Table of Contents

International Journal of Secure Software Engineering

Volume 7 • Issue 2 • April-June-2016 • ISSN: 1947-3036 • eISSN: 1947-3044
An official publication of the Information Resources Management Association

Editorial Preface

Research Articles

The *International Journal of Secure Software Engineering* is indexed or listed in the following: ACM Digital Library; Bacon's Media Directory; Cabell's Directories; DBLP; Google Scholar; INSPEC; JournalTOCs; MediaFinder; The Standard Periodical Directory; Ulrich's Periodicals Directory

International Journal of Secure Software Engineering
Volume 7 • Issue 2 • April-June 2016

The Case for Privacy Awareness Requirements

Inah Omoronyia, School of Computing Science, University of Glasgow, Glasgow, UK

ABSTRACT

Privacy awareness is a core determinant of the success or failure of privacy infrastructures: if systems and users are not aware of potential privacy concerns, they cannot effectively discover, use or judge the effectiveness of privacy management capabilities. Yet, privacy awareness is only implicitly described or implemented during the privacy engineering of software systems. In this paper, the author advocates a systematic approach to considering privacy awareness. He characterizes privacy awareness and illustrate its benefits to preserving privacy in a smart mobile environment. The author proposes privacy awareness requirements to anchor the consideration of privacy awareness needs of software systems. Based on these needs, an initial process framework for the identification of privacy awareness issues is proposed. He also argues that a systematic route to privacy awareness necessitates the investigation of an appropriate representation language, analysis mechanisms and understanding the socio-technical factors that impact the manner in which we regulate our privacy.

KEYWORDS

Privacy Awareness, Privacy Awareness Requirements, Privacy Threats, Requirements Engineering

1. INTRODUCTION

The emergence of mobile and pervasive technologies has transformed everyday life (Aker & Mbiti, 2010), but privacy concerns threaten their acceptance by some users (Shin, 2010; Satyanarayanan, 2003). In part, the problem is with *privacy awareness*, which often arises when technologies blur the boundaries between public and personal spaces (Lahlou, et. al., 2005), and users are unaware of when and for what purpose sensitive information about them is being collected, analyzed or disseminated. Traditional theories suggest users should be able to manage their privacy, yet empirical research evidence suggests that users often lack enough awareness to make privacy sensitive decisions (Acquisti & Grossklags, 2005). This suggests a need for more systematic approaches to enable the explicit consideration of privacy awareness in software systems.

DOI: 10.4018/IJSSE.2016040102

Privacy awareness imbibes the notions of privacy and awareness (Figure 1). In requirements engineering, these two notions have been investigated in a number of research studies. In privacy research, the engineering of privacy requirements has been proposed (Kalloniatis, et.al., 2008; Bijwe & Mead, 2010; He & Antón 2003). Similarly, awareness requirements have been seen as an avenue to systematically capture the awareness features of systems (Mylopoulos et al., 2010; Endsley, 1993). However, while a number of research papers have pointed to the impact of awareness on the regulation of privacy (Mancini et.al., 2009; Jedrzejczyk, et.al., 2010), there is no approach to systematically describe, represent, and analyse privacy awareness from a requirements perspective.

Pötzsch, (2009) defines privacy awareness as an individual's cognition of who, when, which, what amount, and how personal information about his/her activity is processed and utilized. Pötzsch's view of privacy awareness helps provide a set of constructs for building a context for which privacy can be assessed. However, individuals' cognition of these contexts, and their description and implementation, has not been investigated in privacy engineering (Spiekermann & Cranor, 2009). We suggest that privacy awareness is critical to enable users and systems gain sufficient knowledge about how to act in privacy sensitive situations. As they gain assurance that their privacy is broadly preserved, they may consider forfeiting their privacy when engaging in some interactions. Privacy awareness is also useful to enable users understand the consequences of events on their privacy, and can assist in threat mitigation and subsequent reassurance that privacy is preserved.

In this 'visionary paper', we begin by presenting a short review of privacy and awareness concepts in section 2. In section 3, we then present our argument for privacy awareness by using a scenario to describe the privacy awareness needs that can help users establish appropriate levels of privacy. In section 4, we introduce and illustrate the notion of *privacy awareness requirements* as a novel systematic means for considering privacy during software development. We discuss open research issues for engineering privacy awareness in software systems. These research challenges range from methods and processes for identifying privacy awareness requirements, representation and analysis mechanisms, and the socio-technical issues that are inherent when considering the privacy awareness needs of software systems. Finally, we present our conclusions and own agenda for further work in section 5.

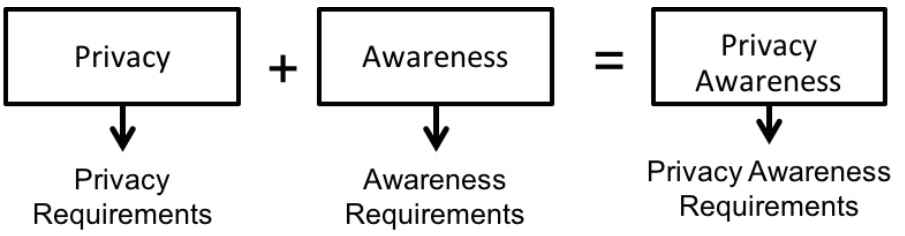
2. BACKGROUND AND MOTIVATION

While awareness and privacy are two distinct concepts that have been investigated separately in the development of software systems, little is known about the benefit of their synergy. This section reviews the background of these two concepts and motivates different aspects of individual privacy negotiations where awareness is essential.

2.1. Awareness

Dourish & Bellotti (1992) view awareness as "an understanding of the activities of others, which provides a context for your own activities". Gutwin & Greenberg (1998) present awareness as a

Figure 1. Privacy awareness and its requirements draw upon notions privacy and awareness



technique for enhancing coordination and efficiency when people work together. In requirements engineering, Mylopoulos et al. (2010) define awareness requirements as the class of requirements about the success or failure of other requirements. In cognitive psychology, awareness refers to the ability to selectively direct attention to specific aspects of the environment, and to be able to cognitively manipulate these aspects (Charlton, 2000). Thus, *attention* and *cognition* are the critical components of awareness. Attention involves an individual concentrating on some features of the environment to the (relative) exclusion of others (Gaver, et. al., 1991). Cognition is the process of gaining knowledge and comprehension from some feature to which an individual is attending. This act of gaining awareness by attention and cognition has been seen as a cognitive learning process – our creation of mental representations of physical objects and events and making sense of them (Williamson & Shneiderman, 1992). So awareness is far more subtle than just telling people what they should know, it involves presenting the message in such a way that it allows people to work out the answer themselves and deal with new or similar situations.

Furthermore, there are different levels of awareness suggested by the varying degrees of cognitive learning. For instance, Bloom's taxonomy (Anderson, et. al., 2000) in its various forms represents the levels of cognitive learning ranging from *remembering* – recall of relevant aspect of the environment, to *creating* – putting together different aspects of the environment to form a novel, coherent aspect. Each cognitive learning level is associated with action words, such as *list*, *identify*, and *infer*, to measure tangibly the extent of its achievement. Remembering is measured using action words, such as *list*, *identify*, and *show;* while creating is measured using to action words such as *modify*, *devise*, and *propose*. Other levels include: *understanding*, *applying*, *analyzing* and *evaluation*. Thus, there is a level of awareness an individual or system can attain that only enables remembering an aspect of the environment, while a higher level of awareness enables the ability to infer new aspects.

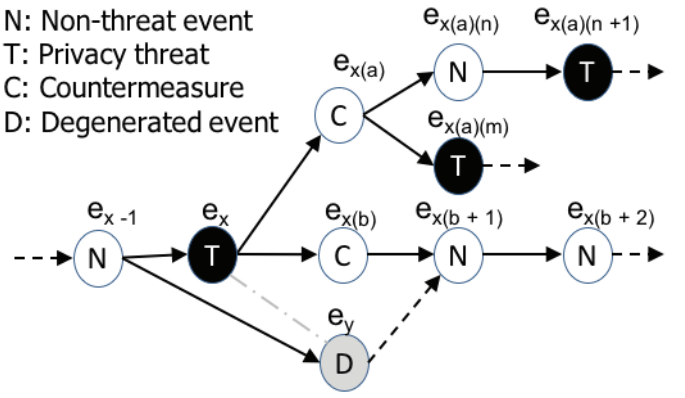
Central to awareness is the notion of *context* and *event*. Context is described by Omoronyia *et al.* (2010) as "the evolving internal and external state information that fully characterizes the situation of each entity in a shared environment". An event is an observable, discrete or coupled occurrence in the environment (Deleuze, 1992). This can be a users' action such as "close the door" or a systems' operation such as "send data". The attributes of an event (the set of circumstances surrounding an event) such as who, what, when, where and how, are the basic core determinants of context. Thus, context attributes are simply a combination of attributes from one or more events. Events also have the capability of adapting or evolving context from one state to another. Context adaptation occurs by the addition of a new attribute from an event, or a change in the value of an existing attribute. For instance, assuming the context of a group meeting is a "public session". Then a user event "close the door" can signal a change of context to "private session". In other cases, an event can depend on other events and/or can act as precursors for other events to occur. For instance, the system event "delete file" is precedent on the event "create file". This precedence relationship creates events precedence graph from which future probable context can be inferred (Figure 2).

A critical challenge for awareness is the recognition that context has changed as events occur in the environment, and the inference of a future context based on new events.

2.2. Privacy

A widely circulated viewpoint of privacy is "the right to be left alone" (Warren & Brandeis, 1890). This viewpoint suggests a *privacy state* where a user can make the choice to remain anonymous, unobserved and free from intrusion. But privacy theories as presented by Altman, (1977) and related works such as Derlega & Chaikin (1977) and Petronio (2010) argued that the determination of such privacy state typically entails a dialectic and dynamic boundary regulation process. Thus, privacy differs from security and does not necessarily mean absolute withdrawal from people, but rather a boundary control process, guarded by purpose (Guarda & Zannone, 2009). Purpose is an attribute of privacy that involves determining why and with whom contact will occur, and how much, how long, and what type the interaction will be. This notion of purpose characterizes interaction context

Figure 2. Event precedence graph



previously discussed in section 2.1 into two main categories: right context of interaction that helps achieve the desired purpose and wrong context of interaction that is a deviation from the desired purpose. Interaction here ranges from a simple communication process (visual, verbal, non-verbal, etc.) that does not involve data recording, to more complex practices involving data collection, processing and dissemination.

Privacy enforcement mechanisms (PEM) are guards enforced by individual(s) or system(s), against events resulting in context that will otherwise be a threat to preserving privacy (Guarda & Zannone, 2009). These mechanisms have evolved over time from behavioural mechanisms and nondisclosure of communications by/about an individual (Solove, 2008), to more mundane ones such as appropriate collection, processing and dissemination of personal information (Solove, 2006). Behavioural mechanisms include verbal, para-verbal (e.g. tone or pseudonyms), non-verbal (gestures), personal and territorial space. In line with existing literature in security and secured software engineering research, we categorise the events that result in context change (Anderson, 2008; Allen et. al., 2009). Hence, a *non-threat event* is an event for which existing PEM can guard against the violation of privacy. Conversely, a *privacy threat* is an event for which an existing PEM cannot guard against the violation of privacy. Finally, a *countermeasure* is an event that nullifies or reduces the consequence of a privacy threat, thus retaining some capability of existing PEM to still preserve privacy. A countermeasure can itself be a non-threat event, or indeed a privacy threat (albeit ideally with lesser impact and viewed as necessary in extreme circumstances to retain a privacy state- for example turning off a network or disabling a server is such am extreme counter measure).

When non-threat events occur, or countermeasures are used in threat mitigation, the risk of subsequent privacy states being threatened or violated can increase or decrease based on an associated events precedence graph. For instance, given the graph shown in Figure 2, and the occurrence of a privacy threat e_x, then the choice of $e_{x(a)}$ as a countermeasure poses an increased risk of a subsequent privacy state being threatened or violated compared to choosing $e_{x(b)}$. This is because $e_{x(a)}$ has set the precedence for the privacy threat $e_{x(a)(m)}$ to occur, or that the risk of $e_{x(a)(n+1)}$ occurring increases given its shorter distance from $e_{x(a)}$. Similarly, a previously non-threat event e_y *degenerates* to a privacy threat as a result of the occurrence of e_x weakening capability of an associated PEM to maintain privacy in a preserved state when e_y occurs.

PEM, privacy threat and countermeasure(s) then provide a pragmatic basis to distinguish between a 'right' and a 'wrong context. A *wrong context* is defined by attributes from privacy threat related event(s), while a *right context* is defined by attributes from non-threat event(s)[1]. The importance of this distinction is based on Pedersen (1999) reasoning that, to preserve privacy, awareness is necessary

of the appropriate choice of PEM that fits the context of interaction. On the whole, the distinction between right and wrong context provides the opportunity to use context attributes such as affinity, location, etc. as a means to categorise the outcome of privacy management into three states. These include *preserved*, *threatened* or *violated*. The right context maintains privacy in a preserved state. The wrong context moves privacy to a threatened or subsequent violated state.

Typically, during interactions, individuals tend towards maintaining their privacy in a preserved state, as this ensures their desired privacy requirements are satisfied. Alternatively, they can then forfeit their privacy and assume a default state with no need for privacy requirements. These privacy requirements represent a set of attributes about an individual's context which, if left unregulated, can result in privacy violation. Existing research literature also suggests that a preventive or curative approach can be used to preserve privacy (Nippert-Eng, 2010; Palen and Dourish, 2003). For a preventive approach, an individual wants to be assured that the initial context, for which an interaction is to be initiated, preserves their privacy need. Also, when privacy is in a threatened state as a result of a subsequent event, a preferred aim is to return to a preserved state rather than resulting in a violation. In a curative approach, a privacy need has not been satisfied, hence privacy is violated. Although the damage has already been done (as privacy has already been violated), the aim is to prevent more violation or to dampen the effect of a violated privacy state.

Given these different contextual issues involved in privacy regulation (Barth et. al., 2006), we argue that privacy awareness is an integral aspect of the appropriate management of an individual's privacy objectives. This is because different levels of cognitive ability that are related to the context attributes, privacy requirement, and PEM are needed to make decisions and adapt in a manner that preserves privacy. When an individual's privacy is violated or threatened, to prevent further degradation of privacy state, they need to gain cognition of events to avoid that were previously considered as non-threat that have now degenerated to privacy threats. Even when privacy is in a preserved state, an individual still needs to gain cognition of the risk of having privacy threatened or violated based on events that have generated current preserved privacy state. From a software privacy engineering perspective, we are interested in understanding what these cognitive abilities are, and the awareness needs that they seek to satisfy. In this paper, we present a case towards a systematic mechanism for capturing these privacy awareness expectations.

3. TOWARDS PRIVACY AWARENESS

We define *privacy awareness* as the cognitive ability to identify and act on a privacy state and the context of interaction that has resulted in such a state. The artefacts essential for acquiring such cognitive ability range from the privacy requirements arising from privacy objectives, the PEM used to guard against violations of privacy requirements, the attributes of an interaction context, and privacy related events that change an interaction context and potentially impact the performance of PEM. We focus on the rationale for privacy awareness using these artefacts.

An extreme scenario illustrating the need for privacy awareness and associated cognitive abilities is described in Case 1 (Figure 3). Aspects of this scenario, involving a smart meeting tool, have been inferred from the work of Zheng & Ni (2006) on smart phones and next generation mobile computing, and from reports on UbiComp workshops on smart mobile computing (John, 2007). The scenario highlights a number of privacy objectives ranging from *selective disclosure* of attendee's personal information; *avoiding intrusion* – acts that disturb attendees' tranquillity; and *preventing decisional interference* – incursion into an attendee's decision making process - see Solove, (2008) for more detailed description of these objectives. The scenario also exhibits privacy related events precedence (Figure 4) that can influence a meeting attendee's privacy objective. For instance, the event e_{2a} or e_{2b} cannot occur unless the event e_1 has occurred. The event e_1 will turn out to be a privacy threat to a privacy objective if the attendee is uninvited, and existing PEM are unable to satisfy the privacy requirement R_1 ('session meeting shall only be attended by invited attendees'). Furthermore, e_3 will

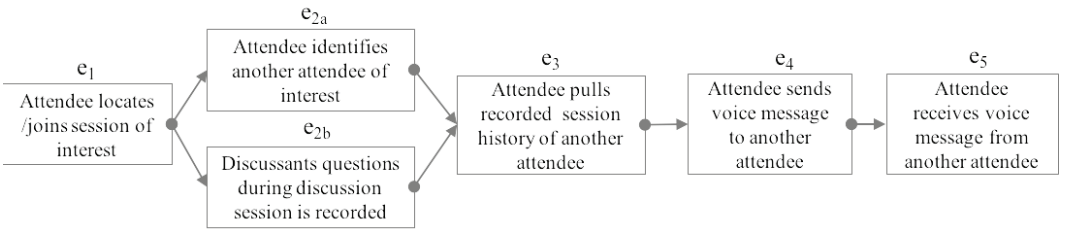
Figure 3. Case 1: Smart meeting

Case 1: *Smart meeting*

A saleswoman of a company is attending a series of physical technical meetings at which her customers are expected to attend. Attendance is by invitation and meeting attendees use their smart phones to locate areas and session meetings of interest. The saleswoman walks into a private technical session with her smart phone, which she uses to quickly find all meeting attendees who are current customers of her company. At the same time, she is able to use the smart phone to pull in other useful information, such as which meeting sessions they have attended and what questions they have raised during those sessions.

Cellular networks, wireless LAN, and Bluetooth are being used in the meeting area. Software on the saleswoman's smart phone scans the data flowing among these wireless networks and finds the most likely sales targets and presents to her accordingly. Using the scanned data from the different wireless networks and with some help from the customer relation management software at the company's headquarters, she comes up with a business plan that incorporates issues raised during previous meeting sessions and products of the company. She then sends voice mails to selected customers in the room asking for a brief meeting sometime later.

Figure 4. Smart meeting event precedence



degenerate to a privacy threat as a result of $e_1$being triggered by an uninvited attendee and existing PEM being unable to satisfy R_1. On the other hand, if the occurrence of e_1-e_5 is guaranteed by used PEM to be non-threat events, then an individual's privacy objectives within such context can be forfeited. In this section we use Case 1 to highlight the impact of context transition on privacy management, and also identify the privacy awareness needs that can help establish appropriate levels of privacy.

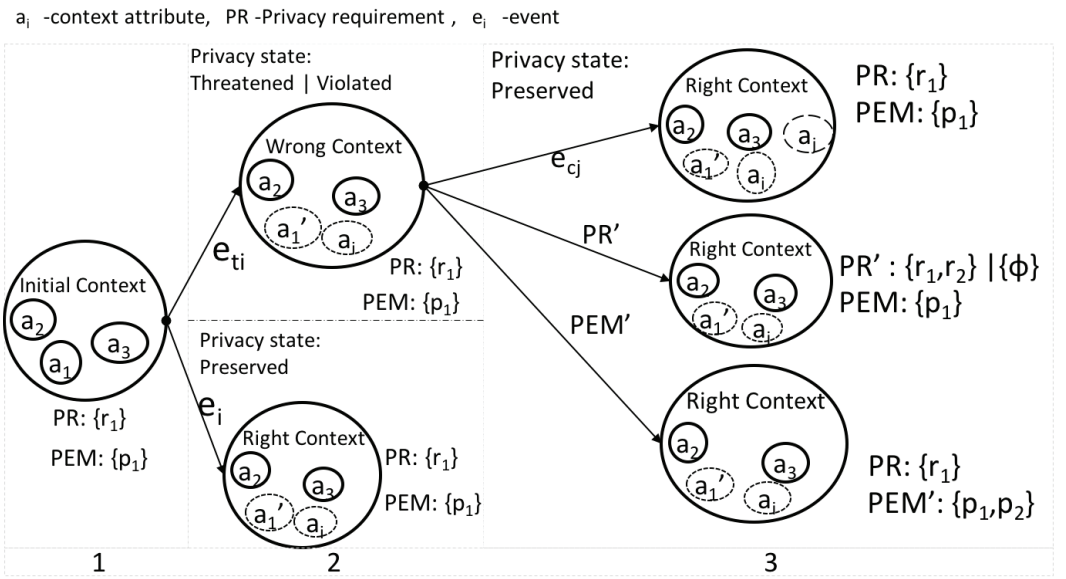
3.1. The Essence of Awareness in Privacy Management

We have identified four main privacy awareness needs that correspond to the duration before, when and after a privacy threat or non-threat event occur (Figure 5). First, privacy awareness should provide individuals the *assurance of privacy preservation* before an event occurs. Typically, if a user is not aware that his/her privacy is preserved, acceptance of the system is still questionable irrespective of the privacy infrastructure in place. This assurance is built as users gain cognition of the context within which they are interacting, and the guarantees provided by the PEM used to preserve their privacy. Second, privacy awareness should enable individuals to *understand the consequence of events on their privacy state* when the event occurs. Third, privacy awareness should enable individuals and systems *understand mitigation options* necessary for critical decisions necessary to mitigate a threat event. Finally, privacy awareness should also provide the *reassurance of privacy preservation* after a privacy threat has been mitigated. Cognitive abilities are required to assess when awareness required to satisfy these needs have been attained. Using the smart meeting scenario, we illustrate each need and the associated cognitive abilities.

3.1.1. Assurance of Privacy Preservation

Before individuals engage in interactions, they need assurance that their privacy is preserved within the context for which interaction is to be initiated. This corresponds to the duration before an event occurs and the first step that can lead to a transition to a right or wrong interaction context (Figure 5 step 1). This assurance of privacy preservation is based on guarantees provided by current PEM

Figure 5. Three steps showing context transition for privacy preservation



being sufficient to preserve privacy by satisfying specified privacy requirements within the identified context. Privacy awareness builds a perception of assurance that privacy is preserved within the context for which interaction is to be initiated. While no context changing event has occurred, the assurance of privacy preservation is the awareness that when the event occurs, the system has the capability to prevent its resulting in privacy being threatened or violated. The cognitive abilities required to satisfy this awareness need include: a) Identifying initial context by its attributes and currently used PEM; b) inferring resulting privacy state based on context attributes and used PEM.

Referring to Case 1, assuming the privacy objective of an attendee is the selective disclosure of his/her personal information, then a privacy requirement such as 'personal information shall not be revealed to unknown attendees' is relevant to maintain privacy in a preserved state. The assurance of privacy preservation for this privacy requirement cuts across different interaction context for which personal information can be disclosed. For instance, when attendees are using the wireless network within the meeting vicinity, when an attendee is moving around the lobby exchanging pleasantries and informally sharing ideas, and when a discussant's is speaking. Each of these contexts has its attributes for which attendees need to gain cognition as s/he seeks the assurance that his/her privacy is preserved. Assuming a context where the discussant is speaking during a meeting session, then the subset of attributes for this context for which cognition is required for assurance of privacy include: type – technical session, facilitator- Saleswoman, location – room A, recorded – true, no participants – 10 [invited=10, uninvited =0]. Furthermore, the assurance of privacy preservation also requires the cognition of currently used PEM within the interaction context to include room space of 10x10m, attendance based on invitation only, only meeting attendees can access recorded discussion, transient private key from a discussant is used by an attendee to decrypt and pull recorded session history, and use of verbal communication where voice is unheard outside room space. Then privacy preservation is assured in the meeting session by the ability of the discussant to infer every PEM within the context for which discussion is to be initiated.

3.1.2. Consequence of Events on Privacy State

When individuals engage in interactions, events are triggered that can result in a change in context. This context change can impact on user privacy. This is because, depending on the capabilities of current PEM to still satisfy the privacy requirement within the new context, the individual's privacy state can be preserved, threatened or violated. The essence of privacy awareness is the cognition of the consequence of triggered events on an individual's privacy state. As shown in Figure 5 step 2, an event can cause the transition of an initial context into either a wrong context resulting in a threatened/violated privacy state, or right context resulting in a preserved privacy state. Privacy awareness of any resulting privacy state is based on two cognitive abilities: a) Identifying an event and resulting new context, and b) inferring if currently used PEM has the capability to guard against privacy violation as a result of a new context.

Using Case 1, given the event e_1, if the attendee is uninvited, the initial context is then adapted to a new one by the change in the attribute value: no. participants – 11 [invited=10, uninvited =1], and the additional attribute: location – present in meeting room. Privacy awareness of the consequence of this event on privacy state first involves the cognitive ability to identify $e_1$and the resulting new context attributes. Secondly, the ability to infer that given the uninvited attendee is present in meeting room, current PEM do not have the ability to prevent the uninvited attendee from listening to the meeting when e_{2b} is triggered. Privacy awareness resulting from these two cognitive abilities is that privacy can be threatened or violated as a consequence of the event.

3.1.3. Mitigation Options

Assuming an event triggered during an interaction threatens or violates an individual's privacy, then coordination steps are normally initiated to mitigate the threat or violation. A threat mitigation process attempts to prevent a threatened privacy state from resulting in a violation, dampens the effect of damage caused by the violation, and avoids subsequent violations. This process involves considering one or more of the following options: the alternative or additional PEM that can preserve privacy by satisfying the individual's privacy requirement within the new context; the possible set of countermeasures that can result in alternative context for which privacy is preserved; and possible changes to individual's privacy requirements. The resulting context for each of these options is as shown in the context transition diagram of Figure 5 step 3. Privacy mitigation using countermeasure(s) results in an alternative context where the individual has additional new or changed attributes. Mitigation using alternative or additional PEM generates an alternative context where individual's attributes are unchanged. Mitigation by adapting privacy requirements also generates an alternative context where an individual's attributes are unchanged, but requires the individual to forfeit or change the desired privacy requirement. The forfeiting of privacy requirement is analogous to an individual no longer seeking to preserve the privacy of affected attributes of the generated context in order to get a service in return. Cognitive abilities essential to satisfy this awareness need for appropriate privacy mitigation include: a) listing unused PEM options, alternative countermeasures and possible privacy requirement adaptations; b) Identifying proposed additional PEM, appropriate countermeasure and/adapted or forfeited privacy requirement.

Using Case 1 where e_1 is triggered by an uninvited attendee, the scope for proposing mitigation measures is enhanced by cognition of possible events that can act as countermeasures (example: 'the attendee moves away from room space', 'the attendee receives an invitation', 'discussant stops speaking', or 'meeting suspended'), potential additional PEM (such as use of pseudonyms that is only understood by invited attendees), possible privacy requirement adaptations which can include the addition of new requirement, updating or forfeiting the initial requirement entirely. Typical additional requirements that can mitigate the consequence of the threat event include new requirements such as '*personal information shall not be displayed on projector screen in the presence of an uninvited attendee*' and '*the meeting type shall be changed to public session in the presence of an uninvited attendee*'. The cognition of each of these proposed mitigation measures, is the first step towards taking

the appropriate decision in transitioning a threatened or violated privacy state back to a preserved state. Thus, privacy awareness during threat mitigation ensures that the system or an individual has gained cognition of the broad scope of mitigation options available, before deciding on the mitigation path to be initiated.

3.1.4. Reassurance of Privacy Preservation

After a threat mitigation path has been initiated, the outcome is a transition into a right context over which privacy is preserved. Privacy awareness serves two purposes in this case. Firstly, it builds a perception of reassurance after mitigation that privacy is preserved within the new context. Secondly, it provides cognition of the impact of the choice of mitigation path to future privacy preservation. The cognitive abilities that provide the reassurance of privacy preservation then include: a) inferring resulting new context and privacy state based on adapted privacy requirement, additional PEM and/or use of countermeasure; and b) given a chosen mitigation path, cognition of possible interaction context, degenerated events and PEM that have lost the capability to preserve privacy.

Using Case 1, assuming the choice of mitigation path involves the use of additional PEM 'pseudonyms that is only understood by invited attendees', and additional new requirement 'personal information shall not be displayed on projector screen in the presence of an uninvited attendee'. Then firstly, privacy awareness involves the cognition that a combination of these two mitigation measures preserves privacy for the current context -an uninvited attendee present in a private technical session. Secondly, privacy awareness involves the cognition that the previous context over which assurance of privacy was attained by using PEM 'attendance based on invitation only' and the additional PEM 'pseudonyms that is only understood by invited attendees' degenerates e_3 to a privacy threat, as these PEM do not have the capability to prevent the uninvited attendee from pulling recorded session history.

The outcome of using privacy awareness as a mechanism to gain reassurance of privacy can sometimes result in further adaptation of privacy requirements, additional PEM and countermeasure negotiations. For instance, gaining the awareness that as a result of the presence of an uninvited attendee, the event e_3 is now a privacy threat, additional privacy requirement such as 'uninvited attendee shall not be able to pull recorded session history of attendees in a meeting' is then negotiated.

4. PRIVACY AWARENESS REQUIREMENTS: VISION AND OPEN RESEARCH ISSUES

A general open question is how privacy awareness needs can be discovered, described, analysed and observed for software systems. Privacy requirements techniques only focus on describing the privacy needs of individuals and not on awareness required to satisfy such privacy needs. In order to bridge this gap, we introduce the notion of *privacy awareness requirements* to support privacy requirements and provide a path to achieving equilibrium between privacy and awareness. This equilibrium reflects on cognitive abilities required to provide users and systems alike the assurance of privacy preservation, enable users understand the consequence of events on their privacy state, and assist in threat mitigation and subsequently reassuring users that privacy is preserved.

A privacy awareness requirement describes testable cognitive abilities that determine if the system satisfies its privacy awareness needs. Such requirements are identified in their use of cognitive action words. For instance, based on Case 1, requirements such as "An attendee shall be able to *differentiate* between invited and uninvited attendees in a private technical session" or "attendees shall be able to *recognise* the mode of communication during private technical session", are both fundamental privacy awareness requirements necessary for session attendees to be guarantee privacy preservation. Each requirement is measured tangibly using Bloom's (Anderson, et. al., 2000) cognitive action words –differentiate and recognise. Thus, privacy awareness is not attained if a meeting attendee is unable to identify an uninvited attendee in the session. Similarly, the requirement "Attendees shall be able to determine that an uninvited attendee has joined the meeting session", is a requirement necessary

to enable meeting attendees understand the consequence of events on their privacy state. Unique properties that identify a privacy awareness requirement include:

- **Subject of Awareness:** Individuals and/or systems that need to acquire awareness to better coordinate a privacy objective;
- **Object of Awareness:** Individuals and/or systems that can trigger privacy threats of which the subject needs to be aware;
- **Cognitive pointer indicating the level of awareness needed:** Described using cognitive action words);
- **Attributes of Interaction Context, Privacy Requirement, PEM and/or Privacy Threats that Impact on the Object of Awareness:** Referred to as privacy awareness artefacts. In mitigating a privacy threat or violation, awareness artefacts encompasses the countermeasures, additional PEM or privacy requirement adaptations necessary to achieve a right context of interaction where privacy is preserved.

We use the term agent when we are referring to an individual or system. A group of agents represents an ecosystem involving a cluster of two or more agents connected by their membership of a bounded set (Forsyth, 2014). An example of a grammar using EBNF (Extended Backus–Naur Form), and representing a meta-syntax for a privacy awareness requirement statement is as shown in Figure 6. Thus, given the statement "attendees shall be able to recognise the mode of communication during private technical session", the properties that identify the statement as a privacy awareness requirement are as follows: subject of awareness –attendees; object of awareness –private technical session; cognitive level of awareness – recognise; and attribute of context – mode of communication.

We focus on a subset of open research challenges: methods and processes compactible with the kind of privacy awareness requirements we have discussed thus far; a representation language and analysis mechanisms; and finally, investigate the socio-technical factors that are inherent in satisfying identified privacy awareness issues (Figure 7). Each of these identified challenges will also require the support of tools and modalities for automation. Addressing these research issues can perhaps constructively impact on the privacy engineering of software systems.

Figure 6. An EBNF grammar for privacy awareness requirement statement

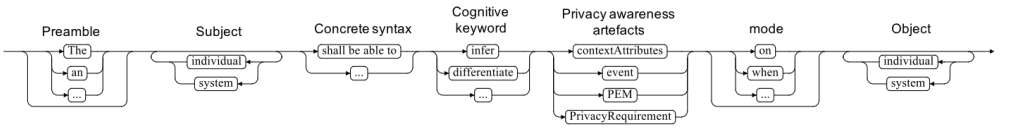
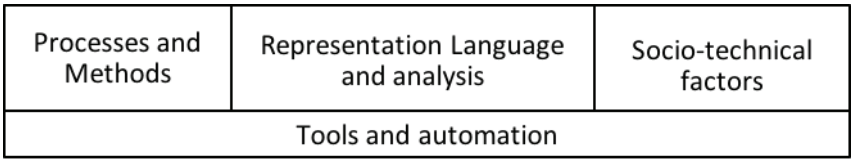


Figure 7. Research challenges for systematic engineering of privacy awareness

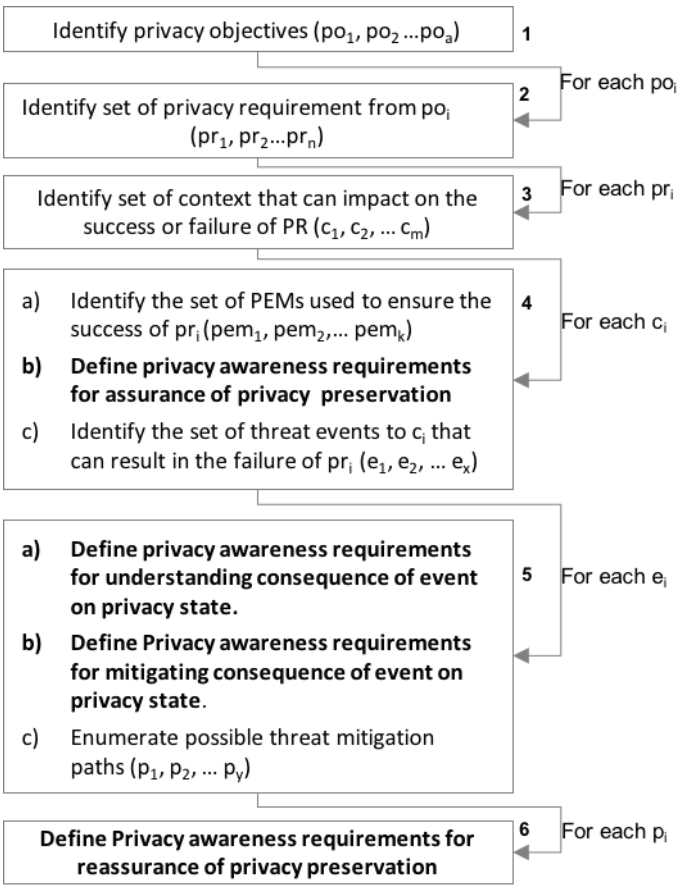


4.1. Processes and Methods

Privacy awareness is secondary as it exists as a result of the need to satisfy an individual's privacy objective already expressed in a privacy requirement. Thus, it is unlikely that users of systems can directly understand what their privacy awareness requirements are until they express a privacy objective. There already exist a number of methods that systematically helps in the identification of these privacy objectives and associated privacy requirements to achieve them (Kalloniatis, at.al., 2008; He & Antón, 2003; Bijwe & Mead, 2010). Thus, the open research issue is to investigate a process for the identification of privacy awareness requirements from privacy requirements. Figure 8 illustrates our initial 6 steps process framework for identifying privacy awareness requirements compactible with the four privacy awareness needs we have identified so far (section 3.1).

The identification of privacy objectives and subsequent associated privacy requirements in step 1 and 2 can leverage on existing solutions such as SQUARE for privacy (Bijwe & Mead, 2010) and the PriS method (Kalloniatis, et.al., 2008). These methods are not fully adaptable to initiating subsequent steps 3-6 as they are not optimised for further identifying the privacy awareness needed for defined privacy requirements. The research challenge is investigating a solution for which given a privacy requirement, representation and modelling of privacy awareness artefacts necessary to fulfil the privacy requirement is possible. Furthermore, the privacy awareness requirements output from steps 4-6 varies depending on context and the mitigation choice that has been taken, this suggest

Figure 8. A process framework for identification of privacy awareness requirements



research insight on a process that is amiable to capturing the dynamic variability of privacy awareness requirements depending on context and mitigation options.

The broader implications for achieving proposed framework is yet to be known. Using empirical studies and industry surveys, we will need to understand the overheads associated with the mapping of user privacy objectives with required awareness needs. We expect that certain approaches will be more effective or cumbersome compared to others. Also, such study will should provide some further insight on the nature of relationship between awareness and privacy. For example, the multiplicities, symmetric and transitive properties that are shared between awareness and privacy. Finally, the nature of awareness needs before, during or after the occurrence of an event may have resultant impact on the process framework. For example, considering the consequence of events at runtime on privacy during design time will require the investigation of appropriate context models, and a clearer understanding of the domain.

4.2. Representation Language and Analysis Techniques

We have demonstrated privacy awareness requirements using structured textual natural language in EBNF meta-syntax. There are other representation techniques such as use case based mechanisms (Jacobson, 1992), goal oriented models (Lamsweerde & Letier, 2000) problem frames (Jackson, 2000), and formal techniques (Fraser, et.al., 1991). Indeed, some of these techniques have already been applied to privacy requirement elicitation (Kalloniatis, et.al.,2008; Mancini, et.al., 2009; Mouratidis, et.al., 2003; Breaux, et. al., 2008; Breaux, et.al., 2006). While these techniques have demonstrated some form of support for the validation and verification of general requirements, they are still open research issues on their suitability for expressing and subsequent validation and verification of privacy awareness.

There are additional issues that need to be addressed beyond those handled during conventional verification and validation of general functional requirements. We need to be able to answer verification questions such as: does the system within the selected context, correctly satisfy a privacy awareness requirement; are the privacy awareness requirement statements consistent with one another; are identified PEM sufficient to satisfy a privacy requirement given known events. Typical validation questions include: are our assumptions about a selected context and events correct; is any undiscovered context attribute or event essential to capture a privacy awareness requirement missing; does the privacy awareness model capture the problem of privacy awareness within the specified context; did we discover all important privacy awareness requirements. Addressing issues necessitates firstly, runtime monitoring and adaptation; and secondly, the need for formal logical analysis to reason about the modal properties of privacy awareness. Reasoning outcome can differ based on the agents (single or group of agents) that characterise a privacy awareness requirement.

4.2.1. Runtime Monitoring and Adaptation

We have used cognitive keywords to describe testable properties of privacy awareness. These properties can be monitored at runtime to determine if an identified privacy awareness requirement is being satisfied or not. Performance monitoring approach differs depending on the agent involved. The monitoring of systems can be achieved by the use of appropriate sensors and actuators. The monitoring of individuals or groups is more subtle, as it is impossible to compel an individual to initiate an event, and the best that can be done is to issue an instruction to be followed (Jackson, 2000). The use of cognitive keywords helps indicate explicitly what a system, an individual or group must do in order to demonstrate privacy awareness.

On the whole, we need to understand how to monitor awareness of different agents based on cognitive insights and amidst a host of controllable and uncontrollable environmental factors. Depending on the outcome of monitoring, there might also be need to adapt our privacy awareness needs. Achieving such adaptation will potentially need some insight on utilisation of autonomic managers (Salehie & Tahvildari, 2009) in the management of privacy awareness amongst agents. A

general understanding of the effectiveness and efficiency of monitoring privacy awareness at runtime is also required. While monitor-based runtime reflection framework has been applied in development of reliable systems (Leucker & Schallhart, 2009), the uniquely subjective properties of privacy may require a further investigation for their suitability for privacy awareness requirements. For example, in generic systems, it may be sufficient to design feedback loops as emanating from an application and back to itself. But that may not be suitable for privacy management involving multitude of agents. As the disclosure behaviour of one agent may impact on the privacy of other agents or the group.

4.2.2. Modal Properties of Privacy Awareness

In reasoning about the privacy awareness of a single or a group of agents, we are able to verify if a model of privacy awareness need is well-formed, and if different aspects of the representations are consistent with one another. We can also confirm the properties that are expected to hold for a given privacy awareness requirement. More specifically, formal logical analysis provides an opportunity to reason about the consequence of a privacy awareness requirement for an agent or group of agents, and if such requirement can ever be satisfied. Alternatively, given that an agent has gained some privacy awareness, we need to understand if the privacy objective of the agent is better guaranteed. This view of reasoning about privacy awareness requirement can be studied by using epistemic and temporal modal logic or the logic of knowledge and time (Fagin, et. al., 2003), as a language to express the notion of privacy awareness.

The underlying idea used in epistemic and temporal modal logic is that of *possible worlds* where the actual world is one of the many possible worlds (Herrick, 1999). A world may be considered accessible or inaccessible depending on primitives that the agent is aware. Modal epistemic claims can be used to analyse the possible outcome of a privacy objective when an agent lacks or gains cognition of awareness primitives. Thus, augmenting the possible world approach with the syntactic notion of privacy awareness requirement, we can thus postulate that: if a subject agent does not have complete cognition of all awareness primitives, the agent would consider a number of worlds possible. These possible worlds are the candidate ways for which an agent can perceive that privacy is threatened or violated. For example, using our smart meeting scenario (Case 1) with the following privacy awareness requirement for the assurance of privacy preservation:

φ: An attendee shall be able to differentiate between invited and uninvited attendees in a private technical session.
ψ:An attendee shall be able to infer when a public meeting session changes to a technical private session.

Assuming a smart mobile device is able to establish that an attendee *P* has awareness for φ and is unable to establish the outcome for ψ. Then, a privacy awareness structure *M,* for *P*'s current world *w* is thus:

$$M,w \vDash (A_p\varphi \wedge A_p\neg\psi \wedge \neg A_p\neg\psi)$$

where A_p φ means "P is aware of φ".

Privacy awareness behaviour in M can also be described as a temporal function. Assuming the event e_1 occurs, we can describe that the P is aware of φ at some time after e_1 occurs, and that P is never aware of ψ as thus:

$$M,w \vDash (\Diamond A_p\varphi \wedge \Box(A_p\neg\psi \wedge \neg A_p\neg\psi))$$

where $\Diamond A_p\varphi$ means "P is aware of φ at some point in time".

Using M, different analysis can then be carried out to understand the consequence of an event on the privacy objective of P. This also reaves a broader research question on a representation language that has formal semantics defined in terms of modal logic. Such language should let requirements engineers specify their privacy requirements, methodologically extract the privacy awareness requirements and also provides the flexibility for monitoring privacy awareness.

It is also useful for us to understand how group of agents can impact on achieving a privacy awareness need. This is so as perhaps most of our daily activities are carried out within formal groups such as the family and work group in the office, or informal groups such as friends, crowd, a queue at the bus stop, or a group of pedestrians on the walkway (Forsyth, 2014). Also, as demonstrated by Nippert-Eng (2010), an agent's privacy objective can turn out to be constrained, guided and sustained by other agents it interacts with within its associated groups.

In reasoning about privacy awareness of single agents, the interest is on understanding the privacy awareness gained by the agent in order to achieve a privacy objective. Assuming the agent exists is in a group, we then need to take into account not only its established awareness about the world, but also the awareness of other agents in the group (Ch. Meyer & van der Hoek, 2004; Herrick, 1999). As stated by Fagin et.al. (2003), "a society certainly wants all drivers to know that a red light means "stop" and a green light means "go." Suppose we assume that every driver in the society knows this fact and follows the rules. Will a driver then feel safe? The answer is no, unless she also knows that everyone else knows and is following the rules. For otherwise, a driver may consider it possible that, although she knows the rules, some other driver does not, and that driver may run a red light".

Again for Case 1, assuming there is another agent *Q* in the session meeting whose mobile device is unable to satisfy φ; then the privacy objective of *P* can be under minded by lack of awareness of *Q*. This is so as *Q* can possibly divulge private information about *P* to an uninvited attendee. In such case, P also needs to be aware if Q has gained awareness for φ. This group notion changes privacy awareness structure *M,* for *P*'s current world *w* is thus:

$$M,w \vDash (A_p\varphi \wedge A_p\neg\psi \wedge \neg A_p\neg\psi \wedge A_pA_Q\neg\varphi \wedge A_pA_Q\neg\varphi)$$

where $A_pA_Q\neg\varphi$ means "P is aware that Q is not aware of φ.

Privacy awareness of agents in a group presents an additional research challenge in understanding a state of common privacy awareness in which 'everyone in the group is aware that everyone is aware'. Privacy awareness can also be distributed. For instance, assuming the presence of an uninvited attendee in a private session meeting, and that P has gained awareness of φ and Q has gained awareness of ψ. Then, P and Q together have distributed privacy awareness of the fact that privacy is threatened by P being aware of the presence of an uninvited attendee, and Q being aware that the current session is a private technical session. Common and distributed awareness are useful tools in helping to understand and analyse privacy awareness situations involving group of agents. Generally, research is required to investigate and mature these notions into a metric for efficacy in privacy awareness. For example, is there some group threshold at which point awareness is contagious with regards to risks to privacy?

Generally, this research challenge can be addressed by investigating a modal deductive framework that analyses the likelihood of privacy violation in a multi-agent setting. Indeed, such framework can be used by software engineers at design time to reason about the satisfaction of privacy requirements at runtime. Such reasoning mechanism then relies on possible worlds semantics and a suite of protocols. Thus, such framework can address questions such as - for a given level of awareness and sequence of protocols for executing an event, what is the likelihood or the extent to which a privacy requirement can be satisfied by agents.

4.3. Socio-Technical Factors

Fundamentally, privacy awareness requirements also represent social and educational challenges that are generated in the use of software systems to coordinate interaction processes. System failures

resulting from privacy violations have been credited to unpredictable change in privacy behaviours of users that compromise their privacy. This unpredictability is evident in the dichotomy that exists in individual's privacy preferences and their actual privacy behaviour (Acquisti & Grossklags, 2005; Chellappa & Sin, (2005). Indeed, Pötzsch, (2009) had suggested that privacy awareness is a means to solve this privacy paradox.

The open research issue is the potentials of using privacy awareness requirements as a means to enhance intelligent social behaviour change of users. This socio-technical dimension of privacy awareness suggests that certain privacy awareness requirements are rather validated against users rather than the system. In other cases, they are validated on how the system helps users in attaining the necessary awareness essential to guard their social behaviour. For instance, using the smart meeting scenario, awareness of mitigating counter events at the approach of an uninvited attendee such as "attendees suspend meeting" or "discussant stops speaking" will require a behavioural change that needs to be effected by the user. On the whole more studies are required to understand the impact of privacy awareness on an individual's social behaviour when using computer devices to coordinate different tasks. We also need to understand computational issues such as how does the identification, representation and analysis of privacy awareness requirements scale; or how many attributes can a person tolerate when managing their own privacy awareness; similarly, when is it beneficial that a software agent acts on behalf of a user given natural human limitations.

5. CONCLUSION AND FURTHER WORK

In this paper, we discussed our vision of enabling privacy awareness in software systems. Our research goals aim to use privacy awareness as a means to achieve privacy assurance, to understand the consequences of threats on privacy, and to manage the mitigation of threats and reassurance of privacy in software systems. We argued and illustrated a novel notion of privacy awareness requirements as part of this systematic approach to considering privacy during the development of software systems.

There are open research issues for the research community to address in this area. These issues cut across methods and processes for identifying privacy awareness requirements, representation languages and analysis mechanisms, and socio-technical factors that impact privacy. We outlined a process framework to guide the investigation of methods and processes to help identify privacy awareness requirements. This led to some key research questions that lie at the heart of software engineering of privacy aware systems. These questions reflect the general need for monitoring and adaptation, together with the need for targeted formal analysis to reason about privacy awareness properties. Finally, we also expect that our focus on privacy awareness can act as a socio-technical bridge between individuals' privacy preferences and their actual privacy behaviour. One consequence of the research issues we have raised may be the need for new techniques for managing privacy awareness.

In this paper we have used simple scenarios only to exemplify privacy awareness. Therefore, there is a need to investigate more substantive and different scenarios. We plan to explore tools and mechanisms that are suitable for enhancing and automating the processes, representation and analysis techniques for the kind of privacy awareness requirements we have discussed in this paper. We also seek to carry out empirical studies better understand the socio-technical characteristics of privacy awareness and the development of novel interaction and user awareness technologies.

REFERENCES

Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy*, *3*(1), 26–33. doi:10.1109/MSP.2005.22

Aker, J., & Mbiti, I. (2010). Mobile Phones and Economic Development in Africa. *The Journal of Economic Perspectives*, *24*(3), 207–232. doi:10.1257/jep.24.3.207

Allen, J., Barnum, S., Ellison, R., McGraw, G., & Mead, N. (2009). *Software Security Engineering*. Addison-Wesley Professional.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *The Journal of Social Issues*, *33*(3), 66–84. doi:10.1111/j.1540-4560.1977.tb01883.x

Anderson, L., Krathwohl, D., Airasian, P., Cruikshank, K., Mayer, R., Pintrich, P., & Wittrock, M. et al. (2000). *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, Abridged Edition*. Allyn & Bacon.

Anderson, R. (2008). *Security engineering*. John Wiley & Sons.

Barth, A., Datta, A., Mitchell, J.C., Nissenbaum, H., (2006). Privacy and Contextual Integrity: Framework and Applications. *Proc of the 2006 IEEE Sym on Security and Privacy* (pp. 184-198).

Bijwe, A. and Mead, N. (2010). Adapting the SQUARE Process for Privacy Requirements Engineering (Technical Note CMU/SEI-2010-TN-022).

Breaux, T., Antón, A., & Doyle, J. (2008). Semantic Parameterization: A Process for Modeling Domain Descriptions. *ACM TOSEM*, *18*(2), 5. doi:10.1145/1416563.1416565

Breaux, T., Vail, M., & Antón, A. (2006) Towards Compliance: Extracting Rights and Obligations to Align Requirements with Regulations.*Proc RE'06*, Minneapolis, Minnesota (pp. 49-58). doi:10.1109/RE.2006.68

Charlton, B. G. (2000). *Evolution and the cognitive neuroscience of awareness, consciousness and language, Psychiatry and the human condition*. Oxford, UK: Radcliffe Medical Press.

Chellappa, K., and Sin, R., (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Inf. Technol. and Mgt*, 2(3), 181-202.

Deleuze, G. (1992). *What Is an Event? the Fold, Leibniz and the Baroque* (T. Conley, Trans.). Uni of Minnesota Press.

Derlega, V., & Chaikin, C. (1977). Privacy and self–disclosure in social relationships. *The Journal of Social Issues*, *33*(3), 102–115. doi:10.1111/j.1540-4560.1977.tb01885.x

Dourish, P., & Bellotti, V. (1992). Awareness and coordination in shared workspaces. *Proc. of the ACM conf on CSCW*, Toronto, 107-114.

Endsley, M. (1993). A survey of situation awareness requirements in air-to-air combat fighters. *The International Journal of Aviation Psychology*, *3*(2), 157–168. doi:10.1207/s15327108ijap0302_5

Fagin, R., Halpern, J., Moses, Y., & Vardi, M. (2003). *Reasoning About Knowledge*. MIT press.

Forsyth, D. (2014). *Group dynamics* (6th ed.). Belmont, CA: Wadsworth, Cengage Learning.

Fraser, M., Kumar, K., & Vaishnavi, K. (1991). Informal and Formal Requirements Specification Languages: Bridging the Gap. *IEEE Transactions on Software Engineering*, *17*(5), 454–466. doi:10.1109/32.90448

Gaver, W., Smith, R. B., & O'Shea, T. (1991). Effective sounds in complex systems: the ARKOLA simulation. *Proc of the SIGCHI: Reaching through tech*, New Orleans, US. doi:10.1145/108844.108857

Guarda, P., & Zannone, N. (2009). Towards the development of privacy-aware systems. *Information and Software Technology*, *51*(2), 337–350. doi:10.1016/j.infsof.2008.04.004

Gutwin, C., & Greenberg, S. (1998). Effects of awareness support on groupware usability. *Proceedings of the SIGCHI conf. on Human factors in comp sys*, LA, US (pp. 511-518).

He, Q., & Antón, A. (2003). *A Framework for Modeling Privacy Requirements in Role Engineering*. Austria: REFSQ.

Herrick, P. (1999). *The Many Worlds of Logic*. Oxford Uni. Press.

Jackson, M. (2000). *Problem Frames: Analyzing and Structuring Software Development Problems*. Boston, MA, USA: Addison-Wesley Longman Pub. Co., Inc.

Jacobson, I. (1992). *Object-Oriented Software Engineering: A Use Case Driven Approach*. Boston, MA: Addison-Wesley.

Jedrzejczyk, L., Price, B., Bandara, A., & Nuseibeh, B. (2010). On the impact of real-time feedback on users' behaviour in mobile location-sharing applications. *Proc. SOUPS*, Redmond, USA doi:10.1145/1837110.1837129

John, K. (2007). *UbiComp 2006 Workshops* (Vol. 6, Part 2, pp. 109-112).

Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2008). Addressing privacy requirements in system design: The PriS method. *Requir. Eng.*, *13*(3), 241–255. doi:10.1007/s00766-008-0067-3

Lahlou, S., Langheinrich, M., & Röcker, C. (2005). Privacy and trust issues with invisible computers. *Communications of the ACM*, *48*(3), 59–60. doi:10.1145/1047671.1047705

Lamsweerde, A., & Letier, L. (2000). Handling Obstacles in Goal-Oriented Requirements Engineering. *IEEE Transactions on Software Engineering*, *26*(10), 978–1005. doi:10.1109/32.879820

Leucker, M., & Schallhart, C. (2009). A brief account of runtime verification. *Journal of Logic and Algebraic Programming*, *78*(5), 293–303. doi:10.1016/j.jlap.2008.08.004

Mancini, C., Thomas, K., Rogers, Y., Price, B., Jedrzejczyk, L., Bandara, A., & Nuseibeh, B. et al. (2009). From spaces to places: emerging contexts in mobile privacy. *Proc* (pp. 1–10). Orlando: UbiComp. doi:10.1145/1620545.1620547

Meyer, J.C., & van der Hoek, W. (2004). *Epistemic Logic for AI and Comp. Sc*. Cambridge Uni. press.

Mouratidis, H., Giorgini, P. and Manson, G. (2003). An Ontology for Modelling Security: The Tropos Approach. In *Knowledge-Based Intelligent Info and Engineering Systems, LNCS* (Vol. 2773, pp. 1387-1394). Springer Berlin.

Mylopoulos, J. (2010). Awareness and Adaptivity Requirements. Proceedings of SEAMS, Cape Town, SA.

Nippert-Eng, C. (2010). *Islands of privacy*. Chicago, London: The University of Chicago Press. doi:10.7208/chicago/9780226584546.001.0001

Omoronyia, I., Ferguson, J., Roper, M., & Wood, M. (2010). A review of awareness in distributed collaborative software engineering. *Software, Practice & Experience*, *40*(12), 1107–1133. doi:10.1002/spe.1005

Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. *Proc. of the SIGCHI conf. on Human fact. in comp sys*, Fl, USA (pp. 129-136).

Pedersen, D. (1999). Model for types of privacy by privacy functions. *Journal of Environmental Psychology*, *19*(4), 397–405. doi:10.1006/jevp.1999.0140

Petronio, S. (2010). Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation? *Journal of Family Theory & Review*, *2*(3), 1756–2589. doi:10.1111/j.1756-2589.2010.00052.x

Pötzsch, S. (2009). In D. Cvrcek et al. (Eds.), *Privacy Awareness: A Means to Solve the Privacy Paradox? The Future of Identity in the Info. Society, IFIP Advances in Inf. and Commun Tech.* (pp. 226–236).

Salehie, M. and Tahvildari, L. (2009). Self-adaptive software: Landscape and research challenges. *ACM Trans. Auton. Adapt. Syst.*, 4(2).

Satyanarayanan, M. (2003). Privacy: The Achilles Heel of Pervasive Computing? *IEEE Per. Comp*, *2*(1), 2–3.

Shin, D. (2010). Ubiquitous Computing Acceptance Model: End user concern about security, privacy and risk. *International Journal of Mobile Communications*, *8*(2), 169–186. doi:10.1504/IJMC.2010.031446

Solove, D. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477. doi:10.2307/40041279

Solove, D. (2008). *Understanding Privacy*. Harvard Uni Press.

Spiekermann, S., & Cranor, L. (2009). Engineering Privacy. *IEEE Transactions on Software Engineering*, *35*(1), 67–82. doi:10.1109/TSE.2008.88

Warren, S., & Brandeis, I. (1890). The Right to Privacy (The Implicit Made Explicit). In *Philophical Dimensions of Privacy: An Anthology* (Ed. F.D. Schoeman) (pp. 193-220). Cambridge, MA: Harvard Law Review.

Williamson, C., & Shneiderman, B. (1992). The dynamic HomeFinder: evaluating dynamic queries in a real-estate information exploration system. *Proc. of the 15th annual int. ACM SIGIR conf. on Research and dev. in info. retrieval*, Copenhagen (pp. 338-346).

Zheng, P., & Ni, L. (2006). *Smart Phone and Next Generation Mobile Computing Morgan Kaufmann*. Elsevier.

ENDNOTES

[1] We note here that our distinction between right and wrong context is rather binary and suggest a clean delineation between desirable and undesirable system behavior. But given the non-functional nature of privacy we also acknowledge there is some likelihood that privacy could be satisfied with some combination of right and wrong representing the current context.

Inah Omoronyia is currently a lecturer (Associate Professor) in software engineering and information security at the University of Glasgow, UK. He obtained his PhD from University of Strathclyde in 2009, where he investigated different awareness models and techniques for enhancing interactions in distributed and collaborative software systems. He previously served as a research fellow both at the Norwegian University of Science and Technology, Trondheim, and The Irish Software Engineering Research Centre, Limerick. His research interest revolves around software engineering, secured information-flows and privacy in connected societies. Inah is a fellow of European Research Consortium for Informatics and Mathematics, and the Higher Education Authority, UK.