Exploring the dimensions of individual privacy concerns in relation to the Internet of Things use situations

Ali Padyab and Anna Ståhlbröst

Ali Padyab is a PhD student at the Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden.
Anna Ståhlbröst is a Professor at the Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden.

Abstract

Purpose – *The integration of internet of things (IoT) devices into daily life introduces challenges for the privacy of their users and those who are affected by these devices. This paper explores the factors that affect individual concerns regarding IoT use and how those factors affect the dynamics of privacy management with the presence of an IoT device.*

Design/methodology/approach – *Four focus groups of individuals and IoT experts were studied to understand the groups' privacy concerns. The authors adopted a qualitative research method based on grounded theory to find relevant dimensions of situational privacy concerns in IoT use situations.*

Findings – *The results revealed that fourteen dimensions of individuals' privacy concerns regarding the IoT are relevant and can be categorized under four key influential factors: collection, IoT device, collected data storage and use of collected data. The authors also analyzed the focus groups using genres of disclosure theory and explored how privacy concerns affect individual privacy management regulations.*

Research limitations/implications – *This paper contributes to how future research can employ genres of disclosure as a theoretical framework to identify situations where privacy violations occur.*

Practical implications – *This study can assist service providers and IoT manufacturers in deriving design principles and decreasing concerns by addressing the information that must be communicated to their users.*

Originality/value – *As opposed to the previous research, which was more inclined to dispositional privacy concerns, this study provides insights into situational privacy concerns when individuals are confronted with the IoT. This study represents the first attempt to investigate the process individuals experience in managing their privacy.*

Keywords *Internet of things, Privacy concern, Genre of disclosure, Individual privacy, Situational privacy concern*

Paper type *Research paper*

1. Introduction

Internet of things (IoT) devices are networks of smart things that enable people and objects to be connected through the internet infrastructure. The increasing availability and diversity of the IoT enable a society in which all members have access to internet services, which are populated by self-configuring, self-managing smart technology anytime and anywhere (Atzori *et al.*, 2010). These devices enable data collection from the surrounding human environment to provide useful services for individuals, such as energy savings, security, home automation, transportation, wellness and many more in the future. Similar to any other technology, the application of the IoT has disadvantages. The collection of data about individuals exposes them to possible violations of privacy, which can make the adoption of IoT devices a challenging task (Dutton, 2014; Gubbi *et al.*, 2013). Perpetual collection of

Received 20 February 2018
Revised 11 May 2018
25 June 2018
Accepted 7 July 2018

This work was funded by the European Commission in the context of the Horizon 2020 project U4IoT (Grant Agreement No. 732078) and the Horizon 2020 project PrivacyFlag (Grant Agreement No. 653426), which are gratefully acknowledged.

people's data enables one to track the actions and behavior of the users and derive sensitive information about individuals, which is not only utilized by the technology itself but also by third parties such as businesses, hackers and governments.

The absence of privacy protection has been shown to be an influencing factor regarding the acceptance and adoption of the IoT (Chow *et al.*, 2015; Hsu and Lin, 2016). Increasingly, many people are becoming vigilant about their interaction with IoT devices, particularly because of recent media coverage about the CIA's program (i.e. Vault7) that turns some IoT-enabled devices into surveillance tools (Coldewey, 2017). This situation is compounded by the fact that the IoT users are not notified when potentially sensitive information is collected, and there is no user interface to specify the privacy preferences for the services (Lee and Kobsa, 2016).

Despite the importance of the developments in the field of the IoT, researchers know little about individuals' thoughts and feelings about privacy in regards to the IoT. The research on privacy concerns from individuals' perspectives of the IoT is limited to privacy concerns from the viewpoint of IoT experts (Virkki and Chen, 2013), coarsely defined contexts (Lee and Kobsa, 2016) or affecting factors that researchers borrow from other research areas such as e-commerce (Kowatsch and Maass, 2012). Compared to e-commerce, where the users have some control over information disclosure, IoT devices unobtrusively collect data. Additionally, previous studies on the IoT have focused on dispositional privacy concerns (Malhotra *et al.*, 2004; Smith *et al.*, 1996). However, there is growing support from recent studies that demonstrate that privacy concerns are also situational and context-specific (Kayhan and Davis, 2016; Li, 2011; Sim *et al.*, 2012). The focus of this research is to understand these situational privacy concerns in the IoT because situational privacy concerns shape an individual's decision of how to behave or regulate to manage their privacy (Glover and Benbasat, 2010). Thus, to maximize the potential of the IoT, it is important to understand the privacy concerns of individuals who are not only users but also non-users (i.e. affected by such devices or "affectees").

The purpose of this study is to explore affectees' and users' perceptions of privacy concerns regarding IoT use situations. A bottom-up approach for IoT policymaking, research and service design allows policymakers and practitioners to account for individual's concerns in relation to their needs (Melis *et al.*, 2016; Shin and Park, 2017). However, individuals' perspectives have been largely absent in the IoT privacy research. Thus, the research questions that guide this study are the following. RQ1: What are the dimensions of situational privacy concerns in the IoT? RQ2: What is the interplay between the dimensions of privacy concerns and an individual's privacy management? To fulfill this goal, we conducted four focus groups (FGs) with 16 individuals. An inductive qualitative analysis was adopted to identify the relevant dimensions of individual privacy concerns particular to the IoT. We applied genres of disclosure (Palen and Dourish, 2003) as an interpretive lens to explore the development of situational privacy concerns in IoT use situations. We posit that this study is the first step to discover the situational privacy concerns in the IoT, which will help future researchers to theorize about privacy threats and individuals' reactions to them. From a practical perspective, this study enables service providers and policymakers to be proactive in mitigating privacy concerns that affect users' decisions and increase users' adoption of IoT services.

The remainder of the paper is arranged as follows. First, an overview of user privacy concerns in the field of the IoT and the research gaps are presented. In Section 3, we introduce the genres of disclosure theory as our theoretical framework. Then, the research process through four FG sessions is described, and the findings of the study are presented. Finally, the contributions and implications of the research findings are discussed.

2. Research background

Privacy is one of the focal points in discussing the IoT because of the volume and granularity of sensor data collected (Howard, 2015). Privacy concerns within the IoT is multifaceted and includes technical, regulatory and social aspects. Various applications of the IoT for end users have been discussed from a technical point of view. Among prevalent usages, health wearables collect a wide range of personal information to help visualize how (in)active a person is in their daily life. Various vulnerabilities within health tracker companies' servers, data tampering vulnerabilities, privacy concerns associated with Bluetooth issues and data integrity in health wearable trackers (Hilts *et al.*, 2016) can lead to location tracking, third-party access to fitness data, selling data to third-parties, demographics collection, device's access to users' sensitive information and vulnerabilities to hackers (Piwek *et al.*, 2016; Troiano, 2017). To alleviate such technical issues, recommendations include adopting https and certificate pinning, on-device encryption and Bluetooth low-energy privacy features (Hilts *et al.*, 2016). Privacy challenges with smart living and smart homes fall within three broad categories: privacy leakage in data sensing, privacy and availability in data storage and processing, and trustworthy and dependable control (Zhang *et al.*, 2017). General privacy requirements for a smart city context include homomorphic encryption, anonymity and access control (ibid.).

Privacy protection in the IoT is barely a technical issue and should be considered in policy implementation (Li *et al.*, 2016). The threats to privacy posed by the IoT industry could be partially alleviated via government involvement. Some authors highlight the role of legislators in being watchful of risks developing in the IoT space and the enforcement of policies and legal frameworks that promote individual rights, trust, ethical behavior, disincentives and penalties for inappropriate behavior, corruption and crime (Berman and Cerf, 2017; Poudel, 2016). However, successful policies surface from a deep understanding of the context they intend to regulate and contributions to policymaking should be developed using a bottom-up framework (Melis *et al.*, 2016). This underlines the social aspects of privacy within the IoT and requires the inclusion of users and affectees in such discussions. In the next section, we will focus on contextual privacy concerns within the IoT from individuals' perspectives and the crucial role of these concerns in developing governance for empowering and enabling the IoT, as motivated by the previous literature (Berman and Cerf, 2017; Dutton, 2014; Hilts *et al.*, 2016; Howard, 2015; Melis *et al.*, 2016; Shin and Park, 2017).

2.1 Individuals' privacy concerns in the internet of things

Before highlighting the relevant literature related to individuals' privacy concerns in the IoT, it is important to differentiate between two types of privacy concerns in general: dispositional and situational privacy concerns. The former has been described in the literature as the static aspects of privacy: people's worries about the opportunistic behaviors of organizations concerning the use of their personal information (Dinev and Hart, 2006a; Malhotra *et al.*, 2004; Smith *et al.*, 1996). This conceptualization of privacy concerns is primarily a dispositional attribute, meaning that it predominantly concerns individual traits. On the other hand, situational privacy concerns account for contextual nuances in which there is information exchange. It is defined as "individuals' worries about the opportunistic behaviors of a specific online service provider concerning the use of their private information" (Kayhan and Davis, 2016, p. 229). The differentiation of dispositional and situational privacy concerns is unequivocal: the former are innate and involve individuals' overall concerns, and the latter are situation-specific conditioned by the context of the information exchange (ibid.).

The constructs related to dispositional privacy concerns are highlighted in various informational privacy literature reviews (Bélanger and Crossler, 2011; Li, 2011; Smith *et al.*,

2011) and include privacy experiences (Belanger *et al.*, 2002), privacy awareness (Malhotra *et al.*, 2004), individual differences (Junglas *et al.*, 2008), social awareness (Dinev and Hart, 2006b), demographic differences (Janda, 2008) and cultural/climate differences (Milberg *et al.*, 2000). Individuals most often have a preconception of static privacy concerns, which are formed before disclosing information. However, static factors do not reflect the situation-specific facets of the process individuals follow while disclosing their personal information (Kayhan and Davis, 2016; Sim, 2010). For example, situational privacy concerns help us to explain why an individual, with a certain level of dispositional privacy concerns, may discriminate between two IoT use situations based on the specific context of each situation (Lee and Kobsa, 2016). Prior research has shown that online users' stated privacy preferences are not consistent with their actual disclosure behavior (Acquisti and Gross, 2006; Berendt *et al.*, 2005), and situational privacy is considered to fill this gap (Sim, 2010).

There have been attempts to apply the existing (dispositional) privacy concern measures in information systems (IS) to the IoT field. Kowatsch and Maass (2012) applied the "extended privacy calculus model" (EPCM) (Dinev and Hart, 2006a) to address critical privacy factors that are relevant to the social acceptance of IoT services. However, EPCM does not appear suitable because the authors assume that users are *willingly* providing information to the IoT device to gain a benefit. There are situations in which individuals are not necessarily users of the IoT device but rather passive objects who are targeted in the data collection of an IoT device, such as FootPath (Schumer, 2011), which is an automated measurement technology that monitors the path of shoppers and visitors in smart retail settings.

In another study, Hsu and Lin (2016) used the "concern for information privacy" (CFIP) (Smith *et al.*, 1996) framework to find the relationship between the CFIP of IoT services and the attitude toward using and the continued intention of using such services. Their results suggest that the CFIP has become an insignificant factor that affects the attitude toward using and users' intentions of using IoT services, although this effect is weak. However, their results contrast with those of Kowatsch and Maass (2012), who could not show that the predictor of privacy concerns against an IoT service had a significant negative effect on the intention to use that IoT service, because of the possible different purposes of the IoT services. These contradicting results suggest that dispositional privacy concerns alone are not sufficient to measure privacy concerns.

Few researchers have studied the situational privacy concerns that could affect individuals' privacy concerns in the IoT from an individual's perspective. Choe *et al.* (2011) surveyed 475 subjects about the places at home where they would not want to be recorded by an in-home sensing system, and the majority (79.7 per cent) of subjects mentioned the bedroom as the most private place. Køien (2011) and Sicari *et al.* (2015) argue that human trust in IoT devices and services is another contextual factor to handle the risks, threats and opportunities. Another study focused on data collection notification preferences and concluded that people are more likely to want to be notified about data practices that they are uncomfortable with (Naeini *et al.*, 2017). However, the overall theoretical basis remains notably fragmented, and studies are either limited in regards to privacy-related factors to a coarsely defined context or are not based on user studies.

In summary, the existing dispositional measures (Dinev and Hart, 2006a, 2006b; Smith *et al.*, 1996) are insufficient to capture all relevant dimensions of user concerns in the IoT context. Moreover, recent studies have shown that the privacy challenges are distinct to the functionality of the IoT and are therefore situational (Chow *et al.*, 2015; Ziegeldorf *et al.*, 2014). A user-centric taxonomy for users' situational privacy-related concerns in the IoT remains underdeveloped. Our study aims at filling this knowledge gap. In the following section, we explore the capacity of the "genres of disclosure" theory to articulate how specific contextual factors play a role in forming situational privacy concerns in the IoT.

3. Theoretical basis

The introduction of context specificity allows for researchers to examine the dynamic relationship between privacy concerns and privacy-related behaviors. Prior studies by Chow *et al.* (2015) and Lee and Kobsa (2016) showed that context-specific scenarios in IoT environments affect privacy concerns differently. However, it was still unclear how contextual parameters form privacy concerns. As opposed to dispositional privacy concerns that view privacy as a static form shaped before individuals disclose information, situational privacy concerns are a dynamic process of boundary-regulation in which people optimize their accessibility over the contexts in which that information is presented (Altman, 1975). Palen and Dourish (2003) proposed that this dynamic process is fundamentally dependent on people having control over three boundaries concerning privacy management in the presence of information technology: disclosure, identity and temporality. These are explained as follows.

The disclosure boundary addresses the tension between privacy and publicity. Following Altman's (1975) theory of privacy regulation, Palen and Dourish (2003, p. 131) argue that people determine "what information might be disclosed under what circumstances, albeit with varying degrees of direct control." Living in the social world requires us to disclose public information concerning ourselves, such as our opinions, views and actions. For example, a desire to present oneself via social media to the public while keeping a degree of privacy about certain aspects of self is determined via negotiation of the disclosure boundary. In this regard, the person allows himself to negotiate their privacy in a public space.

The identity boundary implies tension between oneself and others. Within technological settings, our mutual access is mediated by representations through proxies and control over representations of the self can go awry. Thus, the tension within the identity boundary does not refer to the identity of the person disclosing but to the one receiving and how one's actions are interpretable to others. For example, some argue that people's actions in public spaces (e.g. via security cameras) are already public and thus offer no threat to individual privacy. They fail to consider that we have very little control over representations of ourselves to the information receivers.

The temporal boundaries occur and form tensions between the past, present and future. Our present actions may have impacts in the future; thus, the decision-making process concerning whether to disclose something is regarded in the context of actions taken in the past and their possible effects in the future. For example, some services use positioning sensors, but recording locations via services over the long run activate the temporal negotiation of the past and the future in immediate circumstances and for potential future use situations.

All these boundaries are dynamically negotiated internally and with each other, which can be best described by Palen and Dourish (2003) as *genres of disclosure*, meaning "socially constructed patterns of privacy management." Further, they (p. 6) characterize a genre of disclosure as "the relationship between *forms of disclosure* and *expectations of appropriate use*." Upon the moment of disclosure, e.g. in an IoT use situation, an individual must be able to find a balance between tensions within a boundary and their effects on other boundaries. The IoT can have many impacts by way of spanning boundaries, disrupting them, establishing new ones, etc. Various practices can potentially affect an individual's privacy in certain situations, such as when citizens are occasionally targeted for surveillance via smart devices (Padyab, 2014). We draw upon this theoretical framework to uncover underlying relationships between contextual factors and the development of situational privacy concerns in IoT use situations.

4. Methodology

We used exploratory FGs with qualitative data gathering to find the relevant privacy concerns regarding the IoT. FGs are used for exploratory purposes (i.e. to address "what is" the state of some IS phenomena) to scrutinize the subjects that emerge from the "discussion" and allow for the concepts that were initially unclear to participants to become clearer (Belanger, 2012). An FG is a stimulating milieu for developing awareness through interaction and sharing experiences with each other or, in other terms, "synergistic effects" of focused interactions, which can provide more significant insights than the sum of individual interviews (Morgan, 1996). The participants can follow-up on one another and explain themselves in terms of perceived privacy violations. This process allows for researchers to gain in-depth insights that cannot be sufficiently obtained in one-on-one interviews, such as expressing sensitive topics because group discussions can facilitate the less inhibited members of the group to break the ice for the shyer participants by providing mutual support (Kitzinger, 1995).

4.1 Data collection

We relied on the guidelines of Morgan (1996) regarding the number of groups and group size. To recruit participants, first, an announcement was made on our university's website, which was visible to the public. Sweden is a highly developed country, and IoT devices are widely used in cities, buildings and homes. Therefore, every individual is engaged in IoT activities and is a decision-maker regarding his or her privacy. Thus, these individuals served as experts in our FGs. All people who signed up for the study were invited. To foster a fruitful discussion, homogeneity needs to exist in terms of background but not attitudes (Barbour, 2008). Three participants were experts and had a minimum of 10 years of experience in the design, development and implementation of IoT-based services. Therefore, we created three sessions with non-experts with three, four and six people in each session and a separate session that included the three experts. We found the sample size to be appropriate according to the guidelines of Morgan (1996) and Boddy (2016).

The demographics of the participants were a mixture regarding occupation (10 students, 3 + 3 employed people), gender (11 males, 5 females), cultural backgrounds (11 Swedish, 5 non-Swedish) and age (21-41 years). The average duration of each FG interview was 120 minutes and was conducted during March 2017. A balanced panel minimized the bias imposed by a specific demographic, and the selected panel was representative of a wider group (Morgan, 1996).

4.2 Focus groups procedure

To stimulate the discussion in the group, the concept of genres of disclosure was used to guide the design of the FGs. Genres of disclosure account for situations of potential privacy violations in which there is a disharmony "between forms of disclosure and expectations of use" (Palen and Dourish, 2003, p. 6). The perception of privacy concerns in the IoT is situations that may lead to a privacy violation, and these are the situations that may lead to the unexpected use of personal information. The design of the interview guide focused on a way to motivate participants to discuss the situations where his or her personal information could be used in a privacy-violating way. We had a semi-structured interview guide to minimize the moderator's role in controlling the group dynamics, which allowed for flexibility in exploring new and unexpected ideas (Fern, 1982). The first author was the moderator in all four sessions. The moderator encouraged the participants to talk about their awareness of IoT devices, how they felt about having their information collected and to explain the situations that they fear may result in a violation of their privacy.

In the beginning of the FGs, the participants were familiarized with the idea of the IoT. As privacy is related to personal information, the discussions were limited to smart devices for

personal use, smart home appliances, internet cameras and audio sensors used in smart city implementations. The participants were free to raise and discuss their experiences related to IoT use situations with minimum influence from the moderator to maintain the credibility of the study, as described by Lincoln and Guba (1985). After a general discussion about their privacy concerns, we presented three real-world scenarios to identify and collect feelings, thoughts and behavioral intentions about the cases presented. We selected those cases based on actors that may gain access to personal information, such as organizations providing services (Dinev and Hart, 2006a), secondary actors including third parties, government agencies and illegal entities (Conger *et al.*, 2013). While private contacts and peers, such as relatives, friends and acquaintances, may gain unwanted access to personal information (Karwatzki *et al.*, 2017), we did not include such actors in our group discussions because private contacts are salient interaction partners in social network sites, and this is seldom the case with the IoT. The scenarios were as follows: First, Cayla, a smart doll with an insecure Bluetooth device embedded in the toy to listen and talk to the child playing with it (BBC, 2017) (example of illegal entities). Second, flaws in the design of some models of Samsung smart TVs that listen to their surroundings and send the voice data to a third party during a requested voice command search (Sarkar, 2017) (example of service provider organization and third parties); and third, news about a person that was convicted of fraud by police who gained access to the guilty person's heart monitor data (Johnson, 2017) (example of government agencies). After each scenario, we asked questions about how they felt about the scenario and discussed how the IoT scenario might affect their own privacy.

4.3 Analysis

The FGs were audio-recorded and transcribed, which resulted in 92 pages of transcription and 54,079 words. The data analysis to answer RQ1 was inductive and inspired by the open, axial and selective data coding techniques of grounded theory (Corbin and Strauss, 2015). For open coding, line-by-line coding resulted in the development of concepts and concept categories that emerged from the data. The concepts were then related to each other to find connections between the categories. This helped to reorganize the categories and find the final core categories and narratives to be formed from the observed relations. Two researchers coded the transcripts independently, and to acquire a shared understanding, all categories were iteratively discussed between the researchers through four discussion sessions, each taking four hours, to ensure the credibility of the findings (Lincoln and Guba, 1985). To ensure transferability, we coded the first three transcripts to derive the core categories (resulted in Table I) and then applied content analysis with a deductive category application to the fourth transcription. This was done for two reasons. First, the categories extracted from the non-experts were confirmed to be consistent with other contexts. Second, the categories showed that at least an initial saturation of concepts was reached and no new concepts emerged from the fourth (experts) FG. Therefore, the amount of gathered data was found to be reasonable (Tong *et al.*, 2007). Data analysis was supported by NVivo10 software to conduct the thematic analysis.

5. Results

The analysis results revealed that the situational privacy concerns in the IoT appeared through dimensions that related to *collection, storage* and *use* of information and the *IoT device*. In the following sections, first, we present an overview of the identified categories along with their codebook definitions (Table I) and, then, describe what roles these dimensions play in making tensions within each boundary of disclosure, identity and temporality (i.e. RQ2).

Table I Dimensions of situational privacy concerns in IoT

Category name	*Category definition*
Collection	
Personally identifiable information	Collection of information from the IoT device that could lead to the identification of the users/affectees
Collector	Concerns regarding who is collecting the information from the IoT device
Persistence collection	Concerns that a device continuously collects information about people and their physical environment
What is collected	Concerns regarding being unaware of what information is collected
IoT device	
Security vulnerabilities	Concerns that vulnerabilities, such as backdoors, in the IoT device let hackers and other third parties gain access to the device
Location of device	Concerns regarding the position of the IoT device, such as in a private physical environment
Trust in IoT manufacturer	Concerns that the manufacturer of the IoT device is honest in announcing the types of information collected and how they are used
Storing collected data	
Duration of storage	Concerns that collected data from the IoT device are stored for a long period
Place of storage	Concerns regarding the place of stored data and which laws apply to it
Aggregation from different sources	Concerns that personal data may be combined with other databases, thus creating a "mosaic effect"
Sharing to third parties	Concerns regarding the sharing of information collected with third parties
Secondary use	
Direct use	Concerns that information will be used directly as collected for secondary purposes beyond their awareness
Indirect use	Concerns that data mining techniques applied to stored data to extract information indirectly about users/affectees beyond their awareness
Out-of-context inferences	Concerns that inferences made about a person are out of context for secondary or profiling purposes

5.1 Disclosure boundary

Regarding the disclosure boundary, the tension is in managing privacy by maintaining a balance between private and public realms. The IoT devices can disrupt this balance by increasing, rather than limiting, accessibility to personal information. The perception that an IoT device is gathering information that is not expected raises a concern of whether the private sphere is intruded. The activities that are exposed to a device are observed outside of awareness and context, which challenges the selective disclosure of information and what actions are filtered, but the IoT device might collect and send everything that is happening:

> I think that I really do not know what they are collecting. (female, FG1)

> I think people are getting more and more concerned about this part of data collection, and that is really a deal breaker for them to know that their smart TV is recording them all the time because why do you need to record my speech all the time? It does not really make sense. (male, FG2)

In this regard, the location of the device is another contextual factor that interferes with the public and private boundaries. The presence of devices in public and private spaces creates problems when participation is not deliberate. The concerns for privacy in various places differ, which is also connected to the type of information collected because there is a higher possibility of a camera collecting more sensitive information in a bedroom than in a public transportation vehicle:

> [At home] that is when you do what you like, but when you're walking the street, they do not know where I am going, but when I am home, that is my home… you want to keep it private, but the acts you do in public are already public. (female, FG1)

The notion of "collector" or "who is collecting" is relevant because the extent of publicness is dependent upon who is collecting. Actions recorded by the police in a public transportation vehicle are appropriate to living publicly for the sake of protecting personal safety. However, the same situation with a different collector that does not justify the reason to collect is considered a privacy violation. The collectors (could be legal or illegal, such as hackers) that are not intended as the receiver of a piece of personal information are undesirable because the willingness to disclose the quantity (i.e. amount) and quality (i.e. how detailed) of information are subject to change:

> Baby cam monitors with small cameras that you put in your baby's bedroom when you are away for a short period, and it is really creepy if someone can look around your house or watch your baby, so I will say avoid anything that is related to baby to be connected to the internet. (male, FG4)

Decisions to disclose something about oneself are partly made based on the immediate situation with a lack of awareness about what can be extracted from what is disclosed. At the time of disclosure, it might be assumed that self-disclosure is only about the exact piece that was revealed; however, in a networked world, and especially within the IoT, the use and inference of disclosure is made possible. In that sense, the purpose of direct and indirect use of information that is beyond an individual's awareness may reveal something more than first-hand disclosure:

> This whole phenomenon, IoT, can make our lives so much better I think in the end, but it is also so scary when you look at where it can lead that someone can keep track of you all the time. (female, FG3)

5.2 Identity boundary

Privacy is a social phenomenon that addresses not only the individual but individuals as members of broader social groups, such as families or professional groups. The case with the talking doll was an example of a violation of privacy, not necessarily to the self but others (i.e. a child), because they are both members of a social group (i.e. family). As expected, all participants found the first scenario very scary, and they felt that bringing a vulnerable IoT device into a private space impacts the privacy of all members of that space. Moreover, such a device can act as a proxy to bypass restrictions that members of that social group have enacted:

> Participant 16: You should ask yourself as parents, do you want strangers to talk to your daughter or son when you are not around [. . .].
>
> Participant 14: Exactly. I would say I would never buy such a thing for my nephews, anything connected to the internet for which is intended to record." (males, FG4)

One interesting finding was that participants were concerned about the "who" questions in different IoT use situations. Palen and Dourish (2003) problematize the tension between oneself and others using the phenomenon of "recipient design," which is defined as "the way that one's actions and utterances are designed with respect to specific others" (p. 4). Managing privacy related to an IoT use situation is overshadowed by the difficulty of distinguishing between different audiences in some situations. First, the collector could be the manufacturer of the device or a service provider that uses a brand's device. Both manufacturer and collector could raise different privacy concerns because an individual might feel safe using a certain service but may not trust the manufacturer of the device because of a bad reputation, or the manufacturer may intentionally or unintentionally collect information that is not a part of the service. Second, the device could have security vulnerabilities that allow access to unintended audiences, such as hackers or government

agencies. Third, if the collected information is stored, collectors, third parties, hackers and governments could access and use it for secondary purposes:

> It is not a comforting thought to have personal data recorded in microphones and things to know that it is not going to people that are trying to do things better; even if it is going to a company that is trying to do things better for you, you never consented to that information. (male, FG1)

Therefore, not having a complete picture regarding who has access at different stages makes the interpretability of self-actions in the eye of others more complex. People adjust their actions, demeanor and information through their strategies to withhold or disclose information based on how it will appear and be interpreted by others. In addition to "who" receives our actions, "what" is conveyed is also relevant. Actors that use collected information for secondary purposes reveal something about the individuals. Considerable information could be made available with the help of data mining techniques for profiling purposes (indirect use), which could be out of context and self-awareness:

> That is like the part for Facebook, for instance. That is an active choice to put my information out, like, I am fine with that if they use it for free advertisements and stuff like that, but things I do not actively give out, that is my concern, feels a bit scary, feels uncomfortable having like insurance companies calling me because they know I lost my teeth. (male, FG3)

Errors could occur because of processing information based on inaccurate algorithms or reveal information to the wrong audience. One case in the fourth FG was interesting. Some advertisements are based on the IP address, and if that IP address is shared in a space (e.g. home through a wireless router), then everyone sharing that space could get each other's targeted advertisement based on past activities. In this case, with respect to the identity boundary, not only is the information communicated to unintended audiences by mistake but incorrect information (because of errors in inferences) could also be communicated as well:

> At home, when browsing the web, suddenly I notice that I started getting a lot of advertisement about clothes, so I asked my wife, have you started browsing for clothes? My wife said yes. So, I mean, as her husband, I learned information about her that she had not given to me intentionally. (male, FG4)

5.3 Temporal boundary

The present decision is a process that is the outcome of actions in the past and expected actions leading into the future. Therefore, the tension is between the past and the future. The most relevant dimension related to temporal boundaries is when the collected information from IoT devices is stored. Participants at some point had doubts about why the collected information needed to be stored unless there was a clear purpose for it. For example, it was deemed acceptable if the police use recordings of CCTV cameras to track criminals in the future, but if it is used for surveillance, the purpose was deemed as unacceptable:

> That is a concern I guess; you know I would not be surprised if you know one we will have a scenario someday when somebody says "no, I am sorry, you are not welcome to the US." Why? Because we have seen your pictures. (male, FG4)

The situation is aggravated by information permanence if people in the future judge what was done before. The IoT diminishes the temporal boundary, as people have a generally low awareness of what is recorded and stored. The consequence is that there is no room for negotiation of the temporal boundary, as participation in the IoT is sometimes passive without direct control of disclosure. In this regard, both recording what was assumed to be ephemeral information or recording something unintentional could lead to unexpected future use:

> The type of food you have in your refrigerator can be used to detect what kind of allergies you have, maybe, the TV shows you watch can also be used for opinions, the way of your political spectrum or something like that; your Fitbit data can be used for your health status [. . .]. (male, FG2)

Contemplating actions are not only about immediate circumstances but also consequences for potential future situations. If information is disclosed with the expectation of appropriate use and individuals have consented, tension is in the future uses of information that cannot be controlled, even if technology that is not available today makes it possible tomorrow to extract something new. This was the case with reflections regarding the third scenario when some participants thought that the intention of using a heart monitoring device is for monitoring health status and not as a lie detector:

> It [third scenario] concerns me because I think it is a use of data in a way that it is not intended. . . the person has likely not thought that these data would ever be used for tracking his actions, but instead only to track his health state. (female, FG3)

In sum, different dimensions of privacy concern in IoT use situations affect the tensions that occur with the negotiation between disclosure, identity and temporal boundaries. Table II presents a summary of each dimension and the tension that is encountered at each boundary regulation.

6. Discussion

The present study contributes to previous research by featuring the key dimensions of situational privacy concerns in the IoT from the perspective of the end users and affected people. The results show that the main concerns in the IoT are privacy concerns regarding the collection of data, IoT devices, collected data storage and use. Analysis through "genres of disclosure" revealed that these situational factors impact the dynamic relationship between situational privacy concerns and privacy management regulations in the presence of IoT devices. A notable finding from the FGs was related to specific factors that originate from IoT-related concerns. Previous studies focused on the static privacy-related constructs from other fields of research (e.g. e-commerce). Taking a step forward, the present study grounded the situational factors from the individuals. Moreover, this study contributes to the literature by expanding its focus on affectees, in addition to IoT users.

Privacy awareness of organizational information privacy practices (Culnan, 1995), such as sharing and selling the collected information, is relevant to IS, and our findings show that trust in information privacy practices is particularly important for IoT manufacturers and service providers. Another important finding, which has been neglected in the previous privacy concerns literature, was the storage of collected information. Ståhlbröst *et al.* (2015) suggested that in audio sensing systems, it is important that no human voice should be stored. The stored data are potentially subject to different violations of privacy in two manners. First, long-term storage exposes the individuals to data mining for profiling in the present and susceptible to retrieval and mining with future data-mining technologies (Atzori *et al.*, 2010). Second, the richness of the collected data allows for the linking of different systems and information sources to reveal personal information more accurately. This phenomenon has been observed in the domain of social media (Padyab *et al.*, 2016), and the IoT is expected to follow this path (Ziegeldorf *et al.*, 2014).

Among all privacy dimensions that have emerged, indirect use of information creates a real challenge for the IoT adoption. Our participants were most worried about the utilization of their information beyond their awareness. This is a relevant topic for future discussion within research, practice and policy, especially after the Facebook/Cambridge Analytica controversy (Wagner, 2018). We argue that there is an urgent need to find ways to alleviate

Table II Situational privacy concerns and their relative tensions in privacy management

	Tensions in each boundary		
	Disclosure boundary	*Identity boundary*	*Temporal boundary*
Privacy concern dimensions	*Private ↔ Public*	*Self ↔ Other*	*Past ↔ Present ↔ Future*
Personally identifiable information	If information is rich enough to reveal something private		
Collector	Limiting accessibility to oneself based on who is collecting	To whom will information be available? Each actor accessing information has different interpretations	
What is collected	Selection of what information is collected: IoT devices collect and send everything that is happening		Some information could have serious consequences in the future
Security vulnerabilities	The boundary shift into public space when more parties are involved – the tension is to limit accessibility	Unintended audiences (hacker and governments) that are not part of the intention to disclose	
Location of device	The IoT is intrusive in places where participation is not deliberate and where information is sensitive		
Trust in IoT manufacturer		Trusted "others" treat information confidentially	
Duration of storage			Long-term storage effects regarding how others interpret current actions in the future
Place of storage		Trust in who is storing the information and whether it is treated confidentially	
Aggregation from different sources	Aggregating from different sources might reveal something new, which might be private	Aggregation from different sources might reveal something about "self" and "others in their social group"	
Sharing to third parties	The boundary shift into the public space when more parties are involved – the tension is to limit accessibility		
Direct use	Lack of awareness about the use of information in an IoT situation	If the intent of the device is not communicated, information disclosed might not be regulated toward specific "others"	The purpose of information use might change in the future
Indirect use	If the use of the IoT leads to revelation of something different than first-hand disclosure	If actual use of the device is not communicated, information disclosed might not be regulated toward specific "others"	Future technologies might make it possible to do something bad to stored data
Out-of-context inferences		Errors in data processing lead to "others" receiving an incomplete overview of the person	Actions done in the past could have consequences for the present, if they are interpreted out of context

such concerns caused by data mining and analytical practices applied to individuals' information collected via IoT devices.

6.1 Implications for research and practice

The research findings offer several implications for IoT research. As opposed to the previous research, which was more inclined to dispositional privacy concerns, our study provides insights into situational privacy concerns when individuals are confronted with the IoT. The theoretical contribution highlights what factors affect situational concerns, which should provide future researchers with the prospect to study privacy-related behavior in an IoT context. Moreover, the genres of disclosure theory revealed the underlying relationship

between these factors in shaping privacy concerns. While situational privacy concerns are gaining more attention in the privacy literature, previous theoretical frameworks focused on causal relationships between the role of technology and situational privacy concerns (Kayhan and Davis, 2016; Sim *et al.*, 2012). However, privacy management is not just about technology but also about people and their conflicting internal requirements (Palen and Dourish, 2003). Genres of disclosure as a theoretical lens can improve our understanding of privacy regulation.

The direct and indirect aspects of information usage affect privacy concerns. Some data are used intact, and some information is extracted via data mining. Therefore, individuals can have a limited understanding of the use of their information to make privacy decisions because data mining can enable information extraction beyond the user's awareness (Gürses *et al.*, 2006; Padyab *et al.*, 2016). Our results show that from an individual's perspective, the IoT technologies spark privacy concerns differently regarding direct and indirect use. Therefore, we propose that future research should address these two different aspects of information use and distinguish between them accordingly.

Our findings also present a number of practical implications that can assist service providers in addressing the information that must be communicated, such as the type of collected data, whether it contains personally identifiable information, who the collector is and consents on the collection via opt-in/opt-out options over storage and use of the information. Additionally, our results indicate that users need to see a balance between the information collected and the service provided. Companies providing IoT services or IoT manufacturers should strive to keep this balance and inform its users about the fairness of information collected.

Regarding the concerns that are related to the IoT device, security breaches such as vulnerabilities and backdoors are influencing factors. This finding appears relevant to recent news about the exploitation of IoT devices by the CIA (Coldewey, 2017), since many current IoT devices are targeted for use in private spaces such as homes (Choe *et al.*, 2011). Therefore, a practical implication for IoT service providers is the effective communication of vulnerabilities to their users and providing update patches as soon as vulnerabilities are detected.

Based on our results, privacy concerns are accelerated by confusion over whether the IoT device manufacturer is the same as the service provider. Although one might trust the device to be safe (i.e. secured), he or she may have doubts about the honesty of the service provider in collecting and using the information and taking necessary precautions to protect the information being accessed by other parties, such as governments and hackers. Therefore, it is important for the service providers to communicate this information to its users clearly. Thus, neutral and trusted third-party endorsements can significantly enhance a user's trust. Communicating trust safeguards to the users, such as compliance with regulations (e.g. EU-GDPR), can greatly decrease their concerns.

The list presented in Table I provides important user-centered concerns that have important implications for privacy policies of IoT services. Policymakers can benefit from this research to ensure that their policies reflect the dimensions of privacy concerns, not just for IoT users but affectees as well. The results suggest that a transparent privacy policy that addresses such concerns paves the path toward fair and transparent institutional privacy.

6.2 Limitations and future research

Future studies can address some of the limitations of this study. First, the intention of this paper was not to provide a stratification of the results based on the demographics, although this factor may be interesting in future research. At this phase, it is not argued that the findings represent thoroughly tested theoretical knowledge. Instead, the findings imply a theoretically interesting proposition and motivation for further research to be complemented

by other methodological means. Second, the "privacy paradox" can be regarded as a limitation because of differences in self-reporting and actual privacy behavior. As the IoT is still an emerging field, it would be beneficial to collect data from a situation where an IoT device is present.

7. Conclusion

A user-centered approach in the IoT is required to understand how to avoid negative individual and social consequences (Shin and Park, 2017), and by involving citizens who express their needs, we can address core challenges. One of the challenges of the IoT is privacy concerns of individuals related to its use situations that can negatively influence the adoption of IoT services. This study explored situational privacy concerns in IoT use situations from the perspectives of users and affectees. Fourteen situational dimensions were found to be relevant and were classified under collection, IoT device, and storage of collected data and use. Additionally, using the genres of disclosure theory, our findings suggest that these dimensions significantly affect the dynamics of privacy management in IoT use situations. At a conceptual level, the IoT creates tensions in making information privacy decisions, which is caused by a lack of proper awareness about the context of IoT use. Users need assistance to manage their privacy through privacy awareness programs, communication of institutional practices, enhancing policies and privacy enhancing tools and technologies. We encourage researchers and practitioners to involve users and affectees in their research and development to ensure that the information privacy needs of individuals are met.

References

Acquisti, A. and Gross, R. (2006), "Imagined communities: awareness, information sharing, and privacy on the Facebook", in Danezis, G. and Golle, P. (Eds), *Privacy Enhancing Technologies*, Springer, Berlin Heidelberg, pp. 36-58.

Altman, I. (1975), *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*, Brooks/Cole Pub. Co., CA.

Atzori, L., Iera, A. and Morabito, G. (2010), "The internet of things: a survey", *Computer Networks*, Vol. 54 No. 15, pp. 2787-2805.

Barbour, R. (2008), *Doing Focus Groups*, Sage Publications, London.

BBC (2017), "German parents told to destroy Cayla dolls over hacking fears", *BBC News*, 17 February, available at: https://tinyurl.com/j3hrwrq (accessed 9 July 2017).

Belanger, F. (2012), "Theorizing in information systems research using focus groups", *Australasian Journal of Information Systems*, Vol. 17 No. 2.

Bélanger, F. and Crossler, R.E. (2011), "Privacy in the digital age: a review of information privacy research in information systems", *MIS Q*, Vol. 35 No. 4, pp. 1017-1042.

Belanger, F., Hiller, J.S. and Smith, W.J. (2002), "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes", *The Journal of Strategic Information Systems*, Vol. 11 Nos 3/4, pp. 245-270.

Berendt, B., Günther, O. and Spiekermann, S. (2005), "Privacy in e-commerce: stated preferences vs: actual behavior", *Communications of the Acm*, Vol. 48 No. 4, pp. 101-106.

Berman, F. and Cerf, V.G. (2017), "Social and ethical behavior in the internet of things", *Communications of the Acm*, Vol. 60 No. 2, pp. 6-7.

Boddy, C.R. (2016), "Sample size for qualitative research", *Qualitative Market Research: An International Journal*, Vol. 19 No. 4, pp. 426-432.

Choe, E.K., Consolvo, S., Jung, J., Harrison, B. and Kientz, J.A. (2011), "Living in a glass house: a survey of private moments in the home", *Proceedings of the 13th International Conference on Ubiquitous Computing*, *ACM*, *New York, NY*, pp. 41-44.

Chow, R., Egelman, S., Kannavara, R., Lee, H., Misra, S. and Wang, E. (2015), "HCI in business: a collaboration with academia in IoT privacy", in Fui-Hoon Nah, F. and Tan, C.H. (Eds), *HCI in Business*, Vol. 9191, Springer International Publishing, Cham, pp. 679-687.

Coldewey, D. (2017), "Names and definitions of leaked CIA hacking tools", TechCrunch, 9 March, available at: http://social.techcrunch.com/2017/03/09/names-and-definitions-of-leaked-cia-hacking-tools/ (accessed 3 April 2017).

Conger, S., Pratt, J.H. and Loch, K.D. (2013), "Personal information privacy and emerging technologies", *Information Systems Journal*, Vol. 23 No. 5, pp. 401-417.

Corbin, J.M. and Strauss, A.L. (2015), *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, 4th ed., SAGE, Los Angeles.

Culnan, M.J. (1995), "Consumer awareness of name removal procedures: implications for direct marketing", *Journal of Direct Marketing*, Vol. 9 No. 2, pp. 10-19.

Dinev, T. and Hart, P. (2006a), "An extended privacy calculus model for E-Commerce Transactions", *Information Systems Research*, Vol. 17 No. 1, pp. 61-80.

Dinev, T. and Hart, P. (2006b), "Internet privacy concerns and social awareness as determinants of intention to transact", *International Journal of Electronic Commerce*, Vol. 10 No. 2, pp. 7-29.

Dutton, W.H. (2014), "Putting things to work: social and policy challenges for the internet of things", *info*, Vol. 16 No. 3, pp. 1-21.

Fern, E.F. (1982), "The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality", *Journal of Marketing Research*, Vol. 19 No. 1, pp. 1-13.

Glover, S. and Benbasat, I. (2010), "A comprehensive model of perceived risk of E-Commerce Transactions", *International Journal of Electronic Commerce*, Vol. 15 No. 2, pp. 47-78.

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013), "Internet of things (IoT): a vision, architectural elements, and future directions", *Future Generation Computer Systems*, Vol. 29 No. 7, pp. 1645-1660.

Gürses, S., Berendt, B. and Santen, T. (2006), "Multilateral security requirements analysis for preserving privacy in ubiquitous environments", presented at the Proceedings of the Workshop on Ubiquitous Knowledge Discovery for Users at ECML/PKDD, *Berlin, Germany*, pp. 51-64.

Hilts, A. Parsons, C. and Knockel, J. (2016), "Every step you fake: a comparative analysis of fitness tracker privacy and security", p. 84.

Howard, P.N. (2015), *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*, Yale University Press, Yale.

Hsu, C.L. and Lin, J.C.C. (2016), "An empirical examination of consumer adoption of internet of things services: network externalities and concern for information privacy perspectives", *Computers in Human Behavior*, Vol. 62, pp. 516-527.

Janda, S. (2008), "Does gender moderate the effect of online concerns on purchase likelihood?", *Journal of Internet Commerce*, Vol. 7 No. 3, pp. 339-358.

Johnson, K. (2017), "Middletown man's electronic heart monitor leads to his arrest", WLWT, 28 January, available at: www.wlwt.com/article/middletown-mans-electronic-heart-monitor-leads-to-his-arrest/8647942 (accessed 30 October 2017).

Junglas, I.A., Johnson, N.A. and Spitzmüller, C. (2008), "Personality traits and concern for privacy: an empirical study in the context of location-based services", *European Journal of Information Systems*, Vol. 17 No. 4, pp. 387-402.

Karwatzki, S., Trenz, M., Tuunainen, V.K. and Veit, D. (2017), "Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 688-715.

Kayhan, V.O. and Davis, C.J. (2016), "Situational privacy concerns and antecedent factors", *Journal of Computer Information Systems*, Vol. 56 No. 3, pp. 228-237.

Kitzinger, J. (1995), "Qualitative research. Introducing focus groups", *BMJ: British Medical Journal*, Vol. 311 No. 7000, pp. 299-302.

Køien, G.M. (2011), "Reflections on trust in devices: an informal survey of human trust in an internet-of-Things Context", *Wireless Personal Communications*, Vol. 61 No. 3, pp. 495-510.

Kowatsch, T. and Maass, W. (2012), "Critical privacy factors of internet of things services: An empirical investigation with domain experts", in Rahman, H., Mesquita, A., Ramos, I. and Pernici, B. (Eds), *Knowledge and Technologies in Innovative Information Systems*, Springer Berlin Heidelberg, Berlin, Heidelberg, Vol. 129, pp. 200-211.

Lee, H. and Kobsa, A. (2016), "Understanding user privacy in internet of things environments", 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), pp. 407-412.

Li, S., Tryfonas, T. and Li, H. (2016), "The internet of things: a security point of view", *Internet Research*, Vol. 26 No. 2, pp. 337-359.

Li, Y. (2011), "Empirical studies on online information privacy concerns: literature review and an integrative framework", *Communications of the Association for Information Systems*, Vol. 28 No. 1.

Lincoln, Y.S. and Guba, E.G. (1985), *Naturalistic Inquiry*, SAGE Publications, Thousand Oaks, CA.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model", *Information Systems Research*, Vol. 15 No. 4, pp. 336-355.

Melis, A., Prandini, M., Sartori, L. and Callegati, F. (2016), "Public transportation, IoT, trust and urban habits", in Bagnoli, F., Satsiou, A., Stavrakakis, I., Nesi, P., Pacini, G., Welp, Y., Tiropanis, T. and DiFranzo, D. (Eds), *Internet Science*, presented at the INSCI 2016, Springer, Cham, Vol. 9934, pp. 318-325.

Milberg, S.J., Smith, H.J. and Burke, S.J. (2000), "Information privacy: corporate management and national regulation", *Organization Science*, Vol. 11 No. 1, pp. 35-57.

Morgan, D.L. (1996), "Focus groups", *Annual Review of Sociology*, Vol. 22 No. 1, pp. 129-152.

Naeini, P.E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L.F. and Sadeh, N. (2017), "Privacy expectations and preferences in an IoT world", Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), *USENIX Association*, *Santa Clara, CA*, pp. 399-412.

Padyab, A., Päivärinta, T., Ståhlbröst, A. and Bergvall-Kåreborn, B. (2016), "Facebook users attitudes towards secondary use of personal information", *Proceedings of the 37th International Conference on Information Systems (ICIS 2016)*, *Dublin, Ireland*, p. 20.

Padyab, A.M. (2014), "Getting more explicit on genres of disclosure: towards better understanding of privacy in digital age (research in progress)", *Norsk Konferanse for Organisasjoners Bruk Av IT*, Vol. 22, p. 11.

Palen, L. and Dourish, P. (2003), "Unpacking privacy for a networked world", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, *ACM*, *New York, NY*, pp. 129-136.

Piwek, L., Ellis, D.A., Andrews, S. and Joinson, A. (2016), "The rise of consumer health wearables: promises and barriers", *PLOS Medicine*, Vol. 13 No. 2, pp. e1001953.

Poudel, S. (2016), "Internet of things: underlying technologies, interoperability, and threats to privacy and security", *Berkeley Technology Law Journal*, Vol. 31 No. 2, p. 997.

Sarkar, S. (2017), "Samsung confirms its smart TVs listen & transmit everything you speak", Technology Personalized, 21 February, available at: http://techpp.com/2017/02/21/samsung-smart-tv-privacy-vulnerability/ (accessed 30 October 2017).

Schumer, C. (2011), "Letter to Sharon Biggar, chief executive officer, path intelligence ltd", 28 November, available at: https://tinyurl.com/yba5rjvo (accessed 11 July 2017).

Shin, D.-H. and Park, Y.J. (2017), "Understanding the internet of things ecosystem: multi-level analysis of users, society, and ecology", *Digital Policy, Regulation and Governance*, Vol. 19 No. 1, pp. 77-100.

Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. (2015), "Security, privacy and trust in internet of things: the road ahead", *Computer Networks*, Vol. 76, pp. 146-164.

Sim, I. (2010), *Online Information Privacy and Privacy Protective Behavior: How Does Situation Awareness Matter*?, University of WI-Madison, WI-Madison.

Sim, I., Liginlal, D. and Khansa, L. (2012), "Information privacy situation awareness: construct and validation", *Journal of Computer Information Systems*, Vol. 53 No. 1, pp. 57-64.

Smith, H., Milberg, S. and Burke, S. (1996), "Information privacy: measuring individuals' concerns about organizational practices", *Management Information Systems Quarterly*, Vol. 20 No. 2.

Smith, H.J., Dinev, T. and Xu, H. (2011), "Information privacy research: an interdisciplinary review", *MIS Q*, Vol. 35 No. 4, pp. 989-1016.

Ståhlbröst, A., Padyab, A., Sällström, A. and Hollosi, D. (2015), "Design of smart city systems from a privacy perspective", *IADIS International Journal on WWW/Internet*, Vol. 13 No. 1, pp. 1-16.

Tong, A., Sainsbury, P. and Craig, J. (2007), "Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups", *International Journal for Quality in Health Care*, Vol. 19 No. 6, pp. 349-357.

Troiano, A. (2017), "Wearables and personal health data: putting a premium on your privacy", *Brooklyn Law Review*, Vol. 82 No. 4, pp. 1715-1753.

Virkki, J. and Chen, L. (2013), "Personal perspectives: individual privacy in the IOT", *Advances in Internet of Things*, Vol. 3 No. 2, p. 6.

Wagner, K. (2018), "Here's how Facebook allowed Cambridge analytica to get data for 50 million users", Recode, 17 March, available at: www.recode.net/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data (accessed 5 April 2018).

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J. and Shen, X.S. (2017), "Security and privacy in smart city applications: challenges and solutions", *IEEE Communications Magazine*, Vol. 55 No. 1, pp. 122-129.

Ziegeldorf, J.H., Morchon, O.G. and Wehrle, K. (2014), "Privacy in the internet of things: threats and challenges", *Security and Communication Networks*, Vol. 7 No. 12, pp. 2728-2742.

About the authors

Ali Padyab is PhD candidate at Information Systems, Luleå University of Technology, Luleå, Sweden. Ali Padyab is the corresponding author and can be contacted at: ali.padyab@ltu.se

Anna Ståhlbröst is Professor, at Information Systems, Luleå University of Technology, Luleå, Sweden.