Towards Territorial Privacy in Smart Environments

Bastian Könings, Florian Schaub, Michael Weber
Ulm University
Albert-Einstein-Allee 11, 89081 Ulm
Germany
givenname.surname@uni-ulm.de

Frank Kargl
University of Twente
Drienerlolaan 5, 7522 NB Enschede
The Netherlands
f.kargl@utwente.nl

Abstract

Territorial privacy is an old concept for privacy of the personal space dating back to the 19th century. Despite its former relevance, territorial privacy has been neglected in recent years, while privacy research and legislation mainly focused on the issue of information privacy. However, with the prospect of smart and ubiquitous environments, territorial privacy deserves new attention. Walls, as boundaries between personal and public spaces, will be insufficient to guard territorial privacy when our environments are permeated with numerous computing and sensing devices, that gather and share real-time information about us. Territorial privacy boundaries spanning both the physical and virtual world are required for the demarcation of personal spaces in smart environments. In this paper, we analyze and discuss the issue of territorial privacy in smart environments. We further propose a real-time user-centric observation model to describe multimodal observation channels of multiple physical and virtual observers. The model facilitates the definition of a territorial privacy boundary by separating desired from undesired observers, regardless of whether they are physically present in the user's private territory or virtually participating in it. Moreover, we outline future research challenges and identify areas of work that require attention in the context of territorial privacy in smart environments.

1. Introduction

The term "privacy" is often used to address violations of personal information, meaning that personal information of some individual is disclosed, misused, or transferred to third parties. This understanding of privacy refers to information privacy, sometimes also called data privacy. Information privacy can be defined as "the claim of individuals [...] to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1967). With the rapid development of the Internet and communication technologies during the last decades, information privacy became the leading notion of privacy.

However, in the upcoming age of ubiquitous computing, our environments will contain numerous computing devices, often invisibly embedded in everyday objects and capable of sensing and forwarding huge amounts of real-time information. Furthermore, devices will exist that can actively operate in our environments, either autonomously or controlled by external entities. The presence of those devices will have the effect that physical boundaries lose their capability of demarcating personal spaces.

What before could only be observed about a person in her personal space or territory by entities within its physical proximity, will become observable by any entity having virtual access to the person's private territory. Thus, in smart environments, the concept of territorial privacy will gain significant importance again, but has to be revised in order to address both the physical and virtual dimensions of a personal territory.

Even with today's technology, territorial privacy can already be violated. One example is an attack on remotely controllable household robots equipped with video cameras, as shown by Denning et al. (2009). This shows that territorial privacy is a critical issue and strongly needs future attention in research.

In the remainder of this paper, we first give a brief overview of related work in the field of privacy in smart environments and attempt to clarify the interrelation between information privacy and territorial privacy. Next, we propose a real-time observation model for territorial privacy that enables individuals to shape their territorial privacy boundary in a mixed physical and virtual environment. Finally, we will discuss some research challenges that should direct future work in this area.

2. Related Work

Marc Weiser (1993), who shaped the vision of ubiquitous computing and smart environments, already recognized that those environments will raise new privacy issues. However, his privacy concerns were focused on location privacy. Location privacy is a particular form of information privacy and has attracted considerable research (Beresford and Stajano 2003; Krumm 2008).

In recent years, general information privacy in ubiquitous computing has been investigated as well. Hong and Landay (2004) proposed Confab, a privacy-aware architecture for ubiquitous computing. Confab uses the concept of information spaces by Jiang et al. (2002) in combination with in- and out-filters to manage the flow of context information about a person. Langheinrich (2001) discussed how the fair information practices, a collection of abstract guidelines

Intelligent Information Privacy Management Symposium (Privacy 2010), AAAI Spring Symposium, Stanford University, USA, March 2010
Author version. Definitive version at https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1043/1496

to achieve information privacy, can be adapted to ubiquitous computing scenarios. He pointed out six principles, which he followed to design the privacy awareness system PawS (Langheinrich 2002) in order to address third party data collection in smart environments.

Although some of the former research has already identified the problem of collapsing physical boundaries, the focus is always on protecting particular types of information rather than respecting virtual boundaries of a person's private territory. In social research, some work in the latter direction exists, mainly on trying to find methods for modeling boundaries of personal information flows. Information boundary theory (IBT) (Stanton and Stam 2003; Xu et al. 2008) is one well-known model which attempts to formulate social aspects of information disclosure based on physical and virtual information spaces. The vision of digital territories of Daskala and Maghiros (2006) is similar to IBT. Digital territories should delimit personal information spaces in order to control incoming or outgoing information. Sociologist Gary T. Marx (2001) identified personal border crossings as a core concept of perceived privacy violations. He differentiates between natural borders, social borders, spatial or temporal borders, and borders due to ephemeral or transitory effects.

All of the discussed approaches put the focus on information privacy. Thus, finding mechanisms to protect particular personal information or model the information flow in order to define borders of such information are the core investigations of most existing privacy research in the field of smart environments. However, the aspect of territorial privacy has not received much attention in this context so far.

3. Territorial Privacy

Territorial privacy refers to one of the oldest understandings of privacy and can be described in simple terms as "the right to be let alone" (Warren and Brandeis 1890). This can be interpreted as the right of a person to determine individually when and how other entities are allowed to participate in his or her personal territory. A *personal territory* refers to a personal space of an individual which is delimited by a specific boundary. With the ongoing development towards the vision of ubiquitous computing and smart environments the specification of such boundaries will become much harder. The traditional way of demarcating a personal territory by erecting physical boundaries, like walls and doors of a room or a house, will not be sufficient anymore. On the contrary, a personal territory can now be virtually extended beyond its physical boundaries. This means that not only entities with physical access and presence can participate in a personal territory, but also remote entities, which have only virtual access to the territory.

We distinguish between two forms of possible participation, *intrusion* and *observation*. Intrusion refers to active intervention of an entity into one's personal territory. Observation refers to reception of real-time information gathered by sensing devices in physical range of one's personal territory. For example, a person receiving a live video-stream of a surveillance camera is an observer, that is virtually participating in the personal territory of the observed person.

The observation aspect of territorial privacy converges with the collection phase of information privacy, because what is sensed by nearby devices may encapsulate a large amount of personal information. Collection, together with processing and dissemination, are the three privacy relevant life-cycle phases of personal information defined in the privacy taxonomy of Daniel J. Solove (2008). Collection refers to the point in time where personal information is actively gathered or sensed. Or in other words, where personal information passes the border between the physical real world and the digital virtual world. Processing refers to data handling, like storage or usage of personal information, and dissemination refers to transfer and propagation thereof.

However, although gathering sensor data refers to the collection phase of personal information, the difference is that territorial privacy is not concerned with *what* particular information is collected by a device or could be derived thereof, but with *how* an entity participates in a personal territory. For example, what channels, we call them *observation channels*, an entity can use to physically or virtually receive information from inside a person's private territory. Thus, each raw real-time output of a sensing device can be seen as an observation channel. The aim of territorial privacy is to control access to those real-time observation channels as a whole, whereas information privacy aims to control access to specific personal information that may be encapsulated in those channels, but also information available from several other non real-time sources. The main challenge arising from future smart environments is to find solutions for controlling observation channels in order to define territorial privacy boundaries that are consistent in the virtual and physical world.

4. Real-time Observation Model

So far, we have outlined the issues faced by territorial privacy in ubiquitous environments. In this Section, we propose a new model for territorial privacy that facilitates the coherent definition of territorial privacy boundaries in a mixed real and virtual environment. First, we outline the model conceptually before formalizing it afterwards.

Concept

We take a user-centric approach towards privacy rather than an information-centric approach. In order to define a territorial privacy boundary, we model *who* can observe information about a user and *how* rather than *what* information is observed.

A user is surrounded by multiple observers. Any entity that can observe information about the current situation of the user is an observer with an observation channel to the user. An observation channel is any medium that conveys real-time information about the current state, presence, action, or behavior of the user. For example, a surveillance camera in the same room as the user is connected to the user through a visual observation channel. A microphone is an observer with an auditory observation channel to the user. A person in the user's proximity has multimodal observation channels, e.g., visual, auditory, and haptic. Observation

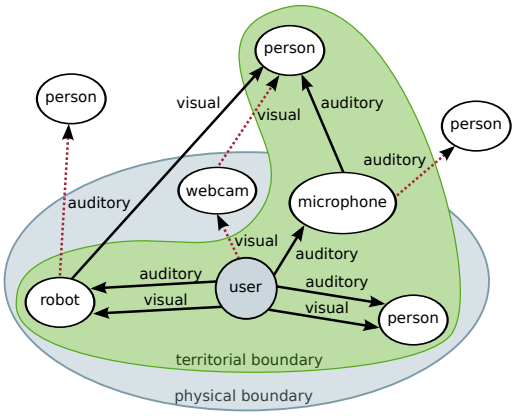

Figure 1: The territorial privacy boundary separates desired from undesired observers.

channels are defined per entity, e.g., several observers can each have a visual observation channel to the user.

We do not distinguish between technological and living entities as observers, but a distinction is made between physical and virtual observers. The aforementioned entities are all physically present, i.e., they are connected to the user through an observation channel with path length 1. A virtual observer is connected to the user through an observation channel with a greater length than 1. In the latter case, the observer is not physically present in the user's proximity, and an observation is relayed by intermediate entities, which we also consider observers. An example for a virtual observer is a backend system that uses input from sensors which in turn are physical observers. A virtual observer does not have to be a technical system but could also be a person that remotely watches a video surveillance stream.

Paths of observation channels originate from the user and go to the observers. The user can define its territorial privacy boundary by separating desired observers from undesired observers, as shown in Figure 1. Because our model incorporates observers in the physical as well as the virtual world, the resulting territorial privacy boundary also spans the physical and virtual environment of the user. Thus, users can effectively control their territorial privacy by eliminating observation channels to undesired observers.

Formalization

Our model can be represented as a directed graph $G(V, E)$. V consists of the source node s, which represents the user, and the set of all physical and virtual observers O. E is defined as the union of the sets of all observation channels, whereby $\mathcal{C}$ is the channel type set.

$$V = \{s\} \cup O,\ E = \bigcup_{i \in \mathcal{C}} E_i$$

A single observation channel $(u, v) \in E_i$ is a directed edge from node u to v of type $i \in \mathcal{C}$, with $u, v \in V$. We use $(u, v)_i$ as a short notation for a type-i observation channel.

All edges $(s, o)_i$, with $o \, in \, O$, are direct observation channels from s to physical observers. An observation channel to a virtual observer is a path of consecutive edges of length > 1, with potentially multiple intermediate nodes. The transitive closure E^* can be constructed, that contains all existing paths of observation channels of arbitrary length from s to any observer. Let E_i^* be the transitive closure of type-i observation channels. We assume that an observation channel of a given type is rooted in s, i.e., it is not possible that an observation channel of a new type emerges at an observer if no channel of the same type ends there. Thus, for the construction of E_i^*, we require

$$\nexists (u, v) \in E_i \Rightarrow (s, v) \notin E_i^* \ .$$

Now, we can make use of G to define the territorial privacy boundary of s in multiple steps.

1. Identify desired observers O_d.
2. Remove observation channels of undesired types $\mathcal{C}_u$.
3. Remove undesired observers O_u.
4. Remove undesired channels to desired observers.

Step 1 has to be performed manually by the user. Once the desired observer set O_d has been identified, the undesired observer set can be derived as $O_u = V \setminus O_d$. Step 2 has the purpose of initially eliminating generally undesired observation channels, hopefully cutting off large observer subgraphs. Step 3 explicitly removes remaining undesired observers. Finally, step 4 allows fine-grained refinement, e.g., when a desired observer may be allowed an auditive observation channel but not a visual one.

In step 2, the user first identifies undesired channel types $\mathcal{C}_u$. Then, all edges of types in $\mathcal{C}_u$ are removed from E and all nodes without a connection to s are removed from V:

$$E \leftarrow E \setminus \bigcup_{i \in \mathcal{C}_u} E_i, \quad V \leftarrow \{v \in V \,|\, (s, v) \in E^*\} \ .$$

In this process, desired observers that only had observation channels of undesired types are removed as well. Such conflicts can be detected by testing if $O_d \subseteq V$. A detected conflict needs to be resolved by the user, e.g., by explicitly allowing the undesired observation channel for a specific desired observer.

In step 3, undesired observers are removed from V:

$$V \leftarrow V \setminus O_u \ .$$

Then, the transitive closure E^* over s is constructed, and V is reduced to the reachable nodes in E^*:

$$V \leftarrow \{v \in V \,|\, (s, v) \in E^*\}, \quad E \leftarrow \{(u, v) \,|\, u, v \in V\} \ .$$

Note, that it can again be detected if desired nodes are removed in the process, e.g., as part of a cut off subgraph.

Step 4 allows further refinement. For desired observers with mutimodal observation channels to s, the user can explicitly specify observation channel types that are undesired for these observers as observer channel type pairs in $\mathcal{M}_u$ ($\mathcal{M}_u \subset O \times \mathcal{C}$). All elements of $\mathcal{M}_u$ are excluded from E:

$$E \leftarrow \{(v, o)_i \in E \,|\, (o, i) \notin \mathcal{M}_u\} \ .$$

Finally, E and V contain desired observation channels and desired observers only.

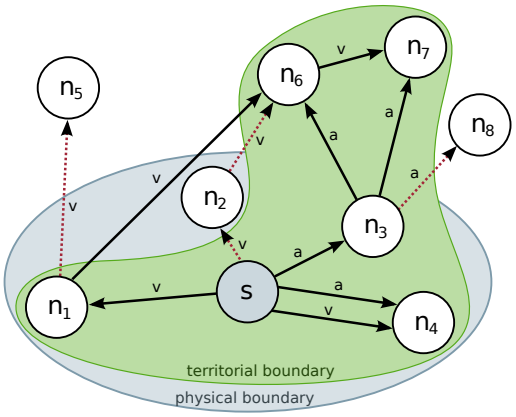

Figure 2: Graph representation.

Figure 2 shows an example of the graph notation. Here, physical observers are $\{n_1, n_2, n_3, n_4\}$ and virtual observers are $\{n_5, n_6, n_7, n_8\}$. The desired observer set is $O_d = \{n_1, n_3, n_4, n_6, n_7\}$ and the undesired observers are $O_u = \{n_2, n_5, n_8\}$. Undesired observation channels are marked by red dotted edges. By applying the steps above, the graph can be reduced so it only contains desired observers (inside territorial boundary) and desired observation channels (solid arrows).

Example Use Case

Now, we show how the model can be employed to an actual use case, and how it can be used to make decisions concerning territorial privacy. In our example, Alice is at home and receives an incoming video call. There is a webcam and a microphone in Alice's room as part of the video call setup. A screen and speakers are also present for video and audio output. But for now, we are only concerned with observers.

While alone, Alice does not want the webcam and microphone to be active. Thus, they would be undesired physical observers lying outside Alice's territorial privacy boundary and must be deactivated.

Now suppose Bob, Alice's boyfriend, is calling. Alice has defined her territorial privacy policies in such a way that incoming calls from Bob are automatically accepted. Therefore, Bob becomes a desired observer when calling. Alice grants him a visual observation channel through the webcam and an auditive observation channel via the microphone. Therefore, Alice's territorial privacy boundary is extended to include the webcam and the microphone as physical desired observers, and Bob as the virtual desired observer for these channels. Similarly, Alice would be moved inside Bob's territorial privacy boundary as a desired observer for his audio and video channels.

At the same time, intermediate nodes, like the video call service provider, would be considered virtual undesired observers that should not have access to Alice's channels. However, if these nodes would be completely removed from Alice's graph the connection to Bob would be lost. Thus, these nodes need to be removed logically by technical means. For example, Alice could encrypt both observation channels. The channels would still be relayed by intermediate nodes but they would not be able to access them.

Discussion

The benefit of our model is that it allows the definition of a complex territorial privacy boundary that spans the physical as well as the virtual world. The model focuses on who can observe real-time information about the user and how, which is orthogonal to information privacy models that describe who can access what information.

Obviously, our model does not capture all aspects of territorial privacy, yet. So far, our model facilitates the user-centric definition of a territorial privacy boundary in a concise way. The graph notation will provide a base for definition, enforcement, and dynamic adaptation of the territorial privacy boundary.

However, intrusions into a user's private territory can currently not be expressed. In our example, the incoming call from Bob and the subsequent activation of speakers and screen as output devices could be considered intrusions. But our model has been designed with extensibility in mind, so that intrusions and other aspects can be incorporated in the future. We believe, that starting with a small yet extensible model is a reasonable approach for tackling the domestication of the territorial privacy problem in future smart and ubiquitous computing scenarios, step by step. The next Section outlines several research challenges that need to be addressed in the future to ultimately give users full control about their territorial privacy.

5. Research Challenges

Our proposed model is a first step towards controlling territorial privacy in smart environments. We are aware that it is not yet a comprehensive solution. In this Section, we outline several research challenges and open issues, which need to be solved in the future in order to achieve a comprehensive protection of territorial privacy in smart environments.

Territorial Intrusion

So far, our model covers territorial privacy aspects arising from entities which receive or observe any type of real-time information about a person. However, territorial privacy also involves aspects of privacy violations, which do not include any information at all, we call them *intrusions*. Such violations may arise when entities physically or actively intrude into a persons territory, regardless of what information they can acquire. For instance, the mere physical presence of another person or a robotic device could be an intrusion. But an active intrusion can also be caused by an entity that is not physically present, like remotely controlling a person's environment. We refer to such an intruder as a *virtual intruder*. Intrusions have already been seen in the discussed example, in the last Section. When Bob's incoming video call is directly output to Alice's screen and speakers, Bob is actively intruding in Alice's private territory albeit not being physically present.

Another aspect which needs further investigation is what we call the *intrusion chain*. Such a chain can be composed

of different virtual and physical entities, which perform actions that trigger other entities to perform certain actions that eventually result in an intrusion. For example, an elderly care system monitors a person with video sensors in order to detect life-threatening events. In the default state the system is a virtual observer. But as soon as a critical event occurs, the system will actively intervene in the situation, e.g., by automatically informing a doctor. This action is not a territorial intrusion in itself but eventually leads to a physical intrusion when the doctor enters the home of the affected person.

This short example demonstrates different challenges. First, modeling such intrusion chains is a complex task also touching information privacy, due to the fact that many different conditions and dependencies may exist which need to be respected. Furthermore, a passive entity, e.g., a recharging household robot, may be seen as an intruder albeit not being active. These kind of passive intrusions are hard to model because they are highly subjective and user-dependent, but need to be considered as well.

Demarcation

Demarcation of the private territory, i.e., the definition of the territorial privacy boundary, depends on two aspects: the user's context and the determination of observers and observation channels.

Contextual parameters can be the current location of a person or the current social context, e.g., what other persons are present and the user's relationship to them. A user may define it's territorial privacy boundary quite differently depending on whether family members, work colleagues, or strangers are present.

A location may be completely private or completely public, but can also be situated in between those extremes. Moving from a private to a public space often implies that a person loses control over the environment which in turn leads to the person losing control over his or her physical and virtual boundary. One might argue that in public spaces the enforcement of boundaries is impractical, because basically everyone can access a public space. Regarding control of physical boundaries this may be correct, but persons can at least perceive physical observers around them and can adapt their behavior accordingly. Examples of physical observers are other people waiting for the train or installed surveillance cameras. Obviously, perceiving physical observers will become increasingly harder the *smarter* our environment becomes. So even if a person believes to be alone in a public space, several hidden physical observers could be present. Those physical observers may in turn provide observation channels to even more virtual observers. Because the person cannot perceive all its observers, she cannot appropriately adapt her behavior. Thus, the detection of physical and virtual observers is an open issue to be addressed. Furthermore, context information needs to be taken into account to achieve accurate demarcation of the private territory by the territorial privacy boundary.

Policies

The dynamic adaptation of the territorial privacy boundary should be governed by the user's preferences for the current context situation. Such preferences need to be defined by some kind of policies. Finding adequate technical solutions for automated generation, enforcement, and adaptation of those policies will be the main challenges. Automated policy generation is necessary in order to simplify the process users have to perform to demarcate their private territory. Defining boundaries for each potential context and all potential physical or virtual observers would be infeasible. Generation mechanisms for new policies should adapt based on former policy decisions, commonalities of existing policies which fit the new situation, and other historical information about the user's behavior. Policies should also be adapted dynamically when context and personal preferences change.

Another aspect that may influence a user's desired level of territorial privacy is the current emotional setting. While in a bad mood, observers that are usually allowed inside the user's private territory may be denied access. For example, after a bad day at work, even calls from close friends may be rejected. The influence of social context aspects on territorial privacy needs to be investigated.

When the private territories of multiple persons overlap, arbitration of territorial privacy policies is required, resulting in a redefinition of territorial privacy boundaries acceptable for all parties involved.

Enforcement

Another issue is the enforcement of both physical and virtual boundaries as they cannot always be determined statically, and often depend on several dynamic contextual parameters.

The demarcation of the private territory requires that observation channels to undesired observers are eliminated, which in turn requires cooperation of heterogeneous systems. Further, guarantees are required that policy decisions are respected and enforced by systems and entities not under the user's control. Thus, reliable access control mechanisms are necessary, which are applicable for both physical and virtual boundaries. Developing these mechanisms will be one of the biggest challenges, due to the fact that all devices, observation channels, and types of intrusion need to be controlled. Extra care is required at the boundary of physical and virtual worlds. For example, Alice may allow Bob access to her webcam, but may not want another person near Bob's screen to see her as well. The coherent combination of physical and virtual access control mechanisms will prove challenging.

Trust is another important aspect which affects technical solutions for enforcement of territorial privacy boundaries. On a technological level, trust needs to be established between system entities to propagate and enforce policy decisions. At the same time, a person needs to establish trust into these mechanisms, on a psychological level. A user needs to be certain that system entities respect and enforce privacy preferences and decisions. User control coupled with direct feedback to the user may help achieve this. Feedback and

control mechanisms should enable the user to perceive how physical and virtual boundaries are going to be protected and enable interventions in the control process of specific boundaries. The user's perception of a system and how it actually operates may also be divergent. A user may trust a surveillance camera only to be active when its red light is on, while from a technical perspective the camera may still be recording when the light is switched off.

6. Conclusion

We have analyzed the issue of territorial privacy in future smart environments. While territorial privacy is actually an old concept, the advent of ubiquitous and pervasive computing requires a reassessment.

We proposed a user-centric observation model for territorial privacy that encompasses physical and virtual observers. Our model enables the definition of a territorial privacy boundary as a demarcation of a user's private territory. In contrast to the traditional understanding of territorial privacy, the boundaries of our model are not limited to the definition of physical spaces, e.g., by walls, but also allow comprehensive definitions which entities are allowed to participate virtually in the user's private territory, and how. Desired observers can be separated from undesired observers by eliminating undesired observation channels. Our graph-based notation facilitates clear definitions of territorial privacy boundaries.

Furthermore, we identified several challenges that need to be addressed in future research. Intrusions into private territories and intrusion chains need to be studied and modeled. The demarcation of private territories requires context information and mechanisms to determine observers. Expressive policies are required to specify user preferences and that also can be dynamically adapted to changing situations and requirements. Finally, the territorial privacy boundary needs to be enforced, which requires suitable mechanisms to establish trust between heterogeneous entities.

Besides addressing these challenges, new laws and legislation are required that recognize the territorial privacy aspect of future smart environments. De Hert et al. (2009) point out several weaknesses to this extend in the existing legal framework. Thus, laws and regulations need to be adapted to these newly arising threats on territorial privacy. Legal pressure is required to ensure that ubiquitous computing systems are built with proper privacy controls in place. So that ubiquitous computing may fulfill its glorious promises without eradicating territorial privacy.

7. Acknowledgments

The authors would like to thank Stefan Dietzel for valuable input on early versions of this paper. Parts of this work have been funded by the EU projects ATRACO (216837) and PRECIOSA (IST-224201).

References

Beresford, A., and Stajano, F. 2003. Location privacy in pervasive computing. *IEEE Pervasive Computing* 2(1):46–55.

Daskala, B., and Maghiros, L. 2006. Digital territories. In *Proceedings of the 2nd IET International Conference on Intelligent Environments*, 221–226.

Denning, T.; Matuszek, C.; Koscher, K.; Smith, J. R.; and Kohno, T. 2009. A spotlight on security and privacy risks with future household robots. In *Proceedings of the 11th International Conference on Ubiquitous Computing*, 105–114.

Hert, P.; Gutwirth, S.; Moscibroda, A.; Wright, D.; and González Fuster, G. 2009. Legal safeguards for privacy and data protection in ambient intelligence. *Personal Ubiquitous Computing* 13(6):435–444.

Hong, J. I., and Landay, J. A. 2004. An architecture for privacy-sensitive ubiquitous computing. In *Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services*, 177–189. Boston, USA: ACM.

Jiang, X.; Hong, J.; and Landay, J. 2002. Approximate information flows: Socially-Based modeling of privacy in ubiquitous computing. In *Proceedings of the 4th International Conference on Ubiquitous Computing*. 176–193.

Krumm, J. 2008. A survey of computational location privacy. *Personal and Ubiquitous Computing* 13(6):391–399.

Langheinrich, M. 2001. Privacy by design - principles of Privacy-Aware ubiquitous systems. In *Proceedings of the 3rd International Conference on Ubiquitous Computing*, 273–291. Atlanta, Georgia, USA: Springer-Verlag.

Langheinrich, M. 2002. A privacy awareness system for ubiquitous computing environments. In *Proceedings of the 4th International Conference on Ubiquitous Computing*. 315–320.

Marx, G. T. 2001. Murky conceptual waters: The public and the private. *Ethics and Information Technology* 3(3):157–169.

Solove, D. J. 2008. *Understanding Privacy*. Harvard University Press.

Stanton, J. M., and Stam, K. R. 2003. Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectives. *Surveillance & Society* 1(2):152–190.

Warren, S. D., and Brandeis, L. D. 1890. Right to privacy. *Harvard Law Review* 4:193–220.

Weiser, M. 1993. Some computer science issues in ubiquitous computing. *Communications of the ACM* 36(7):75–84.

Westin, A. F. 1967. *Privacy and freedom*. New York: Atheneum.

Xu, H.; Dinev, T.; Smith, H.; and Hart, P. 2008. Examining the formation of individual's privacy concerns: Toward an integrative view. *Proceedings of the 7th International Conference on Computer and Information Science*.