for the Study of Language & Info, 259-269, 1997.

25. Want, R., Hopper, A., Falcão, V., & Gibbons, J. The active badge location system. *ACM Transactions on Information Systems, 10(1)*: 91-102, 1992.

26. Weiser, M., Gold, R., Brown, J.S. The origins of ubiquitous computing research at PARC in the late 1980s. *IBM Systems Journal, 38(4)*, 1999.