Measuring Users' Socio-contextual Attributes for Self-adaptive Privacy Within Cloud-Computing Environments

Angeliki Kitsiou[1(✉)], Eleni Tzortzaki[2], Christos Kalloniatis[1], and Stefanos Gritzalis[3]

[1] Privacy Engineering and Social Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, 81100 Lesvos, GR, Greece
{a.kitsiou,chkallon}@aegean.gr

[2] Information and Communication Systems Security Laboratory, Department of Information and Communication Systems Engineering, University of the Aegean, 83200 Samos, GR, Greece
etzortzaki@aegean.gr

[3] Laboratory of Systems Security, Department of Digital Systems, University of Piraeus, 18532 Piraeus, GR, Greece
sgritz@unipi.gr

Abstract. The examination of users' socio-contextual attributes and their impact on their privacy management is of great importance in order for self-adaptive privacy preserving schemes to be effectively designed within cloud computing environments. However, several ambitious adaptive privacy schemes, presented in previous literature, seem to fail to examine those attributes in depth. To address that, this paper proposes the development of an interdisciplinary measurement scale, embodying validated metrics from both privacy and sociological literature. The scale provides the thoroughly identification of users' social landscape interrelated with their privacy behaviours and its utilization is expected to lay the ground for the developers to meet efficiently both users' social requirements and systems' technical ones, before performing adaptive privacy mechanisms in cloud.

Keywords: Self-adaptive privacy · Social identity · Social capital · Measurement scale · Privacy metrics · Privacy management

1 Introduction

The dominant utilization of cloud computing poses new challenges for both providers and consumers, especially as far as privacy protection is concerned [1]. Despite the fact that several privacy models and data encryption technologies have been used to preserve privacy in the cloud, these - regardless of the selected deployment model - do not support perplexed computing [1, 2]. Due to the several stakeholders' involvement and interactions [3], the personal information gathered, analyzed and distributed is rapidly increasing, making privacy protection hard to be achieved [4]. Furthermore, although cloud providers specify and provide a variety of privacy policies, there is no guarantee that they employ these policies efficiently, while in many cases, it is difficult for users to

S. Gritzalis et al. (Eds.): TrustBus 2020, LNCS 12395, pp. 140–155, 2020.
https://doi.org/10.1007/978-3-030-58986-8_10

implement them by themselves. Either they often do not realize the implications of their privacy settings choices, e.g. within Facebook, or sometimes they voluntarily disclose personal information, since they value more the perceived benefits than the risks deriving from this procedure [5]. Up to this point, it had been acknowledged that privacy policies and technical measures cannot safeguard privacy, when ignoring users' social norms, since privacy is a normative concept, reflecting not only technical, but also social, legal and political notions [6]. Consequently, in parallel with cloud computing evolvement, privacy concept and respective frameworks are also shifting, outlined by several different terms and methodologies, e.g. networked privacy, on line privacy, intellectual privacy, informational privacy, decisional privacy, social privacy, institutional privacy, privacy in context, social network privacy [7–10]. Thus, besides their differences, it is important to note that a large body among them acknowledges that users' socio-technical context, characteristics and relationships are important for privacy examination and protection [11], indicating that privacy is defined multi-dimensionally, both individually and collectively [7]. This contextualized nature of privacy brings it to the forefront the need for a new customized design of privacy preservation schemes within cloud, in a more adaptive way, so as for the respective systems to be usable and to mitigate privacy risks [3, 4, 12]. Towards this, self-adaptive privacy schemes and mechanisms are introduced, aiming to provide integrated user-centric models, based on users' social and technological context [13]. Since cloud providers offer more personalized and context-aware services, there is a growing need to further understand users' socio-contextual factors that influence their privacy management and to redefine the interaction among them and the privacy aware systems [4]. Despite the fact that several ambitious adaptive privacy schemes presented in previous literature *(see Sect. 2)* consider users social attributes and context, these seem to fail to examine them in depth. However, in order for the self-adaptive privacy aware systems to be optimally developed, it is essential to take into account empirical data related to users' socio-contextual attributes within their interacting frameworks in and out of information systems [14]. Gaining more input from users [15] is critical for the provided services, so as to face the question of how they will be protected in an adaptive way, when using personal and context-aware services [4], and how to meet efficiently both users' social requirements [16] and systems' technical ones before performing adaptive privacy mechanisms. Consequently, the manner of adequately capturing these attributes is of major importance.

In order to address that, this paper proposes the development of an interdisciplinary measurement scale, embodying constructs and validated metrics from both privacy and sociological literature, aiming to identify in depth and to categorize users' socio-contextual attributes in order that they are introduced into self-adaptive privacy behavioural research models within cloud. The rest of the paper is organized as follows. Section 2 presents self-adaptive privacy preserving schemes, introduced in previous literature. Section 3 analyzes the need to focus on users' socio-contextual attributes, based on social identity and capital constructs, since these have been indicated to impact on users' privacy management and reflect efficiently users' social landscape. Section 4, after analyzing previous privacy validated measures, presents the constructs and metrics that our scale includes. Finally, Sect. 5 concludes our work.

2 Self-adaptive Privacy Preserving Schemes

Users' privacy safeguards within several applications are not adequately underpinned due to static privacy settings that do not fulfill their complex privacy needs in different situations and contexts [6]. Up to this, the necessity for the deployment of dynamic self-adaptation privacy processes is indicated, as a more proper way to support users' needs during their interactions within the systems [17]. To achieve that, according to [14], classified interaction strategies should be applied, which facilitate the connection among users and systems during three stages: a) privacy awareness, b) justification & privacy decision, c) control capabilities. In these stages, the inclusion of users' cognitive processes is crucial, so that preferences can be expressed and privacy settings employed in an adjusting way. Additionally, [18] supports that systems should enable users to select the information disclosure level, by providing the context and the control level over this information, indicating four operations to be performed. These concern monitoring, analysis, design and implementation, which should utilize not only frameworks that identify user's roles and interconnections, but also research behavioral models that indicate privacy threats and calculate users' benefits contrary to information disclosure cost. Thereby, an effective adaptive privacy scheme should provide the proper privacy features [12], capturing users'specific elements based on indicative behavioral models for their privacy management.

Towards this, adaptive solutions under the differential privacy scheme have been suggested from both theoretical and application perspectives [12, 19]. However, they are subsequent to many limitations, satisfying only specific criteria, such as: anonymity [20, 21], systems' access control architecture [22], noise insertion [19], sensitive ratings based on social recommendation [23] or streams data aggregation in real time [2]. So, several challenges cannot be addressed, since only static data were considered and the metrics used were proper only for static data as well. Most of them did not consider real-time aggregated data with high accuracy. The proposed algorithms were only optimally accurate, as it was difficult to have them applied to non-linear queries. Anonymity could not be applied in cases where users willingly disclosed information. Others solutions focused particularly on context-adaptive privacy schemes and mechanisms in order to provide the proper privacy-preserving recommendation and automatization [17]. Previous works put emphasis on users' perceived privacy within smart environments, exploring the grade of their awareness [24], investigate users' personal privacy risks contrary to their disclosure benefits within pervasive scenarios [25], examine the interrelation between privacy and context [26]. In [12] authors explored the interactions among users and their environments, based on users' requests for providing a balanced privacy protection scheme. However, these works rather focused on a specific element than the context as whole, while they ignored the interrelated users' contextual information in depth. In cases that interrelations were deeper considered, the solutions were based mainly on anonymity, while once again users' social attributes were statically analyzed. Efforts for these challenges to be addressed are described in following. [27] present a calendar for providing users with context-adaptive privacy by detecting present persons and giving schedule visibility according to their privacy preferences. In [28] authors proposed an Adaptive Privacy Policy framework to protect users' pictures within cloud, considering users' social settings, pictures' content and metadata. However, these works, focusing more on

users' control, may provoke information and choice overload, making them more doubtful for their privacy decisions [5]. Furthermore, many works focused on context while exploring the location parameter [29–31]. Thus, despite the fact that location provides context information, it practically concerns only one attribute of a user's specific context [32]. In [33], authors, based on users' (un)awareness during information disclosure, aimed to determine their expected privacy utility deriving from the design of specified privacy objectives. However, the relationship among end-users and software designers is considered only from the designers' viewpoint. Other works examine context in social networks based only on users' friends' history ratings in order to provide recommendations, failing thus to distinguish the sensitive information ratings [23]. The contextual integrity framework in [10], considered to be a promising approach for implementing adaptive privacy mechanisms, supported that different stakeholders should comply with certain privacy principles in sensitive information transfer in each context. Although this has set the ground and put added value on the examination of users' socio-contextual attributes, it stands only for users' unique contexts in order to define their daily privacy experiences [8]. Authors in [5, 34] argued that by using recommender system algorithms, users' privacy preferences could be predicted based on their known characteristics. Consequently the systems may provide automatic smart settings according to users' disclosure behavior. Posing, thus, the question of how users' social characteristics could be measured efficiently, they propose the user-tailored privacy framework to address it. Based on this concept, authors in [35] found in their study on Facebook, that the optimal recommended adaptive privacy methods are different for each specific privacy setting, depending on users' awareness and familiarity with the privacy features. Despite the innovativeness of these last works, it should be noted that they ignore that recommendations themselves maybe untrustworthy, since current literature has shown that privacy leaks may occur, based on users' influence from systems' provisions [23]. Additionally, they do not consider users' off line attributes that may affect their privacy behaviors. In general, previous works examine fragmentally users' socio-contextual attributes. They focalize separately either on space or time, or on static social information, provided only within the systems, overlooking users'attributes beyond them, which may also be important for implanting privacy settings. Additionally, they are not flexible enough to execute proper privacy analysis that considers both users' social interactions and users and systems' interactions as well. Therefore, the main question posed is how to capture efficiently users' social attributes in and out of informational systems that affect their privacy management, in order to develop the proper behavioral models, which will enable an optimal design for self-adaptive privacy preserving schemes.

3 Exploring Users' Socio-contextual Attributes

Since cloud services are provided in a more personalized and context-aware way, the need to further understand users' differences in privacy management is indicated [4]. Within context-privacy approaches, and in our opinion beyond them, the definition of privacy is grounded on users' relationships, actors' actions, information and context, while this definition may vary across contexts [11]. Users' privacy notions and decisions are determined by specific actions in specific contexts, such as, the sensitivity in which

decisions are made, the input from other users' decisions, the default privacy settings and the available options among them [34]. Despite these acknowledgements, the limited understanding on users' socio-contextual attributes that should be analyzed at runtime for self-adaptive privacy schemes has also been highlighted [3, 15].

Most of the current approaches do not consider users' semantic context information [29] and therefore in order to move beyond a fragment exploration of users' social attributes, a more user-distinct approach is needed. This should reflect both users' social contexts (e.g. family, employment, hobbies) and technological contexts (e.g. services, platforms, settings) [8], as well as their contextual changes [3], which impact on their social and technical privacy norms. As [34] support a critical step, in order to provide adequate self-adaptive privacy, is to determine its privacy calculus. The examination of how information disclosure is across users and how context-dependent it is will provide a deeper insight on the privacy risks and the social benefits that users consider during information disclosure, on the ways they value these and on how they are affected by systems' settings and provisions. In this regard, in order to determine users' social and privacy needs, previous literature has highlighted the importance of social capital theory [36, 37] and the identity theories (e.g. digital identity, personal identity) [38, 39]. With reference to social networks sites (SNS), as the most widespread cloud-computing environment, it has been shown that self-disclosure is a prerequisite, so as users to access information resources and gain social capital benefits within these, which are determined by shared values, common codes of communication and common decision criteria [40]. Thus, this exchanging procedure between social capital benefits and information disclosure leads to many privacy circumventions [37]. Although this is a recognized finding among researchers, still the perplexed relation between social capital and privacy management has not been examined efficiently [7, 37], due to piecemeal users' social capital investigation, which is taking place without considering users' specific context both online and offline. Networks' shared values and common practices, indicating users' social capital also reflect their social context and identity [41]. Up to this, previous literature has shown that, even though privacy management varies substantially among users, specific subgroups with similar privacy behaviours can be identified when their demographics or other shared attributes are mapped [5]. In this regard, some interesting works that explore users' social attributes in order to achieve self-adaptive privacy deployment within SNS have been elaborated [42, 43]. However, these works ignore that users are defined by multiple social identities, as social identity theory supports [44], which respectively differentiate their behaviours in each specific context, while users' attributes were narrowed to these that were presented within SNS. Consequently, in order to address the question of how to capture efficiently users' socio-contextual attributes in and out of informational systems that affect their privacy management, we argue that we should take input from both sociological and privacy literature, providing an interdisciplinary approach based on metrics from both disciplines. The first step for this exploration is to focus on the measurement of users' social identity and social capital in combination, since they are reinforced concepts and they are both indicated by previous privacy literature as significant parameters that affect privacy management,. Social identity refers to individuals' categorization in social groups, such as nations or organizations, indicating a category prototype. This prototype is defined by a set of attributes, which are intertwined, showing

both similarities within the group and differences between the group and other groups. Prototypes also highlight the ways individuals are supposed to express their attitudes and to behave as category members. Additionally, they are typically not distinctive and tend to be shared, in and out of the groups, describing groups and identities, leading respectively to the determination of different groups' attitudes and group memberships [45]. However, individuals may belong to more than one category prototype and therefore they formulate multiple identities, resulting in several conflicts. In order to further understand their behaviours under this multiplicity, a social identity taxonomy is suggested in [44], as follows: a) *person-based social identities*, indicating individual's incorporation of the group attributes as a part of their self-concept figuration, b) *relational social identities*, reflecting individual's self under interactions with other group members within a specific context, c) *group-based social identities*, indicating the categories in which an individual belongs and d) *collective identities*, reflecting individual's self, based on group membership that differentiates them from the others.

Thereby, we support that the measurement of users' social identity based on this taxonomy and the interpretation of their social identity individual and collective processes will specify the attributes (e.g. the groups they belong, their leisure activities) that eventually define their privacy norms and influence their privacy management within a specific context. Previous literature has already shown that many privacy leaks derive from users' inadequate management of their multiple identities [38]. Additionally, as we pointed out before, this exploration should come along with users' social capital measurement simultaneously. Through this interrelated measurement, we will be able not only to define users' social norms, but also to capture the advantages that users consider they will gain by disclosing information, since social capital has been shown to be one of the major factors that affects the balance among users' social interactions and privacy needs [37]. Finally, we consider that the second step, for this interdisciplinary exploration to be achieved, should be the utilization of privacy metrics indicated by previous literature. In this regard, in the next section, the development of our interdisciplinary measurement scale is presented, aiming to provide a more holistic interpretation of users' privacy management, which may be useful in the developing of self-adaptive privacy aware systems.

4 An Interdisciplinary Scale for Self-adaptive Privacy

4.1 Previous Privacy Management Metrics

Privacy, as a multifaceted concept, has very often descriptive and measurable interactive functions within a society [9]. Hence, several measurement scales have been developed to examine users' privacy management issues [46, 47]. Thus, plenty of them do not include different socio-technical parameters that impact on users' privacy management, meeting privacy as one-bivariate construct. Additionally, they are usually not appropriately validated [4, 48]. In this regard, we moved on the examination among the existed validated privacy measurement scales, those of which consider even loosely users' personal and socio-contextual factors on privacy management.

One of the most used validated privacy scale in previous literature, was the Concern for Information Privacy scale, developed by [49], which focuses on users' privacy concerns in more detail. This identified four dimensions of privacy concerns, namely the collection, errors, secondary use, and unauthorized access to information. Emphasizing also on privacy concerns construct, authors in [50] introduced a scale to examine control, awareness and collection of users' personal information, while they adopted measures from other previous works, such as, unauthorized secondary use, improper access, global information privacy concerns and intention to give information. Users' social and contextual attributes that were examined, concerned sex, age, education, internet experience, misrepresentation of identification and privacy victim, while most of them were adapted from [49]. In [51] authors developed a scale, based on the construct of privacy concerns as well, presenting metrics for internet privacy concerns and social awareness. However, this scale does not focus on users' individual social attributes, but mostly on users' awareness regarding social reality. In [52] authors intended to predict users' on line privacy concerns by developing metrics for users' needs for privacy, their self-efficacy, their beliefs in privacy rights and their concerns about general online privacy and organizational privacy, as well their internet fluency and use diversity. However, these metrics ignored users' other significant socio-contextual attributes, besides gender. [48] introduced a new scale, validated on a group of students, which, beyond attitudinal and behavioral privacy concerns items and privacy caution metrics, included technical privacy protection ones as well. Thus, the users' attributes that were considered concerned only gender, age and educational status regarding their technology-based courses or not. In [53], focusing on Internet Privacy Concerns, authors adopted items from [49] and [50] and they provided metrics for the collection, secondary usage, errors, improper access, control and awareness constructs. [47] developed metrics for users' privacy concerns, privacy risks, privacy control, privacy awareness and users'previous privacy experience. In both [47, 53], users' social attributes were equally fragmentary explored, focusing only on demographics such as gender, age and internet usage frequency. An interesting scale was developed by [46], which considered not only users' demographics but also their roles, their common bonds and identity within an organization, presenting metrics for both individual and group privacy management. However, this scale does not consider the peculiarities of each users' context besides the examined organization. More recent works [54] introduced scales regarding collective privacy management within social network sites, focusing thus only on users' groups within social media. Finally, in [4] work, a scale, considering how users' personal data ecosystem, prior experiences and demographic characteristics may impact on their beliefs regarding the benefits and consequences of their adaptive cyber security behavior, was developed. Despite the novelty of this work, including several privacy-related metrics and considering users' individual differences and context, it should be mentioned that it focuses on users' online contexts, while it ignores their groups' privacy norms, studying only individual differences. In general, most of previous works tend to focus on informational privacy concept, while their metrics usually spotlight specific privacy constructs, such as privacy concerns, risks, trust, data collection [48], neglecting users' socio-contextual attributes. Therefore, they do not provide a more socio-technical perspective that would enable a further understanding of the relations among users' practices and technical data [5]. To our best

knowledge, a measurement scale meeting these issues and focusing on self-adaptive privacy management in particular has not been developed in previous literature. Thereby, our aim is to develop systematic metrics for quantifying users' socio-contextual attributes that could be introduced into self-adaptive privacy behavioural research models within cloud. To address that, taking into consideration that existing privacy scales could benefit from expansion manifold [48], while the combination of the advantages of previous privacy metrics may improve the level of privacy within cloud [2], we present in the following subsection the development of a measurement scale that not only leverages the advantages of previous ones, but also includes metrics from sociological literature, emphasizing on social identity and social capital constructs.

4.2 Scale Development

Social Identity Metrics

As [5] emphatically supports "because privacy behaviors are contextualized, users' actions are based on complex identities that include their culture, world view, life experience, personality, intent, and so on, and they may thus perceive different features as risky and safe". Therefore, in order to further understand users' privacy management, it is important to increase the range of the constructs to be measured, taking input from social identity constructs and metrics. To address that, apart from the user's extended demographic attributes, our scale introduces a number of constructs and metrics, used in [55], in which an online Social Identity Mapping (oSIM) tool was designed to assess the multidimensional and intertwined nature of individuals' social identities. Beyond previous sociological works, which fail to identify the full extent of individuals' social group memberships and to interpret the interrelated nature of their multiple identities, limiting the social identity related information that could be analyzed [56], the oSIM may enable not only the identification of individuals' self-definitional attributes, but also these of their networks, collecting information regarding their relationships within their groups [55]. Even though this issue has been explored in many domains (e.g. work, health services, substance abuse), privacy, and self-adaptive privacy in particular, it does not constitute one of the cases where users' only separate identities or social networks have been fragmentary examined. In this regard, oSIM, compatible with [44] social identity taxonomy, may offer a deep insight on users' identity categories in a range of different life contexts, since it is based on previous scales that could be used at the same time. Based on this, in our measurement scale, the following constructs and their respective metrics are included, in Table 1, using mostly a 5-Point Likert scale.

Social Capital Metrics

Literature suggests that the more groups within individuals belong to, the more likely they are to have access to resources [55]. Bonding and bridging are two of the basic types of social capital that provide informational resources within online social networks. Bonding social capital concerns the development of coherent ties among individuals within tight networks, experiencing similar situations and exchanging support and trust, such as family or close friends. Bridging social capital refers to the development of connective

Table 1. Social identity constructs and metrics

Constructs	Items
Belonging in groups	Listing users' groups both offline and online, indicating*: a) Demographic: (e.g. American), b) Broad opinion-based: (e.g., feminist), c) Leisure or social: (e.g., theatre group), d) Family or friendship, e) Community: (e.g., belief-based or volunteer), f) Sporting or well-being: (e.g., tennis club, yoga, g) Work or professional: (e.g., marketing team), h) Health related: (e.g. cancer support group), i) other users' indicative groups* [55]
High-contact groups	*Rating of how often individuals interact within each of their offline and online declared group* [55]
Positive groups	*Rating individuals' perceived positivity for each of their offline and online declared group* [55]
Representative groups	*Rating of how representative individuals feel for each of their offline and online declared group* [55]
Supportive groups	*Rating of how much support individuals receive from each of their offline and online declared group* [55]
Identity importance	*a) Overall, my group membership [group inserted] has very little to do with how I feel about myself, b) The group [insertion] I belong to is an important reflection of who I am, c) The group [insertion] I belong to is unimportant to my sense of what kind of a person I am, d) In general, belonging to this group [insertion] is an important part of my self-image* [57]
Identity harmony	3 pairwise items: **1**. *a) Membership in one group [group inserted] has a very harmful or conflictual effect on the other[group inserted] & b) Membership in one group [group inserted] has a very facilitative or helpful effect on the other[group inserted].* ***2.*** *a) Membership in one group [group inserted] always takes up so much time and energy that it makes it hard to fulfill the expectations of the other group [group inserted] & b) Membership in one group [group inserted] always frees up time and energy for me to fulfill the expectations of the other group [group inserted].* ***3.*** *a) This group [group inserted] always expect conflicting behaviors from me & b) This group [group inserted] always expect the same behaviors from me"* [57]

ties among individuals within vulnerable, heterogeneous and diverse networks, experiencing different situations, without a common sense of belonging [40]. These types also were indicated that influence users' privacy management [37]. As a result, these constructs are included in our scale, using a 5-Point Likert system, incorporating the metrics derived from [58], as the most used and validated scales in previous privacy research (Table 2).

Table 2. Social capital constructs and metrics

Constructs	Items
Bonding social capital	*a) If I urgently needed 100€ someone from online social network (OSN) could lend me, b) People from my OSN could provide good job references for me, c) I do not know anyone well enough to get him/her to do anything important, d) When I feel lonely there are several people on my OSN I could talk to, e) There are several people on my OSN I trust to solve my problems and f) I do not know anyone well enough from my OSN to get him/her to do anything important* [58]
Bridging social capital	*a) Interacting with people in my OSN makes me want to try new things, b) I am willing to spend time on supporting community activities, c) I meet new people very often, d) Interacting with people in my OSN makes me want to try new things, e) Interacting with people in my OSN makes me feel like a part of a larger community" and f) "Interacting with people in my OSN makes me realize that somehow we are all connected worldwide"*[58]

Privacy Management Related Metrics

Based on previous privacy measurements, analyzed in Subsect. 4.1, the following privacy-related constructs and metrics will be included in our scale, using a 5-Point Likert scale *(strongly disagree-strongly agree)* (Table 3).

Our interdisciplinary measurement scale, while adopting constructs and their respective metrics from sociological and privacy literature, aims to provide multiple information about individuals' social landscape as they experience it, allowing a coherent interrelation both with their privacy norms and behaviours. All social media platforms and the majority of webservices nowadays are based on CCEs. Security and privacy issues in CCEs require specific attention since they bring new types of threats that designers should be aware of when designing respective services [59]. Additionally to the technical security and privacy aspects in CCEs the quantification of the types of users' social identities (e.g. parent, employee, husband), the types of their social groups (e.g. volunteer, feminist, tennis) and the types of their social capital benefits will provide researchers with a further understanding of users' privacy management within CCE, since users' belonging to several identities and groups influences their privacy attitudes and behaviours. Consequently, it will lay the ground for the identification of users' social privacy requirements in CCE, accordingly to their attributes, providing software developers with more concrete guidelines for designing self-adaptive privacy preserving schemes. Its utilization will also enable the developers to support GDPR enforcement, e.g. by providing users the ability to assess the options among their own privacy preferences and the systems' choices, in order for an effective decision-making procedure to be followed that respects subjects' data rights and satisfies their needs. Therefore, the development of an instrument such as the proposed scale, which is the first that promotes a self-adaptive privacy behavioural research model within CCE, has potential for both research and design practices in the field of self-adaptive privacy.

Table 3. Privacy management related Constructs and Metrics

Constructs	Items
Beliefs in privacy rights	*a) users' right to be left alone, b) users' right to use Internet anonymously, c) no gathering of disclosed personal information without users' consent and d) users' right control on their personal information* [53]
Privacy concerns	*a) I am concerned about my online information being linked to my publicly available offline one, b) I am concerned that the information I submit on Cloud Services (CS) could be misused, c) I'm concerned that too much personal information is collected by so many CS, d) It usually concerns me when I am asked to provide personal information on CS, e) I am concerned that others can find private information about me online, f) I am concerned about providing personal information on CS, because it could be used in a way I did not foresee.* [4, 47]
Information collection	*a) It usually bothers me when CS ask me for personal information, b) When CS ask me for personal information, I sometimes think twice before providing it and c) It bothers me to give personal information to so many CS* [49, 50]
Self-disclosure	*a) I frequently talk about myself online, b) I often discuss my feelings about myself online, c) I usually write about myself extensively online, d) I often express my personal beliefs and opinions online, e) I disclose my close relationships online and f) I often disclose my concerns and fears online* [54]
Trusting beliefs	*a) CS would be trustworthy in information handling, b) CS fulfill promises related to the information provided by me c) I trust that CS would keep my best interests in mind when dealing with my provided information* [50]
Privacy control	a*) I have control over who can get access to my personal information online, b) I always optimize my privacy settings when I create an online profile, c) I consider the privacy policy of CS where I give out personal information, d) I would opt out of a service due to privacy issues, e) I only upload information online that is suitable for everyone that can see* [4, 46, 47, 54]

(*continued*)

Table 3. (*continued*)

Constructs	Items
Privacy awareness	*a) Personal information is of value to CS providers, b) I am aware of the privacy issues and practices in CS, c) CS providers do not have the right to sell users personal information, d) I follow the developments about privacy issues and violations within cloud, e) I keep myself updated on privacy solutions that law and CS employ and f) I am aware of protecting my personal information from unauthorized access* [4, 47]
Collaborative privacy management	*a) Prior to disclosing content, my group members (group inserted) and I discuss the appropriate privacy settings, b) I ask for approval before disclosing content from those group members involved (group inserted), c) My group members (group insert-ed) ask for approval before uploading content concerning myself* [55]
Self-disclosure cost–benefit	a*) The risk posed to me if personal information is exposed outweighs the benefits of sharing it, b) In general, my need to obtain CS is greater than my concern about privacy, c) I am happy to provide personal information to support government policy and d) I value the personalized CS I received from providing such personal information* [4]

5 Conclusions

The emerge of Self-Adaptive Privacy schemes within CCE has been highlighted, aiming to protect users' privacy according to their social and privacy needs. Although ambitious self-adaptive privacy approaches have been introduced, these fail to capture efficiently users' socio-contextual attributes that influence their privacy management. To address that, we introduced the development of an interdisciplinary systematic metrics for quantifying users' socio-contextual attributes and privacy management, aiming to establish a research instrument, which focuses on the field self-adaptive privacy within cloud environments. Our scale takes input from constructs and metrics, derived from both sociological and privacy literature, enabling a wider exploration of the factors affecting self-adaptive privacy management. Specifically, it concludes seven constructs of social identity theory, namely, belonging in groups, high-contact groups, positive groups, representative groups, supportive groups, identity importance, identity harmony and two constructs of social capital theory, bonding and bridging social capital, since social identity and social capital have been indicated to affect users' privacy management. Contrary to previous privacy literature, the constructs of the two major concepts (social identity-social capital) are not only considered separately but in combination, since they reinforce one another. As far as the included privacy constructs is concerned, while previous privacy literature tends to focus on constructs such as collection, control, authorized use and awareness, our own provides more extensive ones, such beliefs in privacy rights,

self-disclosure, trusting beliefs, collaborative privacy management, self-disclosure cost–benefit, aiming to address all the emerged issues regarding self-adaptive privacy within cloud. In this regard, our scale provides the thoroughly identification of users' social landscape interrelated with their privacy behaviours and its utilization is expected to lay the ground for the developers to meet efficiently both users' social requirements and systems' technical ones, before performing adaptive privacy mechanisms in cloud. Thus, this work as a first step to establish solid empirical structures among the social and technical aspects of privacy. Despite its novelty, since our presented approach is part of our ongoing project on the identification of socio-technical requirements in self adaptive privacy, the validation of the proposed measurement scale is critical towards leveraging knowledge about the respective issues, so that the adequate design of these systems is achieved.

Acknowledgments. This research is co-financed by Greece and the European Union *(European Social Fund- ESF)* through the Operational Programme "Human Resources Development, Education and Lifelong Learning 2014-2020" in the context of the project "Adaptive Privacy-aware Cloud-based Systems: Socio-technical requirements" (MIS:5047231)".

References

1. Cook, A., et al.: Internet of cloud: security and privacy issues. In: Mishra, B.S.P., Das, H, Dehuri, S., Jagadev, A.K. (eds.) Cloud Computing for Optimization: Foundations, Applications, and Challenges, SBD, vol. 39, pp. 271–301. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-73676-1_11
2. Huo, Y., Yong, C., Lu, Y.: Re-ADP: real-time data aggregation with adaptive-event differential privacy for fog computing. Wirel. Commun. Mob. Comput. **2018**(6285719), 1–13 (2018)
3. Salehie, M., Pasquale, L., Omoronyia, I., Nuseibeh, B.: Adaptive security and privacy in smart grids. In: Proceedings of the 1st International Workshop on Software Engineering Challenges for the Smart Grid, Zurich, pp. 46–49. IEEE (2012)
4. Addae, J.H., Brown, M., Sun, X., Radenkovic, M.: Measuring attitude towards personal data for adaptive cybersecurity. Inf. Comput. Secur. **25**(5), 560–579 (2017)
5. Knijnenburg, Bart P.: Privacy in social information access. In: Brusilovsky, Peter, He, Daqing (eds.) Social Information Access. LNCS, vol. 10100, pp. 19–74. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-90092-6_2
6. Nissim, K., Wood, A.: Is privacy? Philos. Trans. R. Soc. A Math. Phys. Eng. Sci. **376**(2128) 20170358 (2018)
7. Kitsiou, A., Tzortzaki, E., Kalloniatis, C., Gritzalis, S.: Towards an integrated socio-technical approach for designing adaptive privacy aware services in cloud computing. In: Benson, V. (ed) Cyber Influence and Cognitive Threats, pp.9–32. Elsevier, Amsterdam (2020)
8. Sujon, Z.: The triumph of social privacy: understanding the privacy logics of sharing behaviors across social media. Int. J. Commun. **12**, 3751–3771 (2018)
9. Chang, C.H.: New technology, new information privacy: social-value-oriented information privacy theory. NTU Law Rev. **10**(1), 127–175 (2015)
10. Nissenbaum, H.: Privacy in Context: Technology, Policy and the Integrity of Social Life. Stanford University Press, California (2009)
11. Martin, K.: Understanding privacy online: development of a social contract approach to privacy. J. Bus. Ethics **137**(3), 551–569 (2016)

12. Pallapa, G., Das, S.K., Di Francesco, M., Aura, T.: Adaptive and context-aware privacy preservation exploiting user interactions in smart environments. Pervasive Mob. Comput. **12**, 232–243 (2014)
13. Belk, M., Fidas, C., Athanasopoulos, E., Pitsillides, A.: Adaptive & personalized privacy & security workshop chairs' welcome and organization. In: Proceedings of 27th Conference on User Modeling, Adaptation and Personalization, Cyprus, pp. 191–192. ACM (2019)
14. Schaub, F., Könings, B., Weber, M.: Context-adaptive privacy: leveraging context awareness to support privacy decision making. IEEE Pervasive Comput. **14**(1), 34–43 (2015)
15. Weyns, D.: Software engineering of self-adaptive systems: an organised tour and future challenges. In: Cha, S., Taylor, R.N., Kang, K. (eds.) Handbook of Software Engineering, pp. 339–443. Springer, Cham (2019)
16. De Wolf, R., Pierson, J.: Researching social privacy on SNS through developing and evaluating alternative privacy technologies. In: Proceedings of the Conference on Computer-Supported Cooperative Work and Social Computing, Texas. ACM (2013)
17. Schaub, F.: Context-adaptive privacy mechanisms. In: Gkoulalas-Divanis, A., Bettini, C. (eds.) Handbook of Mobile Data Privacy, pp. 337–372. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98161-1_13
18. Omoronyia, I.: Reasoning with imprecise privacy preferences. In: Proceedings of the 24th International Symposium on Foundations of Software Engineering, Seattle, USA, pp. 920–923. ACM (2016)
19. Phan, N., Wu, X., Hu, H., Dou, D.: Adaptive laplace mechanism: differential privacy preservation in deep learning. In: Proceedings of the International Conference on Data Mining, New Orleans, pp. 385–394. IEEE USA (2017)
20. Dwork, C.: Differential privacy: a survey of results. In: Agrawal, M., Du, D., Duan, Z., Li, A. (eds.) TAMC 2008. LNCS, vol. 4978, pp. 1–19. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-79228-4_1
21. Hong, J.I., Ng, J.D., Lederer, S., Landay, J.A.: Privacy risk models for designing privacy-sensitive ubiquitous computing systems In: Proceedings of the 5th Conference on Designing Interactive Systems, Cambridge MA, USA, pp. 91–100 2004)
22. Li, C., Miklau, G.: An adaptive mechanism for accurate query answering under differential privacy (2012). arXiv:1202.3807. Accessed 01 Mar 2020
23. Meng, X., et al.: Personalized privacy-preserving social recommendation. In: Proceedings of 32nd AAAI Conference on Artificial Intelligence, Louisiana USA, pp. 3796– 3803. AAAI (2018)
24. Beckwith, R.: Designing for ubiquity: the perception of privacy. IEEE Pervasive Comput. **2**(2), 40–46 (2003)
25. Lederer, S., Hong, J.I., Dey, A., Landay, J.: Personal privacy through understanding and action: five pitfalls for designers. Pers. Ubiquit. Comput. **8**(6), 440–454 (2004)
26. Heiber, T., Marrn, P.: Exploring the relationship between context and privacy. In: Robinson, P., Vogt, H., Wagealla, W. (eds.) Privacy, Security and Trust within the Context of Pervasive Computing, pp. 35–48. Springer, USA (2005). https://doi.org/10.1007/0-387-23462-4_4
27. Schaub, F., Könings, B., Lang, P., Wiedersheim, B., Winkler, C., Weber, M.: PriCal: context-adaptive privacy in ambient calendar displays. In: Proceedings of the International Joint Conference on Pervasive and Ubiquitous Computing, USA, pp. 499–510. ACM (2014)
28. Kumar, R., Naik, M.V.: Adaptive privacy policy prediction system for user-uploaded images on content sharing sites. Int. Res. J. Eng. Technol. **5**(7), 148–154 (2018)
29. Gu, Q., Ni, Q., Meng, X., Yang, Z.: Dynamic social privacy protection based on graph mode partition in complex social network. Pers. Ubiquit. Comput. **23**(3–4), 511–519 (2019)
30. Zhu, J., Kim, K.H., Mohapatra, P., Congdon, P.: An adaptive privacy-preserving scheme for location tracking of a mobile user. In: Proceedings of the International Conference on Sensing, Communications and Networking, USA, pp. 140–148. IEEE (2013)

31. Agir, B., Papaioannou, T.G., Narendula, R., Aberer, K., Hubaux, J.-P.: User-side adaptive protection of location privacy in participatory sensing. GeoInformatica **18**(1), 165–191 (2013). https://doi.org/10.1007/s10707-013-0193-z
32. Vgena, K., Kitsiou, A., Kalloniatis, C., Kavroudakis, D., Gritzalis, S.: Toward addressing location privacy issues: new affiliations with social and location attributes. Future Internet **11**(11), 234 (2019)
33. Omoronyia, I., Etuk, U., Inglis, P.: A privacy awareness system for software design. Int. J. Softw. Eng. Knowl. Eng. **29**(10), 1557–1604 (2019)
34. Knijnenburg, B., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., Sloan, H.: Death to the Privacy Calculus? (2017). Available at SSRN 2923806. Accessed 05 Mar 2020
35. Namara, M., Sloan, H., Jaiswal, P., Knijnenburg, B.: The potential for user-tailored privacy on Facebook. In: Proceedings of the Symposium on Privacy-Aware Computing, USA, pp. 31–42. IEEE (2018)
36. Taddicken, M.: The privacy paradox in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self disclosure. J. Comput. Med. Commun. **19**(2), 248–273 (2014)
37. Stutzman, F., Vitak, J., Ellison, N.B., Gray, R., Lampe, C.: Privacy in interaction: exploring disclosure and social capital in Facebook. In: Proceedings of 6th Annual International Conference on Weblogs and Social Media, Ireland, pp. 330–337. AAAI Publ. (2012)
38. Marwick, A.E., Boyd, D.: Networked privacy: how teenagers negotiate context in social media. New Med. Soc. **16**(7), 1051–1067 (2014)
39. Wessels, B.: Identification and the practices of identity and privacy in everyday digital communication. New Med. Soc. **14**(8), 1251–1268 (2012)
40. Tzortzaki, E., Kitsiou, A., Sideri, M., Gritzalis, S.: Self-disclosure, privacy concerns and Social Capital benefits interaction in FB: a case study. In: Proceedings of the 20th Pan-Hellenic Conference on Informatics, Greece, pp. 1–6. ACM (2016)
41. Kramer, R.M.: Social identity and social capital: the collective self at work. Int. Pub. Manag. J. **9**(1), 25–45 (2006)
42. Hoang, L.N., Jung, J.J.: Privacy-aware framework for matching online social identities in multiple social networking services. Cybern. Syst. **46**(1–2), 69–83 (2015)
43. Calikli, G., et al.: Privacy dynamics: learning privacy norms for social software. In: Proceedings of 11th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, Texas, pp. 47–56. ACM (2016)
44. Hogg, M., Abrams, D., Brewer, M.: Social identity: the role of self in group processes and intergroup relations. Group Process. Intergroup Relat. **20**(5), 570–581 (2017)
45. Hogg, M., Smith, J.: Attitudes in social context: a social identity perspective. Eur. Rev. Soc. Psychol. **18**(1), 89–131 (2007)
46. De Wolf, R., Willaert, K., Pierson, J.: Managing privacy boundaries together: exploring individual and group privacy management strategies in Facebook. Comput. Hum. Behav. **35**, 444–454 (2014)
47. Xu, H., Dinev, T., Smith, I., Hart, P.: Information privacy concerns: linking individual perceptions with institutional privacy assurances. J. Assoc. Inf. Syst. **12**(2), 798–824 (2011)
48. Buchanan, T., Paine, C., Joinson, A.N., Reips, U.: Development of measures of online privacy concern and protection for use on the Internet. J. Am. Soc. Inform. Sci. Technol. **58**(2), 157–165 (2007)
49. Smith, J.H., Milberg, S.J., Burke, S.J.: Information privacy: measuring individuals concerns about organizational practices. MIS Q. **20**(2), 167–196 (1996)
50. Malhotra, N., Kim, S., Agarwal, J.: Internet users' information privacy concerns: the construct, the scale, and a causal model. Inf. Syst. Res. **15**(4), 336–355 (2004)
51. Dinev, T., Hart, P.: Internet privacy concerns and social awareness as determinants of intention to transact. Int. J. Electron. Commer. **10**(2), 7–29 (2005)

52. Yao, M., Rice, R., Wallis, K.: Predicting user concerns about online privacy. J. Am. Soc. Inform. Sci. Technol. **58**(5), 710–722 (2007)
53. Hong, W., Thong, J.Y.: Internet privacy concerns: An integrated conceptualization and four empirical studies. MIS Q. **37**, 275–298 (2013)
54. Cho, H., Knijnenburg, B., Kobsa, A., Li, Y.: Collective privacy management in social media: a cross-cultural validation. ACM Trans. Comput. Hum. Interact. **25**(3), 1–33 (2018)
55. Bentley, S., Greenaway, K., Haslam, S., Cruwys, T., Haslam, C., Cull, B.: Social identity mapping online. J. Pers. Soc. Psychol. **118**(2), 213–241 (2020)
56. Postmes, T., Haslam, S.A., Jans, L.: A single-item measure of social identification: Reliability, validity, and utility. Br. J. Soc. Psychol. **52**(4), 597–617 (2013)
57. Brook, A.T., Garcia, J., Fleming, M.A.: The effects of multiple identities on psychological well-being. Pers. Soc. Psychol. Bull. **34**(12), 1588–1600 (2008)
58. Williams, D.: On and off the 'net: Scales for social capital in an online era. J. Comput. Med. Commun. **11**(2), 593–628 (2006)
59. Kalloniatis, C.: Incorporating privacy in the design of cloud-based systems: a conceptual metamodel. Inf. Comput. Secur. J. **25**(5), 614–633 (2017)