# Development of a Privacy Addendum for Open Source Licenses: Value Sensitive Design in Industry

Batya Friedman[1], Ian Smith[2], Peter H. Kahn Jr.[3],
Sunny Consolvo[2], and Jaina Selawski[4]

[1] Information School
University of Washington, Seattle, WA, USA
batya@u.washington.edu
[2] Intel Research, Seattle, WA, USA
{ian.e.smith, sunny.consolvo}@intel.com
[3] Department Of Psychology
University of Washington, Seattle, WA, USA
pkahn@u.washington.edu
[4] Intel Corporation, Santa Clara, CA, USA
jaina.c.selawski@intel.com

**Abstract.** Drawing on Value Sensitive Design, we developed a workable privacy addendum for an open source software license that not only covers intellectual property rights while allowing software developers to modify the software (the usual scope of an open source license), but also addresses end-user privacy. One central innovation of our work entails the integration of an informed consent model and a threat model for developing privacy protections for ubiquitous location aware systems. We utilized technology that provided a device's location information in real-time: Intel's POLS, a "sister" system to Intel's Place Lab. In January 2006, POLS was released under a license combining the substantive terms of the Eclipse Public License together with this privacy addendum. In this paper, we describe how we developed the privacy addendum, present legal terms, and discuss characteristics of our design methods and results that have implications for protecting privacy in ubiquitous information systems released in open source.

## 1 Introduction

Within the fields of ubiquitous computing and human-computer interaction, there has been increasing attention to issues of privacy. One strand of research, for example, has investigated users' views, values, and experience of privacy with respect to novel ubiquitous technologies [5,6,14,22,24,28,31]. A second strand has investigated conceptual models for privacy management that, in turn, can be used to guide subsequent technical work [1,25,27,30]. A third strand has investigated privacy-sensitive technical solutions [3,4,7,11,16,20,21].

All three strands remain vitally important. At the same time, we sought to break some new ground – conceptually, technically, and with respect to social policy. Specifically, we asked ourselves: Is it possible to create a workable open source software license that addresses the privacy rights of end-users of software in addition

P. Dourish and A. Friday (Eds.): Ubicomp 2006, LNCS 4206, pp. 194 – 211, 2006.

to the usual provisions of such licenses (that seek to protect, for example, intellectual property rights and the ability of software developers to modify the source code)? If so, what would such privacy protections look like? Can these protections be translated into enforceable legal terms? Should the protections be defined specifically for location aware systems, or could the protections and corresponding terms be defined more generally for ubiquitous information systems overall? How would the privacy terms be shaped by the technology and, in turn, how might the terms impact the technology development, interaction design, and user experience?

To even begin to answer such difficult questions, we believed we needed two components. First, we needed an actual implementation of technology that created potential privacy implications to think with and act upon. Here we chose a system for providing a device's location information in real-time – Intel's POLS (the Privacy Observant Location System, a "sister" system to Intel's Place Lab [26]). Second, we needed a robust research and design methodology to help structure our analyses. Here we utilized Value Sensitive Design [9,12,13].

In this paper, we first provide a brief background on open source software licenses, POLS, and Value Sensitive Design. Next we report on one of our central innovations: the working out individually of an informed consent model and a threat model for a ubiquitous location aware system, and then integrating the results of both models in the development of the privacy addendum. Then we present the legal terms of the addendum itself, emphasizing the intellectual source of its various terms. Finally, we conclude with a statement of our contributions, and some open questions and reflection on the co-evolution of technology and policy.

## 2 Open Source Software

The subjects of "free software [http://en.wikipedia.org/wiki/Free_software]" and "open source software [http://en.wikipedia.org/wiki/Open_source]" are complex and interrelated; as such, a full discussion of would be well outside the scope of this paper. At the highest level, both free and open source software provide a means for software developers to examine other developers' code so as to understand how the code works as well as to utilize and improve techniques manifested in the code. For the purpose of simplicity, we will define "free software" as software that allows use[1] *without any restrictions*, whereas open source may bear restrictions. We have chosen this simplification because it makes the privacy addendum's difference most clear; certainly there are many arguments about which difference between the two types is the "most important." Throughout this paper we describe our work as an extension of the open source idea to emphasize our commitment to the idea that just because a piece of software can be studied, does not mean that it may be used in any way that a developer wishes.

The principal idea and ideals of open source – the ability to share techniques and to "see under the covers" – has had broad implications for the intellectual community. Extending beyond software, the intellectual property framework developed for open

[1] Typically the "four freedoms" of free software are the ability study the software, copy the software, redistribute the software, and use the software without restriction.

source software has been generalized to include creative works (http://creativecommons.org/), courseware (http://ocw.mit.edu), and genetic code (http://rsss.anu.edu.au/~janeth/home.html). To date, the open source concept has not been extended beyond ownership and licensing of intellectual property to include in its scope other central social values, such as that of privacy. Moreover, the terms of most open source and free software licenses expressly prohibit modifications or additions to the terms of the license.

Thus, from the perspective of open source what we propose here offers two innovations: First, we sought to extend the construct of making intellectual output widely available under specific conditions to address commitments to privacy along with intellectual property. Second, we sought to construct the parameters for a small, vetted set of modifications or addenda that could be appended to and not invalidate the underlying open source license.

## 3 Genesis of an Idea, POLS, and the Problem of Pre-existing Open Source Software Licenses

In early discussions, we asked the question: How might the designers of Place Lab (http://placelab.org/) ensure that those who built upon that technology would continue Place Lab's privacy-sensitive practices? An intriguing potential solution emerged: that Place Lab's license terms would address commitments to end-user privacy along with the license to intellectual property.

Thus, the early thinking about the privacy addendum took Place Lab as its starting point. However, Place Lab was built using open source code licensed in part under the GPL, and as a result, the Place Lab code would be deemed a "derivative" and therefore subject to the GPL. Part way into the project, it became apparent that a new code base, unfettered by the complications of a pre-existing license (i.e. the GPL), would be needed to move the project forward. Thus a distinct, new system, POLS, the Privacy Observant Location System (http://pols.sourceforge.net/), was built from scratch, to allow the designers to license the code subject to the "restrictions" implemented in the privacy addendum, which would not be permitted under the GPL.

That said, POLS resembles Place Lab in many key respects. Currently running on mobile phone platforms, POLS uses the location data of "nearby" radio transmitters, *beacons*, to determine the location of the device running the POLS software. The output from POLS is roughly the longitude and latitude of that device. In terms of privacy, POLS is implemented with an in-bound information only architecture. This type of architecture dictates that the device passively monitors the radio environment (the in-bound information) and then computes its location locally without communicating with the infrastructure. Systems that rely on some outside infrastructure to locate a user's device inherently compromise the user's privacy to some degree, since the owners and operators of the infrastructure portion of the system are at least somewhat aware of the user's location. POLS works quite differently: Each user's device carries a list of known positions of the environments' beacons and the phone's radio is monitored too see which beacons can be "heard" at the present time, allowing POLS to estimate the location based on the known position of the beacon.

## 4 Value Sensitive Design

This research was conceived within the framework of Value Sensitive Design, a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process [9, 12,13]. Central to this work is Value Sensitive Design's interactional stance that articulates mutual dependencies and interconnections both across levels within the technology as well as between the technology and the surrounding social systems. Thus, we expected the technical features of POLS (and location aware systems more generally) to shape the requirements for the privacy addendum. For example, the privacy addendum would need to address the ways in which access to real-time location information can put end-users at risk. In turn, as we developed the privacy addendum, we expected our analyses to push back on how the technology should function. For example, analyses that required certain end-user capabilities – that the end-user be able to give active consent, to revoke prior consent, to remove data from the system – would require corresponding technical implementations.

In addition, prior work in Value Sensitive Design alerted us to two practical challenges that we would likely encounter [9,11,12]. The first involves the balance between human values and usability. Here, we anticipated places in the privacy addendum where we would need to relax the required stringency of a privacy protection in order to allow for a workable level of usability. The second involves limitations in the state of professional knowledge. Here, we recognized that we might encounter places in our privacy analyses which would suggest technical requirements that as a field we do not yet know how to meet. Should that occur, we would need to carefully identify such areas and set them aside for the time being. Moreover, the identification of such areas could provide useful information for setting the direction for new technical work and moving the field forward. Such an approach parallels that in other fields such as medicine, where the state of standard professional practice co-evolves with the state of medical knowledge.

Methodologically, key to Value Sensitive Design's conceptual investigations are stakeholder analyses that identify relevant stakeholders by role and examine how those stakeholders might be impacted by the system under investigation. In the case of POLS (and other ubiquitous location aware systems), three stakeholder groups were identified that became the focus of this work: the *application developer* who would build upon the ubiquitous open source system, the *end-user* who would experience the system's privacy implications, and *third parties* – malicious or otherwise – who might exploit the system for their own purposes. Specifically, we sought to balance end-user privacy protections with realistic demands on the application developer, in light of a technology that may be vulnerable to attack from third parties. Toward that end, two conceptual investigations were undertaken. The first examined the behaviors we wished to require or, at a minimum, to recommend on the part of the application developer. We employed an informed consent model here. The second investigation examined end-user vulnerabilities and the corresponding behaviors we wished to prevent on the part of the application developer or a third party. We employed a threat model here. Results from the two models were then integrated.

# 5 Development of the Privacy Addendum

We report on our analyses, deliberations, and eventual design decisions that led to the privacy addendum.

## 5.1 Informed Consent Model

Informed consent provides a powerful construct for providing privacy protections by empowering the end-user with knowledge and choice about participation. In effect, when implemented well informed consent creates conditions by which end-users are positioned to protect themselves and their privacy as they want through selective participation. To develop initial parameters for the privacy addendum, we drew on an established model for informed consent for information systems, one that has been applied successfully in areas such as network security, cookies and web browsers, and web email [10,15].

The informed consent model is comprised of six components: *disclosure, comprehension, voluntariness, competence, agreement*, and *minimal distraction*. We systematically examined each component to identify design requirements. Our strategy was to require those that were reasonable given current technical knowledge and practices; others that we judged to be desirable but too difficult to implement or beyond the state of current knowledge, we would recommend or set aside completely. Throughout these deliberations, we used our experience with ubiquitous location aware systems in general, and POLS in particular, to ground our analyses in real features and consequences.

Table 1 summarizes the informed consent model and implications of our analyses for the privacy addendum. We describe each component in turn.

**Disclosure**
The act of informing entails disclosing appropriate and accurate information to the intended audience. In particular, end-users of ubiquitous location aware systems will likely want to know: (a) what information will be collected (e.g., my current location, including an association with a place name such as Seward Park); (b) who will have access to the information (e.g., my spouse and children); (c) how long the information will be archived (e.g., on the order of hours); (d) what the information will be used for (e.g., to coordinate family activities, such as soccer carpool); and (e) how the identity of the individual will be protected(e.g., not at all). With that information in hand, end-users are positioned to decide if they want to participate in use of the system for these purposes. As shown in Table 1, there is a close overlap between the type and level of specificity of information the informed consent model suggests be disclosed and that identified for the privacy addendum.

**Comprehension**
In order to truly inform, what is disclosed must be understood by the intended audience. Understanding is the crux of comprehension. While currently it is not possible to guarantee full end-user comprehension for all possible end-users, we can require that application developers disclose information to end-users in a manner reasonably designed to be understood and provide actual notice (e.g., using a "friend-finding" application to locate my sister will also reveal my location to my spouse as well as my friends Alice, Bob, and Chris).

**Table 1.** Summary of Informed Consent Analysis for Privacy Addendum

| Component | Description | Implication for Privacy Addendum |
|---|---|---|
| DISCLOSURE | Refers to providing accurate information about the benefits and harms that might reasonably be expected from the action under consideration, including explicitly stating the purpose or reason for undertaking the action, and avoiding unnecessary technical detail. Moreover, if the action involves collecting information about an individual then the following should also be made explicit: (a) what information will be collected; (b) who will have access to the information; (c) how long the information will be archived; (d) what the information will be used for; and (e) how the identity of the individual will be protected. | • Disclose the following information: (a) what personal information will be collected; (b) how the personal information will be used; (c) who will have access to the information, including whether the recipient can transfer the information and, if so, if these principles continue to apply; (d) how long the personal information will be retained |
| COMPREHENSION | Refers to the individual's accurate interpretation of *what* is being disclosed. | • Effort should be made to disclose information to end-users in a manner reasonably designed to ensure the end-user's understanding – in effect, to provide actual notice |
| VOLUNTARINESS | Refers to ensuring that the individual's action is not coerced (e.g., controlled by compulsion, threat, or prevention) or overly manipulated (e.g., unduly altered or influenced by some means other than reason). | • Beyond the current state of knowledge in human-computer interaction |
| COMPETENCE | Refers to the individual possessing the mental, emotional and physical capabilities needed to give informed consent. | • Beyond the current state of knowledge in human-computer interaction |
| AGREEMENT | Refers to providing a reasonably clear opportunity for the individual to accept or decline to participate. Aspects to consider include: (1) Are opportunities to accept or decline visible, readily accessible, and on-going? (2) Is agreement by the participant on-going? | • Agreement must be obtained prior to any data collection<br>• The opportunity to accept or decline must be visible and readily accessible<br>• Where practicable, end-users should be able to revoke their prior consent and, if revoked, no further data collection should occur until a future agreement is made<br>• Where practicable, opportunities for giving and/or withdrawing agreement should be on-going |
| MINIMAL DISTRACTION | Refers to meeting the above five components without overwhelming users with intolerable nuisance. | • Reasonably simple mechanisms should be used to disclose information and obtain agreement |

## Agreement

Once informed, the end-user then needs an opportunity to agree or decline to participate. That said, it was not entirely straightforward how to realize the component of *agreement* in the privacy addendum. The informed consent model

presents a robust conception of agreement that includes not only visible active consent prior to data collection but also the on-going visible opportunity to revoke consent and potentially withdraw prior data. Here the privacy addendum is able to go some but not all of the distance. There have been disagreements among both the authors and those scholars that have reviewed the addendum about the degree to which active consent from the user should be required. . In part, there were concerns that passive consent might make sense for some applications (e.g., applications that run in the background should not be required to ask for user permission at every turn). Second, given limitations in technical know-how and interaction design the addendum stops short of requiring the opportunity to remove past data (because if the data has been aggregated with no links back to the end-user, then it may not be possible for past data to be removed) or to revoke agreement (because some viable applications may make it impossible to access the device at regular intervals and, thus, to change permissions).

**Competence and Voluntariness**

To fulfill the most robust conception of informed consent, the two components of *competence* and *voluntariness* all need to be addressed. Competence refers to the individual possessing the mental, emotional and physical capabilities needed to give informed consent, voluntariness to the ability to do so without coercion or undue manipulation. For remote interactions of the sort envisioned for ubiquitous applications, no one knows how to make these assessments. Thus, for purposes of the privacy addendum, we set them aside. As knowledge in the field develops, then one or both of these other two components may become relevant.

**Minimal Distraction**

Finally, usable informed consent requires a streamlined "informing" and "consenting" process that does not unduly distract end-users from their goals. While easier to state than implement, the requirement was integrated into the privacy addendum in phrases such as "provide an easy method by which an end user can …."

### 5.2 Threat Model

The informed consent model provides protections for end-users by giving them control over their participation. By itself, it goes a good distance. With this research we sought to complement our informed consent analysis with an analysis of potential threats. In analyzing threats we consider both those that occur as "by-products" of the technical design without the intentional action of a third party, as well as those that result from the intentional and often malicious acts of others whom we shall refer to as "attackers."

Traditionally threat models have been employed within the field of security to systematically identify system vulnerabilities and potential harms to users. For example, Felten [8] writes: "[T]he first rule of security analysis is this: understand your threat model. Experience teaches that if you don't have a clear **threat model** – a clear idea of what you are trying to prevent and what technical capabilities your adversaries have – then you won't be able to think analytically about how to proceed." Such analyses have been used to assess the vulnerabilities of Internet

protocols [2], web applications [29], and software-defined radio [19] to name but a few. While there are numerous variations in how threat models are conducted – what sorts of steps are taken and the order of those steps – the models share an emphasis on identifying what can be harmed (assets), who or what can cause those harms (threats), the ease with which those harms can be perpetrated (vulnerabilities), and means to address or mitigate the vulnerabilities (see, for example, [17,18,29].

For our purposes, we followed a process similar to that described by Goldberg [17] in which we (1) identified system assets, (2) identified system vulnerabilities, (3) classified potential attacker types, (4) identified potential entry points, and (5) constructed threat scenarios and mitigation plans. In conducting our threat analysis, we drew on potential harms and vulnerabilities identified in the literature, conceptually distinct categories of harms (e.g., physical, psychological, and financial), and our understanding of the technology. As with our analysis of informed consent, we considered location awareness systems as a touchstone to aid with identifying potential harms and vulnerabilities for the end-user.

Table 2 summarizes the four classes of threats that emerged from our analysis. We describe each class in turn.

**Table 2.** Summary of Threat Analysis for Privacy Addendum

| Threat | Description | Implication for Privacy Addendum |
|---|---|---|
| I. DISCLOSURE TO UNAUTHORIZED PARTIES<br>I.1 Reputation (Publicity)<br>I.2 Solitude (To be "Left Alone") | Refers to threats to reputation and solitude that can occur when one person simply "knows" information about another person. | • Provide a general warning about malicious use<br>• Provide a specific warning for vulnerable populations |
| II. UNAUTHORIZED USE OF INDIVIDUAL INFORMATION<br>II.1 Attention<br>II.2 Physical Welfare<br>II.3 Data Privacy<br>II.4 Property | Refers to threats to attention, physical welfare, data privacy, and property that can occur when information provided for one purpose is used without authorization for a second purpose, | • Same as for Threat I<br>• Delete no longer needed identifiable information at reasonable intervals |
| III. UNAUTHORIZED USE OF AGGREGATED INFORMATION<br>III.1 Attention<br>III.2 Physical Welfare<br>III.3 Data Privacy<br>III.4 Property | Refers to threats to attention, physical welfare, data privacy, and property that can occur from the unauthorized use of aggregated information, | • Same as for Threat II<br>• Delete no longer needed links between identifiable and aggregated information at reasonable intervals |
| IV. UNAUTHORIZED INFERENCE WITH UNEXPECTED EXTERNAL INFO. | Refers to threats that can occur from the unauthorized use of information when it is combined with other externally available information. | • Beyond the software developer's purview |

**Threat I. Disclosure to Unauthorized Parties**

At times the simple act of one person knowing information about another person results in harm. In particular, unauthorized disclosure of information can affect someone's "reputation" (Threat I.1), at a minimum leading to embarrassment (e.g., a

system reveals to Alice's friend that she almost always spends Tuesday evening in close proximity to a building labeled as Alcoholics Anonymous). Unauthorized disclosure of information can also intrude on an individual's ability to be "left alone" (Threat I.2) (e.g., a location system that reveals an employee's location to an employer during the employee's vacation, "I saw you were back in the hotel so I decided to call and ask you about…"). Moreover, the concept of being "left-alone" has a strongly temporal element to it and, thus, links authorization with time and context (e.g., during work hours, an employee such as a traveling salesperson may be fine with an employer know his or her location but not so for non-work hours).

**Threat II. Unauthorized Use of Individual Data**

A second class of threats results when information provided for one purpose is used without authorization for a second purpose. While Threat I concerns *who* has access to the information, Threat II concerns *secondary uses* of the information.[2] At least four types of harms can be identified here: (1) Harm to "attention" (Threat II.1) can result when the unauthorized use requires a response from the user or otherwise places demands on the user's attention. (2) Unauthorized information use can also put users at risk for "physical welfare" (Threat II.2), either directly (e.g., when a system reveals that Chris's personal device is at particular location, say in a dark alleyway at 7 PM and can be mugged there) or through inference based on historical data about the individual (e.g., Chris usually travels home on weekdays at about 7 PM via this alley). Moreover, certain individuals due to their personal circumstances (e.g., prior victims of domestic violence) may be at greater risk than others. These populations may warrant special warnings and/or protections. (3) A third type of harm which we refer to as "data privacy" harm (Threat II.3) involves unauthorized use of one sort of information to "discover" other information about the user (e.g., since the locations where people spend most of their time is home and work, by analyzing location data an attacker could determine a user's home address). (4) Unauthorized use of information can also put the user's personal property at risk (Threat II.4). In the case of location information, the risk is typically for theft (the fact that a user is **not** at a given location can be used as a suggestion about when might be a good time to attempt a robbery).

**Threat III. Unauthorized Use of Aggregated Data**

While Threat II entails harms that result when information about a single individual is used for unauthorized purposes, the third class of threats entails harms that result from the unauthorized use of aggregated data. These attacks are more impersonal in the sense that an attacker does not identify a specific person to attack but rather a class of people. Each of the four types of harms – attention (Threat III.1), physical welfare (Threat III.2), data privacy (Threat III.3), and property (Threat III.4) – identified for Threat II are possible here, though cast in terms of aggregated data. For example, in terms of physical harm, rather than an attacker knowing that a particular person, say Chris, is walking down an alley at 7 PM and could be mugged, the attacker knows that most evenings at 7 PM at least one person walks alone down the alley and could

[2] When neither the party nor the use is authorized, then both Threat I (unauthorized disclosure) and Threat II (unauthorized use) are involved.

be mugged. Other threats based on unauthorized use of aggregated data arise when the aggregated data can be linked back to specific individuals. For example, if aggregated data suggests that a group of 102 people are currently at places labeled by the yellow pages as places of business, then an attacker could reasonably assume that a significant fraction of these individuals have empty houses right now. When possible, it is beneficial to design systems that do not maintain links from the aggregated data back to specific individuals.

**Threat IV. Unauthorized Inference with Unexpected External Information**
Threat IV represents a special case of Threat II, one in which the unauthorized use involves inference that combines information from even the best-designed, most privacy-sensitive system with other information externally available to the attacker. For example, Alice may choose to disclose to Bob her location at specific points through the day for a sensible set of reasons. However, Bob uses external knowledge—say of a city's demographic patterns—to conclude that Alice spends large amounts of her free time in an area that has a particular political affiliation. Alice intended to disclose one piece of information, but Bob used external knowledge to draw other conclusions that Alice never intended.

From the perspective of the privacy addendum class IV Threats, while a significant challenge to privacy are not tractable because they fall outside the purview of the application developer's control. That is, the application developer is not in a position to determine what other external information might be brought to bear and combined with the typical data of the software system.

**Threats Beyond Privacy**
In the process of conducting the threat analysis, we identified several additional threats that while legitimate, went beyond the scope of the privacy addendum. We mention them here both for completeness and to call attention to the ways in which privacy implicates other important human values such as *accessibility* and *credibility* (see [32] for a review; [14] and [33] for related discussion). These included threats to (a) the *quality of information* (e.g., due to limited precision, missing data, or other technical limitations the information system does not contain or produce wholly accurate or complete information), (b) *access to information* (e.g. due to technical limitations of the system or supporting infrastructure, the information system is not always available for use), and (c) *credibility of information* (e.g., due to malicious tampering of the system by a third party, the information system produces output that is intentionally misleading).

### 5.3 Integrating Results from the Informed Consent and Threat Models

Results from the informed consent analysis provided detailed insight into what information to disclose, how to disclose it, when and what type of agreement to obtain, and what assessments (e.g., of competence and voluntariness) would be reasonably beyond our reach. In contrast, results from the threat analysis pointed to vulnerabilities and means to remedy them. How then to bring the results of the two distinct models together to inform a single coherent set of legal of terms?

Our method proceeded as follows: We began with the key implications identified in the informed consent analysis (summarized in Table 1): namely, the comprehensible disclosure of information use prior to data collection and the on-going opportunity to provide agreement. This informed consent model provided a good deal of specificity and substantive direction. Where the state of knowledge was limited (e.g., the ability to remove data once it had been collected and aggregated), we correspondingly recommended but did not require action. Within the privacy addendum, this material formed the bulk of what became the Location Aware Privacy Principles (see Table 3, Addendum 2, Sections 1 and 2).

Next we examined implications identified by the threat analysis (summarized in Table 2); we acknowledged those that dovetailed with the informed consent model but focused our attention on unique aspects. One implication was the general adage to warn end-users of risk from third parties, if malicious software should access the system. This general warning overlapped with implications from the informed consent model and was incorporated into an "initial screen" warning (see Table 3, Addendum 1, Section II). A second implication entailed attention to the vulnerability of special populations, such as victims of domestic violence who can be placed at greater risk should their location be discovered. Thus, we added an additional requirement in the addendum for a special warning for these populations (see Table 3, Addendum 1, Section II). A third key implication entailed the recognition that deleting links or removing data could minimize the duration of time for which a threat was "active". Thus, in the Location Aware Privacy Principles we incorporated text to encourage safeguards against malicious software such as deleting personally identifiable information at reasonable intervals when it is no longer needed (see Table 3, Addendum 2, Sections 3 and 4).

We also considered interactions among results from the two models and corresponding design implications. For example, from the threat model we recognized that unauthorized disclosure depends not only to whom one discloses but also when and where that disclosure occurs. Thus, in order to provide meaningful informed consent, end-users may need to do so at a level of specificity that includes not only the recipient of the information but the context (e.g., location and time) as well. In turn, recognition of the dynamic nature of risk and consent, points to the need for ready-to-hand mechanisms that enable end-users to give and withdraw consent (e.g., to dynamically opt-in and opt-out of the location aware system).

Finally, we recognized that to be workable the privacy addendum would need to allow for legitimate circumstances in which application developers would need to access to personal information in order to provide the service, debug code, and otherwise maintain the system.

## 6 POL's Privacy Addendum

Based on our Value Sensitive Design analysis that integrated results from the informed consent and threat models, a premier legal team drafted the legal terms of the privacy addendum. The process used by that team is outside the scope of this

paper. In this section we describe the structure of the privacy addendum in its current form. Table 3 contains the entire text of the addendum and section by section indicates the intellectual source (e.g. informed consent model, threat model, general Value Sensitive Design practices, general privacy addendum concept).

**Table 3.** Legal Text of POLS Privacy Addendum with Source

| Privacy Addendum Legal Text | Source |
|---|---|
| **Addendum 1: Privacy Addendum**<br><br>This addendum contains the additional terms applicable to development and distribution of a work (Work) containing all or a portion of the Program or that is otherwise derived from the Program.<br><br>**I. You agree that:**<br>1. Your compliance with this Addendum is a material condition of your license to the Program.<br>2. You will include in any follow-on licenses you make with other developers for building other applications or services for the Program and your Work the same terms and conditions as this license addendum provides (and you will bind any firm that acquires your firm to the same terms and conditions as this license provides).<br>3. Your development, use, and/or distribution of a Work constitutes an enforceable public commitment to comply with the provisions of this addendum.<br>4. Any collection, use, disclosure, and/or storage of personally identifiable location information about end-users will be undertaken in accordance with the Location Aware Privacy Principles (attached).<br>5. End users are entitled to enforce the terms of this Addendum and the Location Aware Privacy Principles as third party beneficiaries of the Agreement or as otherwise permitted under applicable law.<br>6. Any violation of the terms of this Addendum may constitute an unfair and/or deceptive trade practice in violation of state and federal consumer protection law. | PRIVACY ADDENDUM CONCEPT |
| **II. You further agree that all distributed Works will:**<br>Clearly, conspicuously, and verifiably (a) warn end users that the Work may disclose their physical location to third parties; and (b) obligate you to comply with the Location Aware Privacy Principles (set forth in Addendum 2, attached) by, without limitation, causing the following text (with sections in parentheses modified accordingly) to appear when the Work is first installed and at reasonable intervals thereafter:<br>*When you use this application, (Software Name) (or other malicious software which takes advantage of (Software Name)) may cause your mobile device to communicate its physical location - and therefore your location - to application providers and/or third parties online* | INFORMED CONSENT MODEL<br>• Disclosure<br>• Comprehension |
| *Please be aware of your circumstances and your safety and use appropriate caution when using (Software Name).* | THREAT MODEL<br>• Threat II |
| *(Developer/Distributor) adheres to the Location Aware Computing Privacy Principles (attached). These principles require us to get your prior informed consent for any collection, use, disclosure and/or storage of your location information. Please review the (Software Name) privacy policy (include URL)* | INFORMED CONSENT MODEL<br>• Disclosure<br>• Comprehension<br>• Agreement |
| **III.** You also agree that to the extent practicable, your implementation of the Location Aware Privacy Principles will be consistent with the best practices set forth from time to time at the Intel Research/University of Washington Privacy Best Practices website. | GENERAL VALUE SENSITIVE DESIGN PRACTICE |

**Table 3.** (*continued*)

| **Addendum 2: Location Aware Privacy Principles** | |
|---|---|
| 1. End users will be informed, in a manner reasonably designed to provide actual notice and prior to any collection, use, retention, or disclosure of personally identifiable location information, of the following:<br>a. What personal information will be collected;<br>b. How that personal information will be used;<br>c. To whom that personal information will be disclosed, how the recipient will be able to use the personal information, whether the recipient in turn will be able to transfer the information and whether the recipient is obligated to comply with these Principles.<br>d. How long (or how often) the personal information will be disclosed (e.g. at the time of initial connection only, or periodically during the use of the software) | INFORMED CONSENT MODEL<br>• Disclosure<br>• Comprehension |
| 2. To the extent reasonably practicable under the circumstances, end users will be given conspicuous notice of the opportunity to prohibit the proposed collection, use, retention, and/or disclosure of their personally identifiable location information in whole or in part, and a reasonably simple mechanism for taking advantage of such opportunity. Where practicable, a Work will provide an easy method by which an end user can prohibit such collection, use, retention, and/or disclosure, on a case by case basis, at their discretion. | INFORMED CONSENT MODEL<br>• Agreement<br>• Minimal Distraction |
| 3. Personally identifiable location information will be deleted regularly when it is no longer needed by the end-user or for the correct functioning of the Work. | THREAT MODEL<br>• Threat III |
| 4. Licensees will implement administrative, technical, and/or other safeguards appropriate in light of the sensitivity of the data to protect personally identifiable information from unauthorized access, use, disclosure, or damage. | THREAT MODEL<br>• Threat I, II, III |

### 6.1 The Legal Text

The text of the POLS Privacy Addendum is divided into two parts: Addendum 1 creates the general legal framework, and points to Addendum 2 for the particulars of location-aware systems. Addendum 2 is intended to provide guidelines specific to the problems of location-aware systems. This two part structure was devised by the team of legal scholars for two reasons. First, if the privacy addendum might someday be amended to open-source licenses of technology implicating other aspects of end-user privacy (say, genetic data in an open-source biology system) the general legal framework can still apply, when taken together with a new Addendum covering the specific implications of the specific technology and the types of data used by that technology. Second, to win industry and open-source community acceptance, it is necessary for the addendum to appeal to a broad spectrum of potential reviewers with many different points of view. The attempt to segregate the general legal framework from the specific issues would allow the overall scheme to move forward in cases where people agree with the general framework, but have a specific disagreement with the details of how location privacy should be handled, as the particulars of Addendum 2 may be debated. Similarly, the proposed best practices web site provides a way to assist application developers with potential solutions without burdening the legal document with specifics that could cause adoption problems.

A critical aspect of the addendum is Addendum 1, Sections 5 and 6, as they are designed to facilitate enforcement of the terms of the Privacy Addendum. The parties to the software license (which is a contract that includes the Privacy Addendum) are the technology developer and the application developer who wishes to incorporate and build on to the licensed technology. The end-user (whose privacy the addendum seeks to protect) is not a party to the agreement. Under contract law, normally only the parties to a contract have a right to enforce that contract. Section 5 is intended to convey a legal right to the non-party end-user, to enforce the terms of the privacy addendum if the terms are breached, because the non-party end-user is the one most likely to experience damages in case of breach of these terms. Similarly, Section 6 asks the software developer to agree that violating the terms of the Privacy Addendum may equate to a deceptive or unfair trade practice. In the United States, this could facilitate the process if the US Federal Trade Commission (FTC) or Department of Justice (DOJ) were to decide that encroachments on end-user privacy in breach of the terms of the Privacy Amendment should be handled as unfair or deceptive trade practice. When the developer has "acknowledged and agreed" that a violation may constitute an unfair trade practice, that element may then as a result be easier for the FTC or DOJ to prove in litigation.

### 6.2 Technical Implications

POLS' privacy addendum brings with it several design implications for application developers who build on POLS' infrastructure. These include: (1) First screen notifications about possible harms, vulnerable populations, and informed consent practices (Table 3, Addendum 1, Section II). (2) Interaction design and interface components for informing the end-user about the collection, use, retention and disclosure of personally identifiable information (Table 3, Addendum 2, Section 1). (3) Interaction design and interface components to provide end-users the opportunity for providing agreement and, if possible, also revoking agreement for participation (Table 3, Addendum 2, Section 2). (4) At reasonable intervals, deletion of personally identifiable information when it is no longer needed for the successful functioning of the application. (5) As feasible, other safeguards to protect personally identifiable information from unauthorized access, use, disclosure, or damage.

## 7 Contributions and Next Steps

POLS was released under a license combining the substantive terms of the Eclipse Public License together with this privacy addendum to the public in January 2006. As of this writing, the POLS system is being used by early university adopters from several academic institutions. As POLS application developers gain experience with the privacy addendum, we envision a best practices web site that would help to disseminate good design solutions as they are developed, and which would be a reference for developers implementing technology consistent with the principles outlined in Addendum 2. In this early phase of the privacy addendum's deployment, we are actively seeking input and commentary from the open source community.

The central contributions of this work are six-fold:

- Provides a "proof-of-concept" for what a privacy addendum might look like for a ubiquitous location aware system – that is, actual legal terms – and the release of a real system under those legal terms.
- Combines an informed consent and threat analysis to tackle the problem of privacy. Demonstrates that more comprehensive privacy solutions may be possible by combining approaches as compared with utilizing either approach alone.
- Demonstrates the co-evolution of policy and technology in the sense that (a) the legal terms were developed in response to current technical possibilities and limitations of ubiquitous location aware systems, and (b) the legal terms, in turn, are shaping and will continue to shape aspects of the interaction design and interface.
- Extends the scope of open source software licensing to commitments to end-user privacy as well as licenses to intellectual property. In so doing, we establish the possibility that open source licenses could embrace a range of other values.
- Extends the structure of open source licenses to consider accepting a small set of vetted addenda as a means to tailor these licenses to specific needs and desires on the part of the original developers.
- Demonstrates the success of using Value Sensitive Design theory and methods in an industry setting, namely within Intel Corporation. This effort represents one of the first industry applications of Value Sensitive Design.

As we move forward with the privacy addendum, a number of open questions remain. First and foremost: How can the privacy addendum be improved? As with any first effort, we expect there to be imperfections. For the addendum to succeed, it must strike the right balance between providing real protections for the end-user with reasonable constraints on the application developer. Is this version of the addendum too stringent, overly constraining application developers in some ways? We think not but are open to being shown otherwise. Is this version of the addendum not stringent enough in some aspects? Here we suspect so. In particular, there are differences of opinion about the need for a more active form of consent. Currently the addendum is United States centric, written in terms of US state and federal consumer protection law. How can the addendum be expanded to operate effectively in other jurisdictions? As applications developers gain experience working with the privacy addendum, other limitations of the addendum may be exposed. Thus, we expect to modify the addendum based on these experiences.

A second set of questions concerns how the privacy addendum will be integrated with existing open source software licenses. Virtually all open source licenses prohibit modification of the license terms. Such prohibitions protect against changes that could undermine the intention of the original license. Thus the privacy addendum cannot typically just be placed at the end of an existing open source license. Toward resolving this issue, we are currently beginning an engagement with the Open Source Initiative (OSI) the standards body that certifies open source licenses. Our hope is that OSI will certify the privacy addendum and allow the addendum to be added to

existing certified open sources licenses without invalidating the prior certification. These discussions are beginning and will be on-going.

A third set of questions concern generalizing the privacy addendum. Beyond POLS, our hope is that the privacy addendum can evolve and generalize for use with other technology. It may be useful to begin with other location awareness systems or, at least, other ubiquitous computing systems. Over time, we hope to migrate the privacy addendum to a wide variety of information systems. The process of adapting the privacy addendum to a variety of technology areas would provide invaluable information and first hand experience with generalizing the privacy principles.

## Acknowledgments

We would like to thank those who contributed in various ways to the project's success: Alan Borning, Dmitri Chmelev, Nathan G. Freier, Jeff Hughes, Dave Hoffman, Donald Horowitz, James Landay, Jessica Miller, Dierdre Mulligan, Fred Potter, Pamela Samuelson, Peter Seipel, and Jaina Selawski. This material is based, in part, upon work supported by the National Science Foundation under Grant No. 0325035. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

## References

1. Ackerman, M., Darrell, T., Weitzner, D.J.: Privacy in context. Human-Computer Interaction, 16, (2001) 167-176
2. Atkins, D., Austein, R.: Threat Analysis of the Domain Name System (2004) Retrieved March 30, 2006 from http://www.ietf.org/rfc/rfc3833.txt?number=3833
3. Boyle, M., Edwards, C., Greenberg, S.: The effects of filtered video on awareness and privacy. Proceedings of CSCW '00 New York: ACM Press (2000) 1-10
4. Borriello, G., Brunette, W., Hall, M., Hartung, C., Tangney, C.: Reminding About Tagged Objects Using Passive RFIDs. Proceedings of UbiComp '04 (2004) 36-53
5. Consolvo, S., Roessler, P., Shelton, B. E.: The CareNet Display: Lessons Learned from an In Home Evaluation of an Ambient Display. Proceedings of UbiComp '04 (2004) 1-17
6. Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., Powledge, P.: Location Disclosure to Social Relations: Why, When, & What People Want to Share. Proceedings of CHI 2005. ACM Press New York (2005) 81-90
7. Cranor, L.F., Garfinkel, S.: Security and usability: Designing secure systems that people can use. Cambridge, MA: O'Reilly (2005)
8. Felten, E.: DRM, and the First Rule of Security Analysis. Freedom to Tinker (2003) Retrieved March 30, 2006 from http://www.freedom-to-tinker.com/index.php?p=317
9. Friedman, B. (ed.): Human Values and the Design of Computer Technology. Cambridge University Press and CSLI New York Stanford University (1997)
10. Friedman, B., Felten, E., Millett, L. I.: Informed Consent Online: A Conceptual Model and Design Principles. CSE Technical Report 00-12-02. Department of Computer Science and Engineering, University of Washington, Seattle, Washington (2000)

11. Friedman, B., Howe, D.C., Felten, E.: Informed consent in the Mozilla browser: Implementing value-sensitive design. Proc of HICSS '02 Abstract, p. 247; CD-ROM of full-paper, OSPE101. Los Alamitos, CA: IEEE Computer Society (2002)
12. Friedman, B., Kahn, P.H., Jr.: Human values, ethics, & design. In Jacko, J., Sears, A. (Eds.): Handbook of human-computer interaction. Mahwah, NJ: Lawrence Erlbaum Associates (2003) 1177-1201
13. Friedman, B., Kahn, P.H., Jr., Borning, A.: Value Sensitive Design & information systems. In Zhang, P., Galletta, D. (Eds.): Human-computer interaction in management information systems: Foundations. Armonk, NY: M. E. Sharpe (in press)
14. Friedman, B., Kahn, P.H., Jr., Hagman, J., Severson, R.L., Gill, B.: The Watcher and The Watched: Social Judgments about Privacy in a Public Place. Human-Computer Interaction (in press)
15. Friedman, B., Lin, P., Miller, J.: Informed Consent by Design. In Cranor, L., Garfinkel, S. (eds.): Designing Secure Systems that People Can Use. O'Reilly & Associates, Cambridge, MA (2005) 495 – 521
16. Goecks, J., Mynatt, E. D.: Leveraging Social Networks for Information Sharing. Proceedings of CSCW '04 (2004) 328-331
17. Goldberg, Y. Practical Threat Analysis for the Software Industry. SecurityDocs.com. (2005) Retrieved March 30, 2006 from http://www.securitydocs.com/library/2848
18. Grinter, R.E., Smetters, D.K.: Three Challenges for Embedding Security into Applications HCISEC Workshop at CHI '03. Fort Lauderdale, Florida. (2003) Retrieved March 30, 2006 from http://www.andrewpatrick.ca/CHI2003/HCISEC/hcisec-workshop-grinter.pdf
19. Hill, R., Myagmar, S., Campbell, R.: Threat Analysis of GNU Software Radio. Proc. of WWC'05. Palo Alto, CA (2005)
20. Hudson, S.E., Smith, I.: Techniques for addressing fundamental privacy & disruption tradeoffs in awareness support systems. Proceedings of CSCW '96 (1996) 248-257
21. Hull, R., Kumar, B., Lieuwen, D., Patel-Schneider, P.F., Sahuguet, A., Varadarajan, S., Vyas, A., "Enabling Context-Aware and Privacy-Conscious User Data Sharing," Proceedings of MDM '04 (2004) 187-198
22. Iachello, G., Smith, I.E., Consolvo, S., Abowd, G.D., Hughes, J., Howard, J., Potter, F., Scott, J., Sohn, T., Hightower, J., LaMarca, A.: Control, Deception, and Communication: Evaluating the Deployment of a Location-Enhanced Messaging Service. Proceedings of UbiComp 2005 (2005) 213-231
23. Iachello, G., Smith, I.E., Consolvo, S., Chen, M., Abowd, G.D.: (2005). Developing Privacy Guidelines for Social Location Disclosure Applications and Services. Proceedings of SOUPS '05. ACM Press New York (2005) 65-76
24. Jancke, G., Venolia, G.D., Grudin, J., Cadiz, J.J., Gupta, A.: Linking Public Spaces: Technical & Social Issues. Proceedings of CHI '01. Seattle, WA (2001) 530-537
25. Jiang, X., Hong, J.I., Landay, J.A.: Approximate information flows: Socially-based modeling of privacy in ubiquitous computing. Proceedings of UbiComp '02 (2002) 176-93
26. LaMarca, A., Chawathe, Y., Consolvo, S., Hightower, J., Smith, I.E., Scott, J., Sohn, T., Howard, J., Hughes, J., Potter, F., Tabert, J., Powledge, P., Borriello, G., Schilit, B.: Place Lab: Device Positioning Using Radio Beacons in the Wild. Proceedings of Pervasive '05, Munich, Germany (2005) 116-133.
27. Langheinrich, M.: Privacy by design–Principles of privacy-aware ubiquitous systems. Proceedings of UbiComp '01. Berlin, Heidelberg (2001) 273-291
28. Lederer, S., Hong, J.I., Dey, A.K., Landay, J.A.: Personal Privacy through Understanding & Action: 5 Pitfalls for Designers. Personal & Ubiquitous Computing. 8(6) (2004) 440-54.

29. Meler, J.D., Mackman, A., Dunner, N., Vasireddy, S., Escamilla, R., Murukan, A.: Threat modeling. In Improving Web Application Security: Threats and Countermeasures (2003)
30. Palen, L., Dourish, P.: Unpacking "privacy" for a networked world. Proceedings of CHI '03 (2003) 129-136
31. Patil, S., Lai, J.: Who gets to know what when: configuring privacy permissions in an awareness application. Proceedings CHI '05, Portland, OR, USA (2005) 101-110
32. Schoeman, F. (ed): Philosophical Dimensions of Privacy: An Anthology. Cambridge, UK: Cambridge University Press (1984)
33. Warren, S.D., Brandeis, L.D.: The Right to Privacy. Harvard Law Review 4(5) (1890)