

Article

Pervasive Computing, Privacy and Distribution of the Self

Soraj Hongladarom

Department of Philosophy and Center for Ethics of Science and Technology, Faculty of Arts,
Chulalongkorn University, Bangkok 10330, Thailand; E-Mail: hsoraj@chula.ac.th;
Tel.: +66(0)2218-4756; Fax: +66(0)2218-4755

Received: 5 April 2011 / Accepted: 20 May 2011 / Published: 27 May 2011

Abstract: The emergence of what is commonly known as “ambient intelligence” or “ubiquitous computing” means that our conception of privacy and trust needs to be reconsidered. Many have voiced their concerns about the threat to privacy and the more prominent role of trust that have been brought about by emerging technologies. In this paper, I will present an investigation of what this means for the self and identity in our ambient intelligence environment. Since information about oneself can be actively distributed and processed, it is proposed that in a significant sense it is the self itself that is distributed throughout a pervasive or ubiquitous computing network when information pertaining to the self of the individual travels through the network. Hence privacy protection needs to be extended to all types of information distributed. It is also recommended that appropriately strong legislation on privacy and data protection regarding this pervasive network is necessary, but at present not sufficient, to ensure public trust. What is needed is a campaign on public awareness and positive perception of the technology.

Keywords: pervasive computing; ubiquitous computing; ambient intelligence; privacy; self; distribution; trust; personal identity; public perception; ethics; metaphysics

1. Introduction

The emergence of what is known variously as “pervasive computing”, “ubiquitous computing”, “ambient intelligence”, or “internet of things” has created a number of conceptual and normative issues that deserve closer attention. Basically speaking, these refer to the ability of devices, which are normally not computers, to communicate with one another through a data network so that the network itself is not limited to the traditional structure of a computer network, but extends to ordinary things,

including the human body. Applications of this ability for things to network with one another are many. For example, a refrigerator might be able to connect with a grocery store in order to inform the store when certain items are running out so that the store can supply these items automatically (assuming, of course, that the owner of the refrigerator has agreed to this networking). Another application might include networking between the human body and medical care units, so that when certain physical indicators fall below a certain threshold, data can be sent out from the sensor in or on the body to the medical unit in order for the latter to take appropriate action. One can certainly imagine more applications that could be potentially useful, such as a car that can sense the condition of the driver. With such an application, if the driver is unacceptably tired or sleepy or has more alcohol in his bloodstream than the lawful limit, the driver's commands can be negated or overridden.

In this paper, I would like to focus on the conception of self that is affected by this emerging technology. This issue is significant because guidelines designed to protect the privacy of the individual are justified on the basis of a conception of the self. As the self of an individual should be accorded dignity and treated with respect as ends and not merely as means, the mainstream argument is that privacy is needed as a necessary ingredient so that the individual is accorded respect and dignity. Without the space made available with privacy protection guarantees, it is not possible for an individual to enjoy dignity or respect. According to the mainstream argument, this line of reasoning seems to require that there be an objective conception of the self such that the self exists as the basis on which the individual is maintained as an actual subsisting, objectively existing, entity. This is often overlooked in the mainstream argument, but it is certainly implicit in it. An implication is that, as we are considering how the conception of privacy is affected by the phenomenon of ubiquitous computing, the conception of self needs to be considered because the phenomenon does affect how the self is constructed and understood in significant ways, or so this paper will aim at arguing.

The structure of the argument presented in this paper is that: The phenomenon of ubiquitous computing or ambient intelligence does affect the conception of the self in a significant way, and as the self is necessary as the basis on which privacy guidelines can be developed and defended, the emergence of ubiquitous or pervasive computing does have a significant impact on how privacy should be justified and how privacy guidelines could be developed and enforced.

2. Ubiquitous Computing and the Self

The body itself becomes part of a pervasive or ubiquitous network when information pertaining to the body is distributed in the network in a significant way. The example alluded to above about a sensor attached to the body sending out signals on vital information, such as blood sugar level, blood pressure number and other medical statistics, to the medical unit is a clear indication that the body can indeed become enmeshed in the network. Indeed, not only is the body already becoming part of such a network, but in fact much of the mind is also fast becoming included, if not entangled already. A vast majority is already well acquainted with the ability to engage in a computer network, sharing the content of one's mind—one's thinking, one's beliefs, desires and so on—with one's peer. This is an example of the potential for sharing the mind throughout a network, and this sharing predates ubiquitous computing. However, one can certainly imagine a scenario where the content of one's mind

is shared through a ubiquitous computing network. This could be done by installing a device in the brain that senses the electrical movements inside the brain representing various thoughts and desires and sending out information of these movements to a network. This could of course be controlled by the subject so that he can choose which mental information can be sent out. For centuries there has been talk about some very special people having telepathic ability, but now with advanced technology this appears to be an impending reality. The upshot is that information pertaining to both the body and the mind of an individual may soon be distributed throughout a network.

What this means is that the self itself is distributed throughout the network too. This may sound rather surprising at first, but when it is understood that the self itself is constituted through information then it does not sound so surprising at all. One recognizes that the self is constituted through information when one realizes that anything that one encounters when one encounters one's own self is nothing but information. This does not mean that everything is information only, but what we know of our selves is all information. For example, consider a very simple statement describing my body:

(1) I weigh 80 kilograms.

The statement obviously refers to a condition of my body at the moment of this writing, that it weighs 80 kilograms. The first-person pronoun "I" refers to the person who is writing this paper and more accurately to his body, which weighs 80 kilograms. Since it is my body that weighs 80 kilograms and since it is the actual referent of the first-person pronoun, it is not too wide off the mark to say that my body is at least part of my own self. To say that I weigh 80 kilos has some subtle difference with saying that Soraj's body weighs the same, for when I say that it is "I" which weighs this much, the term has indexical force which is lacking when I say that Soraj weighs 80 kilos. The indexical force is more intimate in that it refers to the person who is uttering the statement himself. This is the conception of self that is normally understood. We have access to our selves through the use of the first-person pronoun "I", or "me".

In addition, when I think of something, such as when I am thinking of how to formulate the argument for this paper, I might be thinking thus:

(2) I am thinking of how best to formulate the argument for this paper

Here I am referring to an episode of my mental events. The idea here is that my mental life—all of my personality and everything that constitutes myself which is not overtly physical—is constituted by a series of events, each of which is an episode. As before, I am referring to myself which is thinking of something. Here the indexical force of the first-person pronoun is also there, for it is clear that (2) differs markedly from the statement.

(3) Soraj is thinking of how best to formulate the argument for this paper.

It is the indexical force that is indicative of the self.

Now suppose that we can accumulate all the statements about one's body throughout a period of time, as well as statements describing one's mental episodes as they progress through his or her life. It does not seem too far fetched to conclude that these statements taken together represent the account of that person's self. After all, the self is given content through these statements which are true of it and

which all together give it its uniqueness vis-à-vis other selves. For example, I have my own unique narrative which constitutes my life story. Everybody has his or her own unique story that accounts for his or her own self. But if it is story, if it is narrative, that gives a self its uniqueness, its standing as a self, then it seems that the self is constituted through information, for it is information that is contained in the statements that make up the narrative of a self. In fact, Paul Ricoeur has written much on the role of the narrative in self and identity [1-3].

Consequently, statements such as “I weigh 80 kilograms now” or “I am feeling very pleasant with the cool breeze” and so on are constitutive of the unique narrative of an individual self. These statements presumably do include such statements as “My current blood pressure measure is 140/90 mmHg” or “My pulse rate is 102 beats per minute”. These vital statistics do not seem to belong any less to the conception of the individual’s self than those measuring his weight or his height. In short, they are constitutive of the individual’s self as well.

What is true for bodily episodes is true for mental episodes as well. It can be said that information sent out by the subject is part of the self of the subject. Suppose that the subject sends out the message “I am very tired.” through a telepathic network. The message contains information that describes the state of the mental and physical condition of the subject that is part of the self of the subject at that moment, since it refers to the referent of the first-person pronoun. Moreover, even information sent out without the subject’s conscious awareness, such as when a sensor sends out information pertaining to the subject’s condition of his brain through some kind of implanted device, is also a part of the subject’s self as it portrays the condition of the subject’s mental episodes (assuming that the mental can be mapped onto the function of the brain). Since these episodes belong to the subject, it is as much a part of his own self as anything is.

A consequence of this is that through a pervasive computing network the self can be distributed across the network in a variety of ways. We can say rather informally of information about ourselves that is distributed this way that “this is part of me.” That the information can be a part of the subject means that the self in a way does not have to be located within the confines of the subject’s body, but can spread out of it too.

Basically speaking, this implies that information that can be related back to the subject’s self or person is thus part of the subject’s self. In this way my national identification card, which every Thai citizen is required to carry, is part of my own self as it contains information that is uniquely related to me. It contains a unique national identification number, which is specific to each and every Thai citizen; thus it is always possible for the authorities, or those with the appropriate means, to know much more about myself if they know only my thirteen-digit number. They will know where I live, who I am married to, how many children I have, who my parents are, who my siblings are, and possibly much more. Also, in roughly the same way, artistic creators often feel that their creation is not only something that comes from them, but the creation is in a significant sense a part of them too. Thus when we listen to a piece by Schumann, we often learn about his personality, his feelings, his temperament, and so on; in short, those traits that constitute specifically who Robert Schumann was and none other. Through his music we have a window to Schumann’s very self. Since Schumann is no longer alive, there is a sense in which his self lives on through his musical creations.

The emergence of a pervasive computing network appears merely to accentuate this ongoing trend. What it does is that it accelerates the rate and level of distribution of information much more than previously possible. It also adds another dimension in which the information can be distributed without the subject being conscious of distributing it all the time, as a sensor device can do this on its own. Hence the self gets distributed much faster, and there is more of the self that is distributed than at any previous time. Nonetheless, this does not seem to detract from the fact that the self is there in the information constituting it. The speed and volume of the distribution, however, raises a number of concerns which are unique to it. The problem is, if we are to reap the optimal benefit from the emerging technology of ubiquitous or pervasive networking, how should we ensure that the system is trusted by the user and that the user's privacy is protected? Without a clear understanding of how trust and privacy can be ensured, the potential benefits of a world of pervasive networking can hardly be made fully available.

3. The Self and Privacy

Privacy is very much related to the self. In fact, it is none other than privacy of the self that is the key issue in formulating privacy protection guidelines. In former times, one was concerned with privacy of the outward, physical body. For example, one was concerned that one had privacy within the domain of one's own home, such that it was not right to peep into somebody's house to find out what he or she was doing there. Also, privacy of communication is protected, so that it is not right, indeed illegal, to open up someone's private mail without permission or to tap into someone's private conversation over the phone. These are well-known privacy violations. With new, advanced technologies, privacy issues have become broadened. One concern has been with the social networking websites, which allow for an unprecedented degree of "opening up oneself" and thereby posing a serious threat to privacy. Social networking websites such as Facebook tend to have an uncanny ability to extract users' private thoughts and information so that users do not feel *prima facie* that their private lives are being threatened. On the contrary, they often feel that they are disclosing private information of their own free will, while in real, offline life they would hardly have revealed so much even to their close friends. Perhaps it is the degree of distance afforded by Facebook—the distance felt by users when they log on to the website, when they are alone with their computer and their "friends" are only blips of images and texts on screen—that gives users a false sense of security so they feel there is little danger in revealing their innermost secrets on the website. As there are a tremendous number of studies on privacy on social networking websites, the present paper will not touch upon this topic in any further detail. But it suffices to show that privacy has become a serious concern with today's technology, and what can be dangerous is that many are not fully aware of the seriousness of the problem.

On Facebook, one can be said to send out one's "self" on the network, to a circle of friends or even to the entire cyberworld. Thus, it is possible to construct a conception of self from the bits of images, videos, sounds and texts that are related to a person who has a Facebook account and who is engaged in online activities there. This self might not be exactly the same as the usual, offline self of the person, as the person might consciously construct an online persona for a variety of purposes. Perhaps the

person might want to project an online persona into the cyberworld as a way of keeping her real identity hidden, or as a way of participating in a specific “community”, a certain type of group of friends. It is possible that the person even maintains more than one persona, each for a certain type of community. For example, someone might project her real identity (a profile containing her real name, real email address, and so on) to a group of friends that are related to the work she is doing, but project a different self for a group of friends who are related to her special interests. In any case, it is plausible to have multiple selves which are manipulated and tailored to the community one is connected to.

However, the situation for ubiquitous computing is a little different from networking on sites like Facebook because with ubiquitous computing the subject does not have to log on to any online system and sit in front of a computer, but the data can be received and transmitted twenty-four hours a day, seven days a week, integrating one’s entire body (possibly including mental episodes) with the network. As the self is constituted by the information pertaining to it, there is clearly a sense in which the self is distributed throughout the network. This does not mean that the whole self of an individual can be found on the network such that one can, for example, speak to a computer screen on which some data pertaining to the individual appears. But it means that, in a significant sense, part of the individual’s self is there on the network. The self can be scattered around throughout space and time in the same way as, in a sense, Schumann’s self is distributed across time when we have a window to it or when we get intimate with it when listening to his music. Schumann does exist through his music when we listen to it and appreciate it. On Facebook, the self of someone is likewise scattered around the network, on the news feed of friends, on the huge database kept by Facebook for the purpose of selling profiles to advertisers, and so on.

So, if the self can thus be distributed, how then should privacy concerns be addressed? How should the privacy of the distributed self be protected? There is an irony involved in all this, for privacy is a value that protects the subject from distribution of information that the subject does not want to be distributed. Thus, if the self is distributed, then it seems that privacy is compromised in the first place. However, if distribution is based on trust, and if there are satisfactory guidelines for privacy protection, then trust and privacy can certainly be a guaranteed component. When a part of myself, for example, does exist on the network, I clearly want my privacy protected so that my information is not abused or misused by anyone who is not authorized to have access to it. Hence the control that I have on how my self is distributed becomes crucial. Furthermore, there should also be a way to protect the privacy of my self as it is distributed too. What this means is that, as a part of my self is distributed across the network, there should be some kind of measure or system to protect the integrity and privacy of the data that represent my self when the data exist on the network. If I were to allow a device to be placed on my body to measure my vital signs in order to send out signals to some appropriate medical unit, I would want some kind of protection, so that the information contained in the signal is available only to those at the medical unit who are responsible for reading and interpreting the data. Hence privacy protection is not only assured to my usual self, located physically within my body, but also extends to the distributed self that exists across the network.

To use the Facebook analogy again, it is clear that many Facebook users tend to disclose private information very casually, as if unconcerned with the privacy of their own selves. Nonetheless, there should be privacy protection of the information so divulged, and it should be the burden of the website

owner and the appropriate political authorities to ensure that the privacy of the user is protected. The authorities should not push the burden of protecting privacy onto individual users alone, especially as most users are not careful enough to ensure their own privacy. There should be appropriate legal mechanisms so that the website owner is forced to install privacy protection measures inside the website in order to ensure that the space available to users on the website is sufficiently protected and safe. This will be to everyone's benefit.

The same should be the case for pervasive computing. In fact, there are already a number of works published dealing with privacy in a ubiquitous computing environment [4,5]. As information pertaining to the self is being distributed throughout the network, appropriate privacy protection measures should be in place to protect the privacy of the self that is distributed, in addition to the protection traditionally given to the individual. However, the protection needs to be commensurate with the type of data that are being distributed. Information one voluntarily divulges on Facebook, even though part of one's own self, should not have the same level of protection as information propagated through the sensors in a ubiquitous computing network. On Facebook and other social networking sites, one ideally should be aware of what kind of information pertaining to oneself (which is actually part of one's self, as we have seen) is being distributed through the network of one's friends or even the public at large, and one should also be aware that there are mechanisms inside Facebook itself by which one can control how the information can be accessed by others. In a ubiquitous or pervasive computing network, however, information appears to be much more intimate; it is not only information such as my preferred restaurants that I share with my group, but something about my own physical body itself. Hence, protection of these varying kinds of information may vary too. But still the bottom line is that no matter how the type of information differs, it is part of an individual self, which needs to be protected. Here, the administrator of the network as well as the political authorities needs to get involved. An effective data protection law, with added clauses specifically mentioning personal data distributed across a pervasive computing network, might be what is needed to ensure both privacy and trust, both of which are necessary for the technology to be accepted widely by the public.

4. Justifying Privacy

The view that the self is distributed throughout the network is predicated on the idea that the self is not an inherently subsisting metaphysical entity that exists objectively. Instead, it is ultimately speaking of a construction out of a large number of physical and mental episodes that all together make up an individual person. This idea is not new. In fact, it is an ancient view found in Buddhism [6]. However, it appears to be corroborated by findings in contemporary cognitive neuroscience. For example, Michael Kurak [7] has compared the recent findings in neuroscience regarding the self and consciousness with the ancient teachings of Buddhism on dependent co-origination. What has been found is that both agree that the self consists of several states or episodes which are collected together in order to form a coherent, working, normal self. This view also finds support in Metzinger, who argues that "Nobody ever *was* or *had* a self" [8]. According to these findings, then, the representation of the self is nowhere to be found physically inside the brain. That is, there is no one locus inside the functioning brain that is directly responsible for the consciousness of the self. On the contrary, the self

is constructed through a variety of factors and many functioning regions of the brain. The old idea of a homunculus inside the brain responsible for all cognitive and self-conscious activities is now as good as dead.

It has to be noted, however, that this does not mean that there is absolutely no such thing as the self. If such scholars and scientists as Kurak and Metzinger do deny that there is a self, then they are clearly wrong. This is so because our experience of our own selves is so basic and visceral that it is almost impossible to deny one. What we should be focusing our attention on is not whether the phenomenon that presents itself to us as the self is in fact an illusion or not (perhaps it is), but even if it is an illusion, the fact that it is a very persistent illusion shows that the self phenomenon is something that we need to investigate and explain. We cannot deny our experience of the self, but it seems that, according to Kurak and Metzinger and according to the Buddhist system, what we do experience is ultimately nothing but a collection of mental and bodily episodes. Nonetheless, that something is a construct does not mean that it does not exist *tout court*. The idea that the self is a construct is also found in Susan Blackmore. In her book, *The Meme Machine* [9], Blackmore shows that what we understand to be the self in fact consists of a myriad of self-replicating cultural and informational entities known as “memes.” (The term actually originated with Richard Dawkins [10], who proposed the term as an analog of the gene. As the body of a biological organism is seen by Dawkins as only an instrument of the gene to carry itself on through replicating itself, the meme is then a *cultural* gene where what is replicated is an idea rather than genetic information.) Whatever we take to be the self, after analysis, we will find that this “self” is nothing but a collection of memes, which can consist of such things as memories, desires, thoughts, feelings, ruminations, and so on.

In sum, what these recent findings in neuroscience of the self show is that the idea of the self is constructed out of different episodes. These episodes, moreover, do not have to lie within the brain or the body, as we have already seen how a part Robert Schumann’s self can still be found in his music even though the composer himself is long dead. These episodes—the unique characteristic of Schumann’s music that provides a glimpse to his own personality and inner thoughts—are part of his self through the act of uniting them into one coherent self, and it is this act that collects together the mental and physical episodes of his body into his own self.

An implication of this is that the mainstream view that privacy is justified through reliance on the received view that the self exists as a unitary unit functioning as the seat of thoughts, and hence deserving respect, needs to be reconsidered. Since the self is not there objectively in the same way as the brain exists objectively, the justification of privacy based on the view that the unitary, self-subsisting self is a flimsy one at best. I have argued elsewhere that privacy should instead be justified pragmatically [11,12]. What this means is that we need to consider the goals of privacy guidelines and regulations—how having them contributes to realization of the goals we value—as the way privacy should be justified, rather than relying on the dignity of the person based on the metaphysical self.

That the self can indeed be distributed across a pervasive computing network supports the view that the self is a construction out of various episodes. As the self of the person needs to be protected as to its privacy, the part of the self that is distributed through the network needs protection too. What pervasive or ubiquitous computing does is merely to accelerate the rate at which the self gets

distributed, but the structure of the argument and the general form of how privacy is to be justified remains the same.

It is clear that privacy is pivotal in maintaining a democratic society, one which respects the dignity and rights of the individuals within that society. This is so because privacy provides for a space, a personal space around each individual, which allows the individual to operate freely within that space. Without such space, the individual will not be able to exercise many of the rights and privileges that belong to her as a citizen or a human person. For example, in voting in an election, it is customary, indeed it is necessary, for the voting citizen to have a degree of privacy so that she can decide whom to vote for without anybody looking over her shoulder. Without this minimal degree of privacy it is indeed difficult to see how democracy is possible. Furthermore, individuals should also have protection regarding privacy in their own homes. They should have freedom to communicate freely within the limit of the law and requirements of national security. To encroach upon this freedom would mean that the authorities would be given too much power, which makes it more likely that they could misuse it for their own immediate and self-regarding purposes.

One may wonder how privacy could in fact be justified when the metaphysical underpinning of the self appears to be as loose as the one presented in this paper, especially when privacy is bound up with notions such as moral agency and civic freedom, which are the basis upon which the modern liberal democratic state is founded. Moral agency and civic freedom seem to be founded upon an autonomous self; it is the very autonomy and independence of the self—the very notion that the self must be unified so that it can even begin becoming autonomous and function as a moral agent—that seems to be the reason why privacy of such a self should be safeguarded. By cutting loose this tie between the autonomous self and the notions of agency, autonomy and freedom, it seems that this paper lacks a tenable way of justifying privacy. Nonetheless, as I have argued elsewhere [11,12], a viable justification of privacy can indeed be constructed based on this notion that the self is a construction. Basically the idea is that one does not base privacy on the Western liberal notion of the autonomous, unified self. Instead privacy can be based on its function in a democratic state, as a protection against encroachment on personal freedom and personal space by the authorities. Since a democracy cannot function without such protection, privacy is then justified in this regard. Likewise, when the self is regarded as distributed through a network as presented here, one need not worry that there is not an adequately strong justification or defense of privacy. Such a defense and justification works more effectively, I believe, through regarding privacy functioning as a necessary component of the rule of law in a democratic state, and one defends it through overt demonstration, such as by pointing out what is happening in a state which does not have adequate privacy protection.

In conclusion, the argument presented here does not rely on the condition of individuals as autonomous subject, which seems to be presupposed by right-based arguments [13]. Justifying privacy on consequentialist and pragmatic grounds seems to be more powerful as it shows that privacy is necessary for the values and goals that we all hold dear. Even if the individual self is a construct and does not have firm, objective metaphysical footing, justification of privacy does not have to be weakened. On the contrary, it appears to be stronger when it is tied up with the desired political and civic values and goals.

5. Conclusion: Trust and Privacy

The justification of privacy regulations given above also makes it clear how closely related the concept of privacy is to that of trust, a topic that has been quite extensively explored in the literature [14-16]. What we have seen in this paper, however, is a new way of looking at this issue through the idea that the distributed self works as a basis upon which a reliable system of trust and privacy protection in a pervasive computing environment should be constructed. With emerging technology like ubiquitous computing, the role of trust is very important; if users do not trust the system, then it is hard to imagine how the technology can even get off the ground. Trust can only be generated when users are assured that their interests are protected and they will not be harmed, directly or indirectly, through their involvement with the technology. One of the most serious obstacles against widespread acceptance of internet commerce in Thailand, for example, is that most users do not trust the system. They do not trust putting their credit card information online because there have been many cases of fraud and inefficiency in the online commerce system. Enactment of appropriate legislation, such as the Electronic Commerce Act [17], which ensures trust in the basic documentation infrastructure such as digital signatures and so on, has been somewhat successful in promoting public trust in the system. This example shows that in order to create trust, a strong legal mechanism is important. But more important than the law, is that the technology itself must be designed with the interests and safety of users from the beginning. In designing a pervasive computing network, trust can be ensured when the privacy of users are fully protected so that no possibility of inappropriate use can arise. As telephone users generally trust the technology, believing their privacy in communication is protected, so communication enabled by a pervasive computing network can do the same. As the legislation ensuring trust in electronic commerce shows, strong legislation for a pervasive network is necessary to ensure public trust. This, to be sure, is not sufficient, as public awareness and perception of the technology plays a significant role too. Building up public awareness and perception could begin through a small number of successful uses of the technology in actual situations. Once this is perceived by the public to be useful, then the power of word of mouth can encourage the use of the technology rather rapidly. Here the perception at the first stage is crucial. If the technology fails during its first hurdle, then it will take a long time for it to recover from the injury.

So privacy and trust are intimately connected in the context of pervasive or ubiquitous computing. As the proposed idea of the distributed self through the network discussed above shows, privacy protection should be extended to the data themselves, since the data are in a real sense part of the individual's own self. This point could well be included in the legislation on data protection in pervasive computing. This is clearly necessary to ensure the public trust needed for the technology to be accepted on a wide scale.

Acknowledgements

Research for this paper has been made possible in part by grants from the Commission on Higher Education, Royal Thai Government, and from the National Research University Grant number

AS569A and HS1025A. I would like to thank the anonymous referees of this paper, whose comments have improved the paper a great deal.

References

1. Ricoeur, P. Narrative Identity. In *On Paul Ricoeur: Narrative and Interpretation*; Wood, D., Ed.; Routledge: London, UK, 1991.
2. Ricoeur, P. Humans as the Subject Matter of Philosophy. In *The Narrative Path, The Later Works of Paul Ricoeur*; Kemp, T.P., Rasmussen, D., Eds.; MIT Press: Cambridge, MA, USA, 1988.
3. Ricoeur, P. *Time and Narrative*; University of Chicago Press: Chicago, IL, USA, 1984-1988.
4. Price, B.A.; Adam, K.; Nuseibeh, B. Keeping ubiquitous computing to yourself: A practical model for user control of privacy. *Int. J. Hum. Comput. Stud.* **2005**, *63*, 228-253.
5. Dritsas, S.; Gritzalis, D.; Lambrinoudakis, C. Protecting privacy and anonymity in pervasive computing: trends and perspectives. *Telemat. Inform.* **2006**, *23*, 196-210.
6. Harvey, P. Theravada Philosophy of Mind and the Person: Anatta-Lakkhana Sutta, Maha-nidana Sutta, and Milindapanha. In *Buddhist Philosophy: Essential Readings*; Edelglass, W., Garfield, J.L., Eds.; Oxford University Press: New York, NY, USA, 2009; pp. 265-274.
7. Kurak, M. The relevance of the buddhist theory of dependent co-origination to cognitive science. *Brain Mind* **2003**, *4*, 341-351.
8. Metzinger, T. *Being No One*; MIT Press: Cambridge, MA, USA, 2003; p. 1.
9. Blackmore, S. *The Meme Machine*; Oxford University Press: New York, NY, USA, 2000.
10. Dawkins, R. *The Selfish Gene*; Oxford University Press: New York, NY, USA, 1990.
11. Hongladarom, S. Privacy, Contingency, Identity and the Group. In *Handbook of Research on Technoethics*; Luppigini, R., Adell, R., Eds.; IGI Global: Hershey, PA, USA, 2008; Volume II, pp. 496-511.
12. Hongladarom, S. Analysis and Justification of Privacy from the Buddhist Perspective. In *Information Technology Ethics: Cultural Perspectives*; Hongladarom, S., Ess, C., Eds.; IGI Global: Hershey, PA, USA, 2007; pp. 108-122.
13. Murphy, R.F. Social Distance and the Veil. In *Philosophical Dimensions of Privacy: An Anthology*; Schoemann, F.D., Ed.; Cambridge University Press: Cambridge, UK, 1984; pp. 34-55.
14. Bellotti, V.; Sellen, A. Design for Privacy in Ubiquitous Computing Environments. In *Proceedings of the 3rd European Conference on Computer-Supported Cooperative Work (ECSCW'93)*, Milan, Italy, 13-17 September 1993; Kluwer Academic Publishers: Norwell, MA, USA, 1993; pp. 77-92.
15. Gong, N.W.; Laibowitz, M.; Paradiso, J.A. Dynamic Privacy Management in Pervasive Sensor Networks. In *Proceedings of the Ambient Intelligence (AmI) 2010*, Malaga, Spain, 25-29 October 2010; pp. 96-106.
16. Campbell, R.; Al-Muhtadi, J.; Naldurg, P.; Sampemane, G.; Mickunas, M.D. Towards Security and Privacy for Pervasive Computing. In *Proceedings of Software Security—Theories and Systems Next-NSF-JSPS International Symposium, ISSS 2002*, Tokyo, Japan, 8-10 November 2002.

17. Electronic Commerce Act, B.E. 2544. Available online: http://www.mof.go.th/call_1689/images/stories/pdf/act1.pdf [in Thai] (accessed on March 15, 2011).

© 2011 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/>).