Measuring Privacy in Ubiquitous Computing Applications

Said Jafari, Fredrick Mtenzi, Ciaran O'Driscoll*, Ronan Fitzpatrick, Brendan O'Shea
*School of Computing,*School of Electronic and Communications Engineering, Dublin Institute of Technology, Kevin Street, Dublin 8, Ireland*

Abstract

The concept of "disappearance" underpins the original idea by Weiser on the philosophy of ubiquitous computing. Technology advancement is making ubiquitous computing feasible. The goal is to free users from managing interactions with systems. To achieve this, devices have to acquire sufficient and relevant information to provide the required services. This information is acquired without human assistance thus it poses a threat to personal and organisational privacy.

Measuring the degree of privacy offered by a particular ubiquitous computing application is a challenging undertaking. A major difficulty lies on the interpretation of the term 'privacy' itself. However, to ensure successful use of these applications for both users and organisations, it is important to devise a means to measure privacy.

This paper brings forward a discussion on measuring the degree of privacy offered by a particular ubiquitous application by assessing systems' components and their information needs. To address the problem, privacy metrics are proposed. These metrics will be of benefit to systems' designers as well as to users of applications.

1. Introduction

The proliferation of Ubiquitous Computing (UC) devices and smart environments add extra concerns to the privacy of individuals and organisations. Weiser explained the concept ubiquitous computing as disappearance of computing devices from human attention while providing services to users [1]. Disappearance property can be exhibited through invisibility of devices and automated control (freeing user from operating the devices). These devices interact and exchange information to provide services to user. How much personal information is acquired and exchanged between devices is a function of a device in that environment [2]. Acquisition and use of this information may infringe privacy.

Privacy is one of the delicate issues in the digital society that is difficult to define precisely and objectively [3]. Our position in this context is that users should be aware of the type of information collected, exchanged and processed in order to make choices. This awareness will permit individuals to limit exposure of their information. Privacy is a matter of choice and balance. The latter is concerned with protecting other entities interests. For a more complete discussion on privacy definitions, the reader is referred to [3, 4]. Objective assessment of information gathered and exchanged between UC components is essential for measuring privacy of UC applications. Metrics are necessary to ensure objective and repeatable assessments are achieved.

Metrics are numerical results pertaining to quantification of the characteristics of chosen attributes of an entity. Metrics differ from measurement (a process of measuring) in that they are generated from analysis of measurements [5]. Privacy metrics can be used to assess the degree to which a particular ubiquitous application or devices there in comply with privacy. Metrics are needed to ensure objective assessment in order to distinguish privacy aware applications from others. As the trend towards more sophisticated devices and ubiquitous applications increase, the need for metrics becomes essential.

2. Privacy Concerns in Ubiquitous Applications

Researchers have addressed and continue to address protection of information privacy in the digital society [2, 3, 6-9]. Privacy concerns in this field are elevated by four prevailing characteristics. These include ubiquity, invisibility, sensing, and memory amplification [6].

Ubiquity: A simple example of a ubiquitous computing device is a mobile phone. One of the consequences of mobile phones is infringe of location privacy. In essence, with ubiquitous applications, computing power becomes everywhere. As users change locations (such as home, office, to public places), different smart environments are visited. How much information is exchanged during this interaction is a function of each smart environment. In general, it is difficult to define a boundary for each application. This characteristic makes privacy protection in ubiquitous application difficult to achieve.

Invisibility: The disappearance nature of ubiquitous devices, from view and attention of the user, inhibits the ability to decide when to connect to smart environment. With no comprehensive

feedback mechanisms on interacting devices, exercising control on information flow is nearly impossible.

Sensing: Advancement of technology makes design of invisible sensors which are powerful and accurate on sensing a variety of environmental situations including personal emotional aspects such as stress and fear. Sensing capability increases concerns about privacy breaches, particularly when coupled with the two previously discussed characteristics.

Memory amplification: advancements of amplification technologies make it feasible to record every action taking place in the environment. Video and speech can be captured, amplified and exchanged as can any other digital information. In presence of these devices, personal privacy can be affected.

As discussed in many contributions [3, 4, 10], privacy is the right to be left alone. This fundamental property of privacy requires that one has to determine what to disclose and what not to. This control mechanism is possible when the user is given autonomy through technology to make their own decisions. Lack of pre-alert (or more formerly consent request) can lead to violation of the oneness principal (the right to be left alone).

In the legal and social frameworks, privacy has been dealt intensively, particularly is determining what constitutes private information and how to deal with it [8]. The later has been relatively easier to deal with. However determining what constitutes private information is a trivial exercise, as the inquirer's identity and context both influence user preference on privacy.

A traditional defense of personal privacy has been restriction of type of information that can be disclosed and the accurateness or depth of information. However, in ubiquitous applications, this type of defense perishes due to discussed characteristics of ubiquitous applications. It is necessary to device a way to measure the level of privacy in order to distinguish privacy-aware ubiquitous applications from others.

3. Related Work

Several measures have been applied to ensure protection of privacy[11-14]. Major efforts have been on devising regulations that focus on protecting privacy. The Organisation for Economic Cooperation and Development (OECD), outlined privacy guidelines in the form of eight principles [11]. The first principle is the collection limitation principle, which requires minimum data necessary to perform the purpose be collected, and with full knowledge of the user. While the OECD privacy guidelines are applicable to both manual and automated information, the design philosophy of ubiquitous computing may contradict this principle [14]. For example, a mobile phone can identify itself in a smart environment disclosing information which may threaten privacy of the person. To ensure limiting the risk of privacy breaches in ubiquitous applications and devices, metrics are needed to provide an insight on the amount and type of information required and exchanged invisibly without users' attention.

Spiekermann [14] proposed scales to measure to what degree UC privacy enhancing technologies (PETs) are able to induce a perception of control in people. The author assumed that if people perceive control over UC environments through their PETs then they will also perceive themselves exercising their right to privacy. The scales developed were used to test peoples' perceived control of their privacy when they interact with intelligent infrastructure. Categories considered for scaling were helplessness, contingency, choice, power, information and ease-of-use. For each category, a set of questions were designed to measure the perceptions. The approach employs interview and factor analysis methods to ensure the suitability of the chosen categories, questions and development of scales. All questions were given ordinal scales on which to compute the perceived measure of a particular category. While its focus was to measure perceived privacy, the scales are of limited use in assessing to what extent a particular application is privacy aware without needing to consider user perception.

Scholtz proposed a framework for evaluating usability in ubiquitous computing applications[13]. In the framework, several metrics to assess usability in the field were suggested. Some of the proposed metrics can be adopted by tailoring and calibrating them to describe the degree of confidence on privacy offered by a particular ubiquitous computing application. Examples of metrics proposed which can be used to measure privacy are shown in Table 1.

Table 1. Examples of Metrics [13]

s/n	Property to measure	Conceptual measures
1	Privacy	Amount of information a user has to divulge to obtain value from application
		Availability of explanations to a user about the potential use of recorded data
2	Customization	Time to explicitly enter personalization information or time for the system to learn and adapt to the user's preferences
3	Behaviour changes	Type, frequency and duration
		Match between user's current job description and application

		role
4	Focus	Number of events not noticed by a user in an acceptable time
		Number of different displays/ actions a user needs to reference to accomplish an interaction or to check on the progress of an interaction

Ranganathan *et al* [12] proposed a set of metrics to evaluate various aspects of ubiquitous computing application. Their metrics cover the areas of context sensitivity, security and discovery. Privacy was not considered. However, some metrics may be useful to illuminate privacy. Such metrics include those related to context-sensitivity and application mobility. Examples of these metrics are given in Table 2.

Table 2. Examples of metrics [12]

s/n	Metric	Interpretation
1	User control over private information	0-3, where 0 = no control provided. 1 = system provides control over the disclosure of one kind of information (content, location, or identity), 2 = system provides control over two kinds of information. 3 = system provides control over all three kinds of information.
2	Expressiveness of the security (privacy) policy	Identified 4 different features for security policy expressiveness. We measure this metric by using a value of 0-4, representing the number of features supported. (1. Support for mandatory and discretionary rules, 2. Context sensitivity, 3. Uncertainty handling, 4. Conflict resolution)

4. Proposed Privacy Metrics

In devising sets of metrics for measuring the privacy level of a particular application, different design principles for privacy-aware ubiquitous are considered [6, 15]. These are alert, choice and consent (control), proximity, anonymity, and feedback [2, 6, 15].

Alert: This is a notification mechanism through which a user becomes aware of 1) smart environment, and 2) Information collection. Also, this property should consider notification when a user is switching between different smart environments. Metrics are devised to assess this design principal. Examples are given in Table 3.

Choice and consent: After notification, user should be given selection mechanisms to choose. This property is important for exercising user control over information.

Proximity: This principle refers to the ability of a system to intelligently understand the location and offer its services selectively. Implementation of this principle will limit unnecessary disclosure of information.

Anonymity: Unless explicitly required, user identity should be anonymous.

Feedback: An application should be able to log all usage of information. The principle will help monitor information usage, successful and unsuccessful requests and operations.

Table 3. Example of proposed metrics

s/n	Principle	Metric	Interpretation
1	Alert	Alert ratio	%ge of operations that goes unnoticed. Ideal value = 0
2	Choice and consent	Choice ratio	%ge of operations with no option. The higher the number of options the better. Ideal value = 0
		Consent ratio	%ge of operation which utilizes user information but do not require user consent. Ideal value = 0
3	Proximity	Scenarios counts	The reciprocal of the # of scenarios (policies or rules) that determine what decision to take. The more the number of scenarios the better the system. Ideal value = 0
4	Anonymity	Anonymity counts	The reciprocal of the # of user identities that are anonymous. The higher the # the better the system. Ideal value = 0.
5	Feedback	Log index	%ge of distinct operations that do not have explicit logging or feedback mechanism. Ideal value = 0.

Based on these four principles, a set of metrics is suggested by this for assessing each of the above mentioned principles. These metrics are given in Table 3.

The proposed metrics are applicable to a wide range of privacy-aware ubiquitous applications. Assessment and scoring for each metric can be aggregated to the total score. For each metric, an ideal value is proposed. They are designed to fall on one (lower) bound. Thus, the ideal value for aggregate score is zero (0), which signifies that a particular application is fully privacy-aware. An application which is not fully privacy-aware would tend towards large number (positive infinity).

5. Discussion and Conclusion

Based on literature, evaluations of UC applications have been done by assessing user perceptions. Privacy is usually perceived differently by different users. Measuring UC applications in terms of perceived privacy will not ensure consistent insights and benchmarks to enhance and distinguish privacy aware UC application from others. Alternatively, measurable system based characteristics should be identified for measuring privacy irrespective of user perceptions.

Despite the effort made towards privacy protection, design of useful privacy metrics for assessing devices and UC applications is largely an unexplored area of research. While recent studies have considered metrics for regulatory compliance, usability and security, there is a need for designing and developing a metrics framework for evaluating UC applications privacy. In this paper, together with review of initiatives for measuring information privacy, a set of metrics have been proposed for measuring privacy levels. While these metrics are not exhaustive, we believe that they contribute towards the derivation of a complete set of metrics for measuring privacy level of ubiquitous computing applications.

6. References

[1] M. Weiser, "The computer for the 21st century," *Scientific American*, vol. 272, pp. 78-89, 1995.

[2] S. Dritsas, D. Gritzalis, and C. Lambrinoudakis, "Protecting privacy and anonymity in pervasive computing: trends and perspectives," *Telematics and Informatics*, vol. 23, pp. 196-210, 2006.

[3] M. Langheinrich, "Privacy in Ubiquitous Computing," in *Ubiquitous Computing*, J. Krumm, Ed.: Chapman & Hall / CRC Press, 2009.

[4] C. O'Driscoll, "Privacy in context: Privacy issues in Ubiquitous Computing applications," presented at Third International Conference on Digital Information Management, ICDIM, London, UK, 2008.

[5] S. C. Payne, "A guide to security metrics," SANs Institute, 2006.

[6] M. Langheinrich, "Privacy by design—principles of privacy-aware ubiquitous systems," 2001.

[7] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, pp. 46-55, 2003.

[8] X. Jiang, J. Hong, and J. Landay, "Approximate information flows: Socially-based modeling of privacy in ubiquitous computing," *UbiComp 2002: Ubiquitous Computing*, pp. 176-193, 2002.

[9] S. Lederer, J. Mankoff, and A. K. Dey, "Who wants to know what when? privacy preference determinants in ubiquitous computing," 2003.

[10] L. D. B. Samuel D. Warren, "The Right to Privacy," *Harvard Law Review*, vol. IV, pp. 193-220, 1980.

[11] D. S. Herrmann, *Complete Guide to Security and privacy metrics; measuring regulatory compliance, operational resilience and ROI*. New York: Auerbach, 2007.

[12] A. Ranganathan, J. Al-Muhtadi, J. Biehl, B. Ziebart, R. H. Campbell, and B. Bailey, "Towards a pervasive computing benchmark," presented at the IEEE International Conference on Pervasive Computing and Communications (PerCom 2005), Kauai Island, Hawaii, USA, 2005.

[13] J. Scholtz and S. Consolvo, "Towards a discipline for evaluating ubiquitous computing applications," *Report from National Institute of Standards and Technology.[Online]. Available: www. itl. nist. gov/iad/vvrg/newweb/ubiq/docs/1 scholtz modified. pdf*, 2004.

[14] S. Spiekermann, "Perceived control: Scales for privacy in ubiquitous computing," *Digital privacy: theory, technologies, and practices*, pp. 267, 2008.

[15] V. Bellotti and A. Sellen, "Design for privacy in ubiquitous computing environments," 1993.

