future internet

MDPI

Article

Identifying Privacy Related Requirements for the Design of Self-Adaptive Privacy Protections Schemes in Social Networks

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, GR 81100 Lesvos, Greece; chkallon@aegean.gr
[2] Information and Communication Systems Security Laboratory, Deptartment of Information and Communication Systems Engineering, University of the Aegean, GR 83200 Samos, Greece; etzortzaki@aegean.gr
[3] Laboratory of Systems Security, Department of Digital Systems, University of Piraeus, GR 18532 Piraeus, Greece; sgritz@unipi.gr
* Correspondence: a.kitsiou@aegean.gr; Tel.: +30-22510-36660

Abstract: Social Networks (SNs) bring new types of privacy risks threats for users; which developers should be aware of when designing respective services. Aiming at safeguarding users' privacy more effectively within SNs, self-adaptive privacy preserving schemes have been developed, considered the importance of users' social and technological context and specific privacy criteria that should be satisfied. However, under the current self-adaptive privacy approaches, the examination of users' social landscape interrelated with their privacy perceptions and practices, is not thoroughly considered, especially as far as users' social attributes concern. This study, aimed at elaborating this examination in depth, in order as to identify the users' social characteristics and privacy perceptions that can affect self-adaptive privacy design, as well as to indicate self-adaptive privacy related requirements that should be satisfied for users' protection in SNs. The study was based on an interdisciplinary research instrument, adopting constructs and metrics from both sociological and privacy literature. The results of the survey lead to a pilot taxonomic analysis for self-adaptive privacy within SNs and to the proposal of specific privacy related requirements that should be considered for this domain. For further establishing of our interdisciplinary approach, a case study scenario was formulated, which underlines the importance of the identified self-adaptive privacy related requirements. In this regard, the study provides further insight for the development of the behavioral models that will enhance the optimal design of self-adaptive privacy preserving schemes in SNs, as well as designers to support the principle of PbD from a technical perspective.

Keywords: social networks; self-adaptive privacy; privacy related requirements; users' social landscape

check for updates

Citation: Kitsiou, A.; Tzortzaki, E.; Kalloniatis, C.; Gritzalis, S. Identifying Privacy Related Requirements for the Design of Self-Adaptive Privacy Protections Schemes in Social Networks. *Future Internet* **2021**, *13*, 23. https://doi.org/10.3390/fi13020023

Academic Editor: Luis Javier Garcia Villalba

Received: 21 December 2020
Accepted: 15 January 2021
Published: 21 January 2021

1. Introduction

The ubiquitous prevalence of Social Networks (SNs) in modern societies, which consist of the most preferable cloud computing services worldwide, has dynamically transformatted not only the field of communication, but also many others socio-economical domains, such as relationships maintenance, entertainment, social interaction, self-representation, professional activities, and e-governance [1]. This intensification of individual and social activities, in several domains within SNs, promotes complexity and it shifts the edges among the determination and the activities of public and private life [2]. This occurs, since, in order for SNs to be effectively utilized, users provide a great amount of personal information, which is further analyzed and used by the SNs providers [3]. Furthermore, taking into consideration that SNs overcome spatiotemporal boundaries as well, they lead to a greater diffusion of users' personal and sensitive information than other informational systems [4]. As [5] maintain this ubiquity of information analyses and distribution impacts on users' social norms of privacy. In this respect, [6] emphatically supports that a new battleground among individuals and service providers is indicated, concerning "a new kind of information war" p. 64, regarding the access, collection, storage, processing and disclosure of users' personal information. SNs' structure challenge the concept of privacy [7–9], which, over the past years, has been determined under different, but often overlapping frameworks and notions [10,11]. Therefore, they challenge users' social privacy norms and their respective practices. Thus, under this "war" and the privacy notion challenges, it has been recognized that users' privacy protection is not adequately achieved within SNs. Furthermore, users' complex privacy concerns and needs, under the different contexts that they use SNs, are not respectively well-considered [12]. Additionally, despite the fact that several privacy and security measures have been introduced by SNs providers in order to provide users' with the sense that they have control over their information, it is proved that only providers have this ability [13].

Previous research has also highlighted that users differ significantly in their privacy management strategies within SNs, raising questions for how to support such broad privacy concerns and needs in a more user-centered way. In particular, in Europe, this is even more immense, considering the enforcement of the General Data Protection Regulation (GDPR), which promotes users' privacy safeguard not only at a socio-legal oriented layer, but also at a technical one, supporting the implementation of the principle of Privacy by Design (PbD). PbD, introduced at first by [14], aims to be a holistic and human-orientated approach for implementing technical privacy measures, offering realistic solutions [15]. According to GDPR, the data controllers and processors, including SNs providers obviously, are obligated to deploy the appropriate technical procedures in order to ensure the protection of the data subjects' rights [16]. In this regard, providing SNs users with the control over their information could be a realistic solution to several privacy issues that derive from users' willing to disclose information, while preventing unauthorized access from third parties. From a technical perspective, as [13] supports, either hosting user's information on a constantly available paid server or providing personal server for each user or a personal virtual machine in a paid cloud, as well as the acting of personal mobile devices with Internet connectivity as servers, could be effective solutions for users' privacy protection.

To that end and towards to provide effective privacy protection schemes within SNs, in a more user-centered way, several self-adaptive privacy approaches have been developed [17]. Self-Adaptive privacy aims at protecting users' privacy, through the development of holistic user models that pay attention to their socio-contextual and technological frames of action [18]. For instance, [19] developed the user-tailored privacy by design framework, aiming to address the types of privacy adaptations that should be implemented, in order for Facebook users with different privacy management strategies to be supported more personalized. However, as other previous ambitious self-adaptive privacy schemes for SNs [20,21] that have been proposed, their work does not identify users' social categories and attributes in depth. These attributes affect their privacy norms, which is of great importance for the developers and the design of adequate privacy solutions [2], in order for instance to support users' authentication, authorization and confidentiality of personal information, which considered being of the most significant privacy challenges in Internet of Things environments [22].

In our previous work [23], we have shown that, in particular for self-adaptive privacy schemes, in order to be effectively designed and deployed, several criteria concerning users' social and technical context should be satisfied. Self-adaptive privacy systems should be able to protect users' privacy in changing contexts, either by providing users with recommendations or by proceeding automated actions based on users' decisions for personal information disclosure or not, within their context. In this regard, specific functions should be deployed, such as classified interaction strategies, which facilitate the connection of the system and the user, providing privacy awareness, justification for each privacy decision and control capabilities. To address that, monitoring, analysis, design, and implementation of self-adaptive privacy systems should be performed through framework and behavioral models, which identify user's environment and their interconnections with each system. Furthermore, the systems should be adapted to the interoperability of the used technologies and to the structure of the systems, such as SNs, so as to balance among systems' privacy choices automation and users' choices. This reveals a number of criteria that should be considered in order to reason about privacy under a socio-technical view. These concern: (a) the identification of users' privacy social needs in each context; (b) the identification of all stakeholders' privacy technical needs; (c) the identification of privacy risks and threats; (d) the indication of users' sensitive information in each context; (e) the systems' adaption to the interoperability of technologies; (f) the assessment of the best options among users' and systems' privacy choices; and (g) an effective decision-making procedure to be followed, which balances users' social and privacy needs.

Among these criteria, the identification of users' social characteristics and privacy needs is crucial, since, in previous works regarding self-adaptive privacy schemes, these were part-substantially or limited addressed. This identification will provide further privacy protection within SNs, enabling for instance the satisfaction of the privacy criteria that [13] supported, such as the addition/removal of users from a SNs group, the efficiency of a user key revocation, the encryption/decryption efficiency, the encryption header overhead, the ability to encrypt for the conjunction/disjunction of SNs groups, the ability to encrypt for a SNs a user which is not a group member. Therefore, to support this aim, the investigation and the capturing of empirical data related to users' social characteristics specifically within SNs is required, since they affect their privacy management. For example, users' privacy safeguard, when they share information concerning multiple users, is of major importance [24]. The lack of the empirically identified social parameters that influence individuals' privacy behaviors within SNs, highlights a major challenge in order to address self-adaptive privacy under a systematic user-centric way. Since SNs, and cloud services in general, are getting more customized and context-aware, there is a greater necessity to understand which of the users' social attributes are important regarding SNs use, as well as which are their specific privacy behaviors.

In this regard, this paper, as a part of our study for the identification of the socio-technical requirements for the design of self-adaptive privacy-aware cloud-based systems, presents the crucial issues of leveraging knowledge about users' specific individual and social factors and of identifying relevant determinants of privacy practices within SNs. We support that this identification will provide input for the design of usable and self-adaptive privacy within SNs. To achieve that and to capture these data, a survey was administrated to the academic and administrative staff of the University of the Aegean in Greece. The survey was implemented by distributing an interdisciplinary measurement instrument that we introduced in a previous work [25]. This embodies validated metrics from both privacy and sociological literature. The instrument promotes the thoroughly identification of users' social landscape and privacy perceptions and behaviors within SNs. The results of this examination provide the further understanding of users' digital and social privacy interests and boundaries, enabling future research for the meeting with technical privacy affordances, so as to balance among users' need for preserving personal information and the need for disclosing such information within SNs. The rest of the paper is organized as follows. Section 2 presents the methodology regarding our research, data collection and sampling, as well as the instrument that was distributed and its measures. Section 3 presents the results regarding users' social attributes and privacy perceptions and management within SNs, while Section 4 discusses the results. Finally, Section 5 concludes our work and poses future research directions.

2. Materials and Methods

Privacy, as a multifaceted concept, presupposes different privacy perceptions and management strategies for different users in SNs, which differentiate even more because their diverse socio-contextual backgrounds. Due to this complexity, it is often difficult to be measured, so as to reflect users' social privacy norms and therefore to lead to the proper technical privacy measures development for managing privacy issues within social networks in a self-adaptive way [26]. Despite the fact that users' social landscape is of vital importance for understanding their privacy perceptions and behaviors, most of previous works, regarding users' privacy management [27,28], fragmentary include social factors in their measurement scales, addressing consequently privacy as a one-layered construct. To meet that need, the measurement instrument that was developed, adopted constructs and their respective metrics from both sociological and privacy literature, aiming at examining multiple information about users' social attributes and privacy management within SNs. As far as the sociological literature concerns, it put special emphasis on social identity theory metrics and social capital theory metrics, since both social identity and social capital concepts have been highlighted by previous research to influence users' privacy management within SNs [29,30].

Social identity refers to the ways that individuals determine their attitudes and practices in each domain of activity, based on specific social attributes, which represent their personal social categories and characteristics [31]. Furthermore, previous literature supports that there is a high possibility for individuals to gain more resources when they belong to many groups [32], and in this sense, users' social identity affects their social capital. Social capital captures the gains and the advantages that individuals obtain by participating in networks and social institutions [33]. Two types of social capital are referred by previous literature to affect privacy management, the Bonding and the bridging one [34]. 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 ties among individuals within vulnerable, heterogeneous, and diverse networks, experiencing different situations, without a common sense of belonging [33]. Consequently, in contrast to previous research that has examined these social constructs separately, in our work they are both examined, in order to provide further understanding of users' social landscape. Privacy literature was thoroughly investigated in order for the validated metrics of previous works regarding privacy perceptions and management to be adopted in our instrument. Since privacy, apart from the several definitions of its concept; it has specific and very often descriptive and measurable interactive functions within a society [26], such as privacy concerns, privacy risks, and privacy behaviors, it was important to incorporate these measures in our instrument. Woo in [35], for instance, argues about individuals' management strategy to remain anonymous and untraceable within SNs, not only by not providing personal information at all, but also by providing untrue information in order for not to be visible while online [36]. The specific privacy metrics are described in detail as follows. Therefore, the questionnaire that was developed for the data collection, included three wider sections, concerning users' social identity, users' social capital and users' privacy management within social networks, along with their respective items. Furthermore, a set of six questions to address participants' socio-demographic characteristics, namely gender, age, family form, educational level, professional experience, monthly income, were included in the last part of the instrument, in order to take advantage of the beneficial time that participants needed to complete it.

2.1. Social Identity

The five items of this section regarding the examination of users' social identity were adopted from [32] work, entitled Online Social Identity Mapping (oSIM), a tool that was designed to assess the multifaceted aspects of individuals' social identities. Participants were firstly asked to indicate in which groups they belong within SNs, by using a social identity taxonomy compatible with [31] work. This include groups, such as broad opinion-based ones, leisure groups, family or friendship, community groups, sporting or well-being ones, professional groups, health related ones or other users' indicative groups. The item high-contact groups concerns the frequency that users communicate with the members of the groups that they belong within SNs and by which participants rated this frequency on a 5-Point Likert scale, ranging from "not often at all" to "every week".

For the rest three items, positive groups, representative groups and supportive groups, participants were asked to rate their agreement on a 5-Point Likert scale as well, declaring of how much positivity they perceive for each one of their SNs indicated groups, of how representative they feel due to belonging to each one of their SNs indicated groups and of how much support they receive from each one of their SNs indicated groups.

2.2. Social Capital

In this section, the two constructs of Bonding and Bridging social capital are examined. The five items that investigate users' bonding social capital within SNs, by using a 5-Point Likert system, are derived from Williams [37] Bonding Social Capital Scale and they are (a) "If I needed 100 € urgently someone of my social network could lend me", (b) "People of my social network could provide good job references for me", (c) "When I feel lonely there are several people on SMs I could talk to", (d) "There are several people on SMs I trust to solve my problems", and (e) "I do not know anyone well enough from my SMs network to get him/her to do anything important".

The Bridging social capital five items of our instrument have been incorporated from [34] as well, as the most used and validated metrics in previous privacy research. These, in particularly, are (a) "Interacting with people in my social network 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 SMs network makes me feel like a part of a larger community", and (e) "Interacting with people in my SMs network makes me realize that somehow we are all connected worldwide".

2.3. Privacy Management

Considering that previous privacy metrics could be further exploited from expansion in many ways [28], while the combination of their advantages may elevate the examination of self- adaptive privacy within SNs, this section is consisting of nine sub-scales, adopted from previous literature. It aims at including as much as possible privacy-related metrics, in order to reflect users' privacy context within SNs in depth. The participants were asked to rate their agreement on a 5-Point Likert scale, ranging from "not at all" to "very much", for the following subscales and their specific items:

i. 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 [38].
ii. 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 SMs could be misused; (c) I'm concerned that too much personal information is collected by so many SMs; (d) It usually concerns me when I am asked to provide personal information on SMs; (e) I am concerned that others can find private information about me online; and (f) I am concerned about providing personal information on SMs, because it could be used in a way I did not forese. [28,39].
iii. Information Collection: (a) It usually bothers me when SMs ask me for personal information, (b) When SMs ask me for personal information, I sometimes think twice before providing it, and (c) It bothers me to give personal information to so many SMs [40,41].
iv. 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 [42].
v. Trusting Beliefs: (a) SMs would be trustworthy in information handling, (b) SMs fulfill promises related to the information provided by me, (c) I trust that SMs would keep my best interests in mind when dealing with my provided information [41].

vi. 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 SMs where I give out personal information, (d) I would opt out of a service due to privacy issues, and (e) I only upload information online that is suitable for everyone that can see [27,28,39,42].

vii. Privacy Awareness: (a) Personal information is of value to SMs providers, (b) I am aware of the privacy issues and practices in SMs, (c) SMs 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 SMs employ, and (f) I am aware of protecting my personal information from unauthorized access [28,39].

viii. Collaborative privacy management: (a) Prior to disclosing content, my group members and I discuss the appropriate privacy settings, (b) I ask for approval before dis-closing content from those group members involved, and (c) My group ask for approval before uploading content concerning myself [43].

ix. 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 SMs is greater than my concern about privacy, and (c) I value the personalized SMs I received from providing such personal information [39].

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 [28], neglecting users' socio-contextual attributes. Therefore, they do not provide a more socio-technical perspective, despite the fact that for SNs, security and privacy is a major issue. [44], specifically, maintain that focusing on privacy requires not only the security of users' personal information and content, but also the security of SNs communication channels from internal or external attacks, as well as the unauthorized access to users' communication by third parties, using access control mechanisms. In this respect, [45] support that the following security and privacy requirements are immense, namely, the identity privacy, the location privacy, the node compromise attack, the layer-removing/adding attack, the forward and backward security, as well as the semi-trusted and malicious cloud security. Considering these, in order to expand previous works and to identify the adequate privacy-related requirements for a self-adaptive privacy protection scheme within SNs, the key issue is to examine users social and privacy needs. To our best knowledge, a measurement scale meeting these issues and focusing on self-adaptive privacy management within SNs in particular has not been developed in previous literature. To address that, taking into consideration that existing privacy scales could benefit from expansion manifold, while the combination of the advantages of previous privacy metrics may improve the level of privacy within cloud, we presented our scale. In the following Table 1 the comparison with these previous measurement scales is presented, indicating that social identity and social capital metrics are not included in other works.

Table 1. Comparison with previous privacy scales.

Privacy and Sociological Metrics	[27]	[28]	[38]	[39]	[40]	[41]	[42]	[43]	Our Scale
Beliefs in Privacy Rights			X						X
Privacy Concerns		X		X				X	X
Information Collection					X	X			X
Self-disclosure					X		X		X
Trusting Beliefs						X			X
Privacy Control	X	X		X			X		X
Privacy Awareness		X		X					X
Collaborative privacy management								X	X
Self-disclosure/Cost–Benefit				X					X
Bonding Social Capital									X
Bridging Social Capital									X
Social identity metrics									X

2.4. Sample, Data Collection and Procedure

The academic and administrative staff of the University of the Aegean in Greece was invited to participate in this survey, considering that adults are more likely to participate in many social groups and to support, due to their age, plenty of social roles. The total research population is consist of 747 members. In total, 123 members of the staff yielded the questionnaire; thus, 10 cases were excluded. Therefore, a total sample of 113 participants was included in our survey, giving a response rate of 15%. Before the distribution of the questionnaire to the research population, the instrument was tested for its form, language, clarity, difficulty and responsiveness to respondents' interests in a pilot study addressed to 20 members of the staff, in order to identify possible design problems and to revise items where it was necessary. The questionnaire was implemented through Google forms and its link was sent in the professional e-mails of the staff of the University of the Aegean. The procedure and the purpose of the survey were explained with clarity in the online questionnaire's introductory note, as well as ethics was plainly described. The instrument was also tested for its validity and reliability (values of Cronbach's Alpha index were >0.7 for each section).

3. Results

3.1. Sample Demographics

In our exploratory on line survey, the male and female gender, 48% and 50%, respectively, are equally represented, while a small percent (2%) declares other gender, without though of being self-determined rearding the kind of the gender. This finding indicates that there is a percentage of the academic and administrative staff that it feels to belong to another gender, besides the traditional biological ones. This participants' declaration may be recorded, since the University of the Aegean has establihed a Gender Equality Committee in order to provide all genders, biological and social, rights. Considering that the total research population is equally gender distributed, this was expected. In the following Table 2 participants' gender profile is fully presented.

Table 2. Gender.

Gender	Value	Percentage%
Male	54	48%
Female	57	50%
Other	2	2%

Most of the participants are belonging to the age group of 41–45 (31%), while other ages groups were lower represented, 36–40 (20%) and 46–50 (23%). However, most of them are older than 35 years old. Previous literature [28] has shown that the elder the users are the more severe privacy rules they deploy, when on line, and therefore this argument is considerable and for our sample as well. In the following Table 3 participants' age profile is fully presented.

Table 3. Age groups.

Age Groups	Percentage%
26–30	4%
31–35	4%
36–0	20%
41–45	31%
46–50	23%
51–55	16%
55–60	2%

Despite that nuclear family is the dominant form of family (67%), a 12% declares to belong to a single-parent family. It is quite interesting that an 8% of the participants declares "other form of family", such as reorganized family or foster family, without though indicating which one. Another 8% of them did not provide any response for its family form at all. This was the only one socio-demographic item that a notable part of our sample preferred not to give a specific answer, making indistinguishable this social characteristic, which is of great importance, considering that the form of family consists a key source of individuals' social identity construction [46] and their social capital as well. In the following Table 4 participants' family profile is fully presented.

Table 4. Family Form.

Family Form	Percentage%
Nuclear Family	67%
Large Family	5%
Single-Parent Family	12%
Other Form	8%
No answer	8%

The most of the responders are highly educated, having gained a Master Diploma (75%), while only 2% does not hold a bachelor. These results indicate participants' high level of cultural capital, according to Bourdieu theory [34], which concerns the accumulated human labor that institutionally takes form through the study evidence, such as diploma degrees, while under certain conditions; it is convertible into financial capital. In the following Table 5, participants' educational profile is fully presented.

Table 5. Educational level.

Family Form	Percentage%
ICD4	2%
Bachelor	14%
MSc	75%
PhD	9%

As far as the years of professional experience concerns, a great proportion of the participants has been engaged in the professional field more than ten years, 11–15 (20%), 16–20 (36%), and 21–25 years (20%) as well. Previous sociological literature has highlighted that employment affects individuals' lives regarding their priorities in several domains [47], and therefore this factor considered important in relation with our sample's privacy perceptions. In the following Table 6, participants' professional profile is fully presented.

Table 6. Years of professional experience.

Years of Professional Experience	Percentage%
1 to 5	10%
6 to 10	7%
11 to 15	20%
16 to 20	36%
21 to 25	20%
>26	7%

Finally, for more than the half of the participants (55%), their monthly income ranges among 1001–1500 €, while a 12% of them declares monthly income higher than 2000 €. This indicates that for most of the participants' cultural capital has been indeed transformed to the financial one, especially when consider the economic crisis in Greece, the large unemployment figures and the low pay-rolls for a large part of the employees. In the following Table 7, participants' income profile is fully presented.

Table 7. Monthly Income.

Monthly Income	Percentage%
301–800 €	7%
801–1000 €	19%
1001–1500 €	55%
1501–2000 €	7%
2001–3000 €	12%

3.2. *Social Identity*

In respect with privacy notion, social identity is also a complex and multifaceted concept, due to the dynamic way that it is formed and redefined in space and time, as well as due to the complexity that characterizes interpersonal interaction [48]. Previous literature indicates that individuals are characterized by multiple social identities that define their behaviors within a context of action [49,50] and respectively this procedure is proved to be taken place for our sample within SNs, as findings indicate.

3.2.1. Belonging to SOCIAL Groups in SNs

Findings show that participants belong to several social groups in SNs and therefore they formulate multiple digital social identities. All of the participants declare to belong to more than five (5) social groups. Thus, the dominant social group in which respondents declare to participate, concerns the "Friends" group (23%), while "Family" and "Companionships" are also highly indicated, 17% and 15%, respectively. Nine percent of the participants indicates its belonging to professional groups, while 6% of them declares and a scientific group as well. Other groups that participants declare in a lower degree, concern the following categories: Political groups, Trade union groups, Voluntary groups, Sport groups, Leisure groups, Cultural groups, Human Support groups, Environmental Groups, mutual Support groups, Technological Interest groups, and gender equality groups, highlighting a wide range of activities within their social networks. In the following Table 8, participants' declarations for belonging to social groups are fully presented.

Table 8. Belonging to Social Groups in Social Networks (SNs).

Group	Percentage
Family	17%
Friends	23%
Companionships	15%
Professional Group	9%
Political group	3%
Trade union group	1%
Voluntary groups	4%
Sport groups	3%
Leisure groups	4%
Cultural group	6%
Human Support group	1%
Scientific group	6%
Environmental Group	3%
Mutual Support	1%
Technological Interest group	2%
Gender equality group	1%

3.2.2. Frequency of Communication with Social Groups within Social Media

Previous research has shown [51] that the determination and the public expression of belonging to several collective groups—and respectively the formulation and recognition of individuals' various social identities—takes place through communication. Our findings indicate that participants communicate more often (every week) with the social groups of Family (M = 4.8), Friends (M = 4.6), and Companionships (M = 4.4), compatible with the groups that most of them declared to belong to. Thus, it is quite interesting that a high frequency of communication is indicated regarding the Political group (M = 4.5). Participants also declare that communication is quite often realized among the leisure (M = 3.75) and cultural groups (M = 3.8) in their social networks. In the following Table 9, participants' declarations about how often they communicate with their social groups in SNs are fully presented.

Table 9. Interaction with Social Groups within Social media.

	Mean	**Mean**	**Mean**	**Mean**	**Mean**
Group	**Frequency of Communication**	**Positive Impact of Groups**	**Support from Groups**	**Representativeness through Groups**	**Importance of Groups**
Family	4.8	3.5	3.64	3	3.42
Friends	4.6	3.7	3.56	2.92	3.35
Companionships	4.4	3.3	3.06	2.60	3.06
Professional Group	3.2	3.33	2.5	2.33	2.77
Political group	4.5	3.5	3	4	5
Trade union group	-	1	1.5	1	1.5
Voluntary groups	2.2	3	2.66	3.4	2.66
Sport groups	3	3.2	3	2.75	2.33
Leisure groups	3.75	2.66	2,5	3	3
Cultural group	3.8	3.66	3.57	3.5	3.71
Human Support group	3	4	2	-	2
Scientific group	2.66	3.2	3.16	1.83	3.28
Environmental Group	3	3.25	2.5	3.33	3
Mutual Support	2.5	4.5	3.5	2	3
Technological Interest group	2	3.33	2.33	2	3.33
Gender equality group	3	4	3	3	3

3.2.3. Positive Impact of Social Groups within Social Media

Most groups that individuals belong to, provide them with a positive social identity, namely, the part of the development of a positive self-concept that results from this membership [31]. It is quite interesting that our findings show that apart from the Mutual Support Groups (M = 4.5) and the Gender equality and Human support groups (M = 4.5), no other participants' group was so highly rated, despite that family and friends' groups have been previously to be indicated as the most frequent groups to participate and communicate. In the following Table 9, participants' declarations regarding the social groups' positive impact in SNs are fully presented.

3.2.4. Support from Social Groups within Social Media

Despite the fact that previous literature maintains that the participation in a group provides support to each one of its members individually and collectively, not only at a practical dimension, but also at a symbolic one—a transaction that contributes to the preservation of the membership, by providing the recognition of the proximity among group-members [33,34], findings show that participants do not rate highly enough the provided support by their social groups. Thus, family, friends, and cultural groups (M = 3.64; M = 3.56; M = 3.57, respectively) were the highly rated among the others. In the following Table 9, participants' declarations regarding their social groups' support in SNs are fully presented.

3.2.5. Representativeness through Social Groups within Social Media

Self-categorization through social groups has been recognized as a procedure that can reduce individuals' uncertainty, since it provides them with internalized prototypes in order to formulate their identity and define their perceptions and behaviors in a predictable way [31]. Surprisingly, participants, despite their participation in several social groups, rate most of the groups, quite low regarding of how much representativeness they perceive, even the Family and the Friends groups. A higher rating concerns the political groups (M = 4), the cultural groups (M = 3.5), the Voluntary groups (3.4) and the Environmental Groups (M = 3.3). In the following Table 9, participants' declarations regarding their representativeness through their social groups in SNs, are fully presented.

3.2.6. Importance of Social Groups within Social Media

Participants finally were asked to rate the importance of each group they declared that they belong within their social networks. Findings show that the political groups (M = 5) and the cultural groups (M = 3.71) were more highly rated, despite the fact that the most of the participants have declared to belong to Family and Friends groups more widely. Therefore, it is indicated that how much is valued a social group does not depend on the frequency of participation, communication or the support the user derives from it.

3.3. Social Capital

Users' size of social capital is subject to the size of their network connections, namely, the links with which he/se is connected and he/she can motivate effectively to gain benefits (practical or symbolic) among them [34]. Findings indicate that users' investment in social capital concerns medium levels. The perceived bonding social capital (M = 2.92) is higher than the bridging one (M = 2.61). These findings may be indicated due to the characteristics of the Greek culture, where family ties are really strong. Thus, regarding the bonding social capital, it is highligthed that participants assess that the most valued benefit concerns the good job references (M = 3.46), which their connections can offer to them. However, despite the fact that participants declare that in general they can share their loneliness with other people within SNs (M = 3.12), the grade of their trust to other connections is lower (M = 2.95). On the other side, as far as bridging social capital concerns, it is quite interesting that participants rate very low the new conncetions and their activity to meet people through their social networks (M = 1.87), indicating that their social groups within them depend on their already known connections. Furthermore, they also provide a medium rate for their willing to support community activities in SNs.

3.4. Privacy Management

Privacy, as a social phenomenon, is interpreted in several ways both individually and collectively [52] Since privacy definitions are shaped in SNs accordingly with users' societal landscape and outlet, it is important to comprehend how users understand and perceive privacy within them and which attitudes they enhance, in order to protect it. The following findings indicate these perceptions and attitudes.

Under the light of GDPR, users' privacy rights are getting to the forefront of the discourse regarding privacy protection. From users' perspective, previous research has shown that the importance of privacy rights varies along with users' personal and social characteristics and along with the usage context [53]. In our case, findings indicate that participants rate really highly the significance of privacy rights when utilizing SNs, especially as far as the right to have control on their personal information (M = 4.73) concerns. The least high-valued—but still high rated-users' right, concerns their ability to use internet anonymously (M = 3.9). The responses for all items concerning participants' Beliefs in Privacy Rights are fully presented in the following Figure 1.

Previous research has shown that privacy concerns are considered to be a highly important issue among SNs users [54,55]. The findings of our survey support this previous evidence. The participants rated highly enough their privacy concerns, especially regarding the amount of personal information that is collected (M = 4.14) through social networks and the ways that it can be misused (M = 4.14). This finding indicates some of the reasons about their low investment on social capital, while previous literature has highlighted that privacy concerns have a negative impact on users' willing to throw themselves into social networks [56]. The responses for all items concerning participants' Privacy Concerns are fully presented in the following Figure 2.

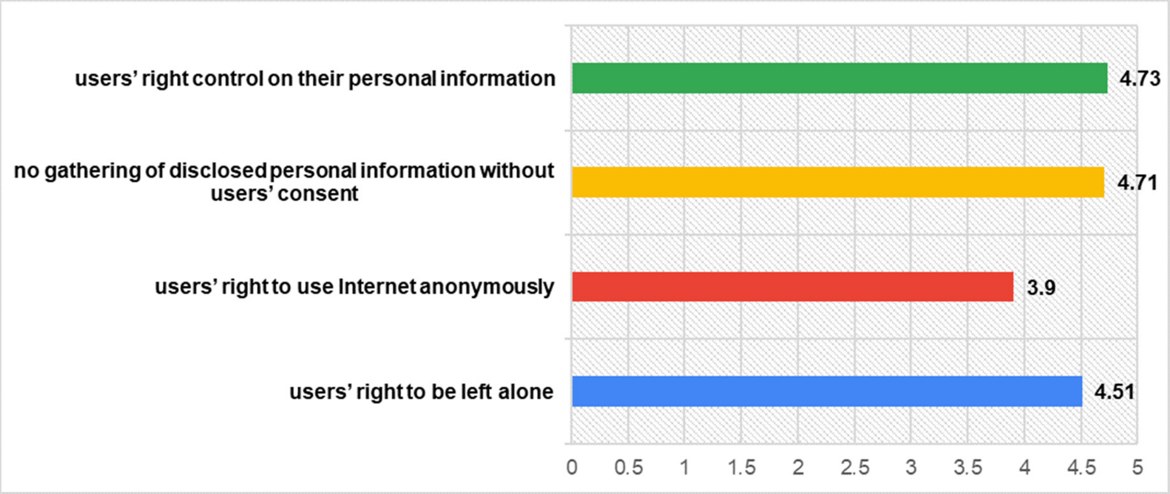

Figure 1. Beliefs in Privacy rights.

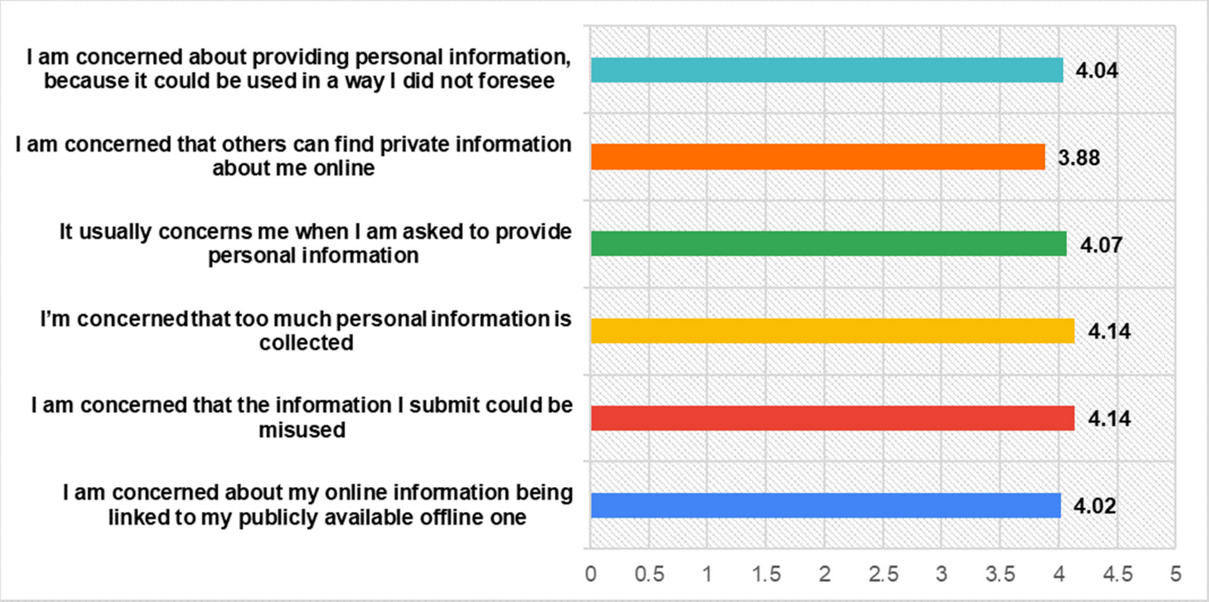

Figure 2. Privacy Concerns.

Compatibly with their responses for privacy concerns, participants declare to be a lot of bothered, when they provide personal information to many social networks (M = 4.32), while they also rate highly enough their doubts to provide them, when they are asked by the networks (M = 4.13). Ref. [57] support that the unwanted access to personal information or the over-collection of personal information constitute important faces of the online privacy issues that should be addressed in a more user-centric way.

Previous research indicates a privacy paradox behaviour of users when utilizing SNs, since besides their concerns, they tend to disclosure personal information on their own [58], while it supports that much more attention should be paid towards the privacy risks they undertake their own due to this sharing information [59]. On the contrast, our findings show that participants' self-disclosure behaviors are consistent with their privacy concerns and their perceptions for information collection within SNs, declaring that they disclose information in a low level, with reference to their concerns and fears (M = 1.72), writing about themselves (1.95) and talking about themselves (M = 1.81), as well as their feelings (M = 1.53). These are illustrated in the following Figure 3.

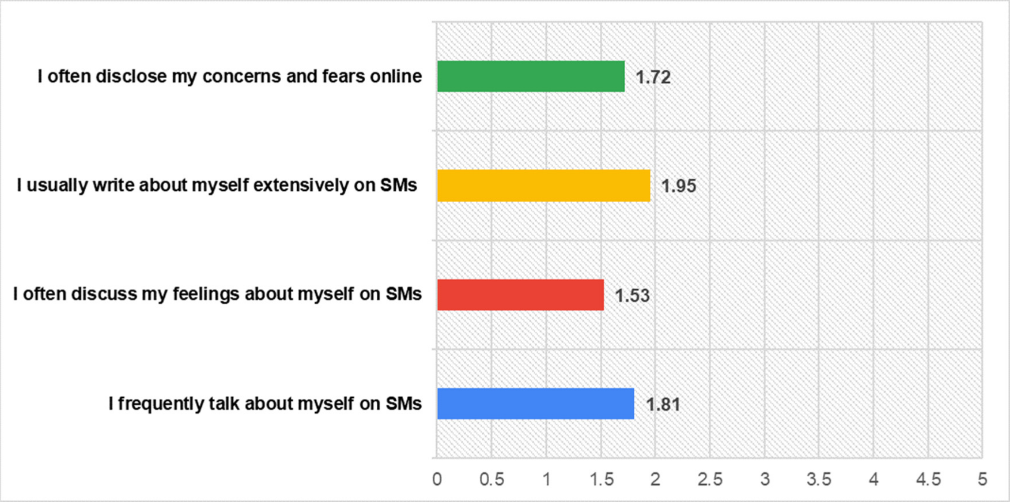

Figure 3. Self-disclosure.

The importance of users' trust on the online environments is widely examined by previous literature [60]. Especially as far as social networks concern, trust is related not only with their engagement, but also with several privacy issues. Privacy concerns, in particular, are highly influenced by users' trust [61]. The participants in our survey, still consistent with their previous responses, rate very low their trust about how their social networks are handling their provided information, with special emphasis on the supporting of their best interests (M = 1.93).

Despite the fact that participants have rated really highly their belief in their right to control their privacy, findings indicate that they do not rate that high their practice of considering social networks privacy policy (M = 2.9), while they declare of achieving a medium level of the appropriateness of their uploaded information related to different audiences (M = 3). Furthermore, they also rate low enough their ability to have control on the audiences that have access to their information (M = 2.18). These indicate the necessity for more effective privacy solutions within SNs that they will provide users with more control on the handling of their information. The participants' responses for privacy control within SNs are fully presented in the following Figure 4.

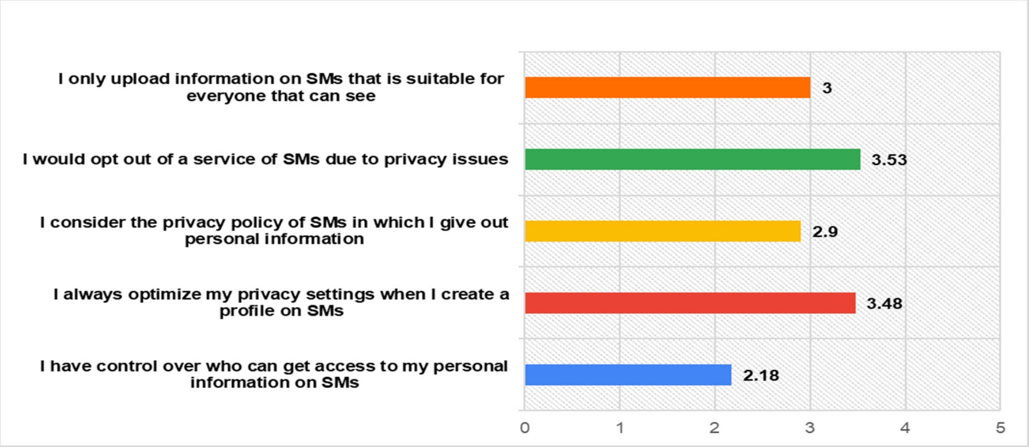

Figure 4. Privacy Control.

Previous literature has shown that users, due to gaining benefits from their social networks, do not weight considerably enough the privacy risks posed by information-sharing activities [53], and therefore their privacy awareness should be enhanced. Findings show that participants declare that they have a medium level of privacy awareness, especially as far as the privacy solutions that law and social networks employ (M = 3.02). However, it is encouraging that participants recognize and rate much higher that their personal information has value for the providers of social networks services (M = 3.86).

This information sharing among users can be a cause of potential risks for each one separately. Personal information disclosures of a user for other users, regardless other users' approval, are common practices within SNS [62]. Findings support this previous knowledge, since participants rate highly enough (M = 3.69) only their own behaviour of asking approval, before disclosing information of their group members. As far as their group members concern, the rating is much lower. The participants' responses regarding the collaborative privacy management within SNs are presented in detail as follows in Figure 5.

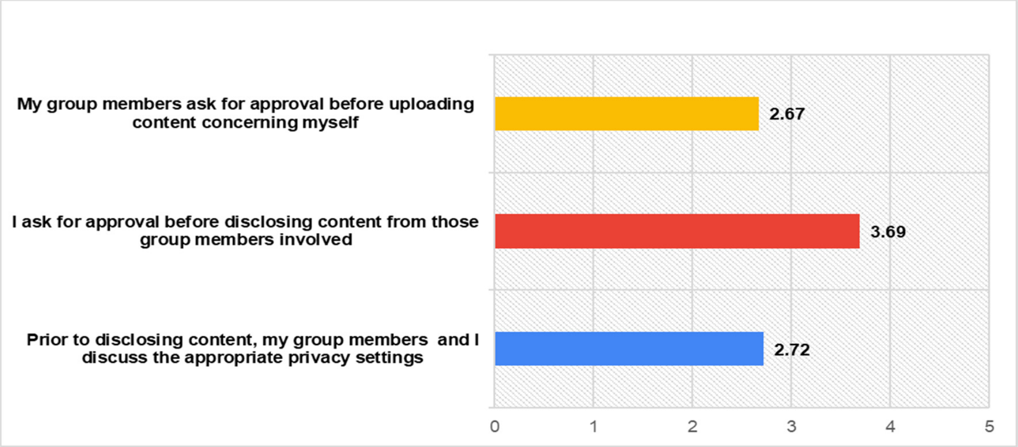

Figure 5. Collaborative Privacy Management.

Previous literature regarding Privacy Calculus [63] shows that users estimate the information disclosure costs and benefits in social networks, indicating that the benefits are constantly irresistible for most of the users. However, our findings highlight that participants evaluate lower the services deriving from their participation in social networks than their privacy concerns and the risks posed due to it.

Our results indicate that, in order to support the design of self-adaptive privacy protection schemes within SNs, users' privacy social and technological context should be considered. SNs cause plenty of privacy concerns for users, while it is highlighted that they do not fulfill their privacy needs or provide them with the adequate trust. Aiming to support this design of self-adaptive privacy safeguard within SNs and the identification of specific privacy related requirements, it is necessary to provide specific constructs that reflect users, SNs and self-adaptive privacy protection schemes parameters in a pilot taxonomic way, as follows.

The users within SNs:

i. Heterogeneous: The users are determined by several social identities, which reflect not only their individual social norms that they are dynamic, but also their reciprocal arrangements with the groups in which they belong within SNs.

ii. Social Interrelated: The users provide access and disclose their personal information in order to gain plenty of symbolic benefits and resources, deriving from their online social networks.

iii. Privacy oriented: The users value the significance of privacy rights on a high level and they raise plenty of privacy concerns when utilizing SNs, while they are characterized by a minimum degree of trust regarding the use of their personal information.

iv. Collaborative: The users co-manage their personal information with other users and they disclose information concerning other users, without, in many cases, having their approval.

The SNs environment:

i. Visible: SNs structure requires from users to provide several personal information regarding their identity, which are visible to a large number of audiences.
ii. Communication varied: SNs structure enables users to communicate by using several means of communication, as well as using many different devices.
iii. Interactive: SNs structure presupposes that users interact with other users, in order to enhance their experiences within these environments and to adapt to the environment context.
iv. Privacy Risky: SNs structure raises several privacy risks, deriving from unauthorized access to users' personal information by unwanted audience or other third parties.

Self-adaptive privacy protection schemes:

i. Context aware: Schemes should be able to identify users' individual and collective values, so as to provide them with the proper privacy choices.
ii. Selective disclosed information: Users should be provided with the opportunity to disclose information in a selective way, depending on the context that they operate, so as to adapt their behaviors accordingly.
iii. Privacy aware enhanced: Users should be informed for the diagnosed privacy risks and be provided with the proper privacy justification for each context in which they operate, in order for their decision-making procedure to be enabled.
iv. Privacy control enhanced: Users should be offered with the opportunity to have control over their information and to decide which of them are willing to disclose accordingly to their individual and social characteristics.

4. Discussion

Users' privacy protection within SNs is an ongoing process, depending on social, legal, and technical aspects [64]. However, their inadequate bridging arises difficulties for an effective privacy protection solution [65], compliant to GDPR principles and rules as well. Towards this, several self-adaptive privacy solutions under the differential privacy scheme [66] or under the context-adaptive privacy scheme [67,68], have been introduced. However, they were subsequent to many limitations, since they did not identify in depth users' social landscape and outlet, failing therefore to correlate them with the appropriate privacy technical solutions [69]. Thus, as we, in detailed, have discussed in a previous work, since self-adaptive privacy focuses on users' integrated context, both social and technical, a group of criteria should be satisfied for its optimal design. Among these, the thoroughly investigation of users' social norms is a focal one and the first step in order for the self-privacy related requirements to be elicited. The determining of users' social attributes will provide developers with further knowledge so as to, not only to include social requirements at their design, but also to build the appropriate technical privacy affordances. After all, previous research for self-adaptive privacy has shown that not enough attention is paid on eliciting requirements from the users' perspective, in order for introducing flexibility in the self-adaptive systems behavior at an early phase of requirements engineering [70], a prerequisite for the implementation of PbD principle. In this regard, our survey highlights the social attributes of a targeted research population within the academic community of a Greek University, this of the academic and administrative staff of the University of the Aegean. It should be noted that, although the utilization and the impact of social networks is growing among the populations of the academic educational settings [71], as far as the privacy issues concern in particular, most of previous research focus on students [52] and not on the adults. Under this, the findings of our survey indicate the social landscape of adults SNs users, which is considerable different from this one of the young adults. Our sample, at the majority, has been indicated to be over the 30 years old, highly educated, with many years of professional experience, while keeping in mind Greece's financial situation, it has a descent monthly income. These entire social attributes, examined separately by previous research, have been shown to influence users' privacy perceptions and behaviors [72,73], leading them to grow their privacy concerns and making them to follow strict enough privacy management strategies when using SNs.

Our findings, while supporting previous evidence regarding privacy concerns and self-disclosure practices, indicate that these attributes do not have the same effect as far as the privacy control concerns, showing a low control level. Despite of the high cultural and financial capital of the participants, privacy control remains an issue of great importance for users and therefore an appropriate self-adaptive privacy scheme should provide users with the control level over the information they want to reveal, as it was argued by [74]. Furthermore, participants in our survey, declare to belong to several social groups within SNs, with most dominant the Friends and Family Groups. This indicates that they belong to more than one social categories, which are significant parts of individuals' self-concept. This categorization enables them to distinguish their personal boundaries and these of their memberships. Thus, participants several social categories create concentrations regarding their "self-interestedness, self-reliance, self-realization and self-determination", as it is shown from their low or medium rates regarding the positive impact, the importance, and the support that they receive from these groups in SNs. This leads to the development of a particular privatism, which can be associated with plenty of personal perceptions and practices in institutional forms of expression as [75] supported, such as the SNs engagement. This privatism development is also indicative for the participants' strong beliefs regarding the necessity of the protection of users' privacy rights, as well as of their annoyance to provide personal information in SNs when is needed.

However, as in previous literature [30,76], privacy managing issues and several privacy implications arise from participants' multiple identities, as it is indicated by fact that the other members of their groups do not take their approval in order to upload their own personal information. It has been already argued that family and close friends group memberships, due to including the baring of emotional needs, enhance risking at various levels. Therefore, this raise further questions regarding the disclosure of personal information within undistinguishable private/public boundaries of contexts, such SNs. In this regard, since self-adaptive privacy protection schemes should have the ability to maintain users' privacy in changing contexts [77], they should provide users with recommendations about their own decisions or of their family and friends group members specifically to disclose or not information. The specification of these groups is of great importance, since [78] in a previous work, attempting to identify distinct social requirements of privacy issues within SNs by interviewing 15 adolescents (14–18) regarding their online behaviour on Facebook, indicated the need to make more explicit which are the "real generalized others". The dominance of Family, Friends and Companionships groups characterizes the frequency of participants' communication within SNs, while it is quite interesting that a great amount of communication takes place among the members of political groups. Especially as far as the belonging to the political groups concerns, participants also declare a high level of representativeness and importance. Therefore, the political social group is also indicated among the social categories that should be taken under consideration, when designing privacy adaptations. In general, the frequent communication contributes to the formulation of a social identity, even though some identities might be more primary than others [79], as it is observed in our case regarding the political group membership. As [80] argue, "mediated groups can develop a meaningful and strong sense of identity through interaction". SNs provide multiple possibilities for interaction and communication. Thus, the technical features of SNs not only alter users' constructs for their functioning and purpose, but they also alter how users actually employ these features for managing privacy, while interacting with other users [2]. The participants, regardless their group memberships, do not find in majority SNs trustworthy enough when handling such information. In this respect, self-adaptive privacy protection schemes should be adapted to the interoperability of SNs technologies and the structure of their systems, considering users communication behavior, in order to determine through these communications, the sensitive information that should not be revealed, at a short time operational function. [78] research, which indicates that a context collision deriving from SNs segments should be avoided, also supports this. In addition to users' social landscape and outlet in SNs, the thoroughly examination of users' privacy perceptions, behaviors and personal information flow is needed. Investigating these as well, since previous works have shown that they affect the identification of the technical privacy requirements, is also a critical step for an adequate self-adaptive privacy solution to be designed.

In our survey, as it was aforementioned, participants' privacy concerns were highly rated. Privacy concerns, among other privacy factors, affect not only users' intentions, but also their actual behaviors [57]. This indicates the reasons that participants invest low in capturing of social capital within SNs through self-disclosing, in contrast with previous findings [81], which show that users willingly provide this information in order to acquire the perceived benefits resulting from their networks. As [82] argue, the interrelation among disclosure attitudes and gaining benefits is not straightforward. Thus, participants rate their privacy concerns higher their needs for SNs services, indicating that their privacy calculus is not expected to change after a privacy violation, since they already respond with mechanisms, such the ones [83] proposed, namely, refusal or negativism. Up to this, considering that the relationship between self-disclosure and benefits is mediated by the factor of control of information [84], it was not surprising that the participants indicate the low degree of control on their information.

However, as results show, they still upload information, for which they are not sure if it is proper for every audience to see or they do not take under consideration SNs privacy policies. After all, previous literature has already highlighted that, while users perceive highly their control over information, they usually ignore the control deriving by SNs policies over the information [85]. With this respect, an effective self-adaptive privacy scheme within SNs should provide users with plenty of control capabilities, enhancing their cognitive processes for implementing their privacy strategies. [77] emphatically support that self-adaptive privacy systems should provide users with adequate opportunities to express preferences and give feedback in relation to the privacy decisions they have to undertake. Nevertheless, ignoring privacy policies, a privacy risky behaviour, indicates another crucial aspect for the participants of our survey, concerning the necessity of the enhancing their privacy awareness. Participants estimate their privacy awareness in medium levels and consequently, privacy aware increase is of great importance to be provided by the designed self-adaptive privacy schemes. This becomes even more crucial, since according to [30], SNs incorporate basic privacy technical features, meeting only typically their responsibility for users' privacy protection, failing to address their complex privacy needs. Up to this, self-adaptive privacy schemes should provide users with the proper classified interaction strategies, facilitating the connection of the systems with them by proceeding to automated actions that enhance their privacy awareness and justify the privacy choices or decisions. This will strengthen users' privacy and it will enhance not only their awareness, but also their knowledge regarding the accessibility and use of information, deriving from SNs structure.

What is more, our survey indicates that participants' information within SNs is co-managed and disclosed by other members of the groups they belong to, leading to risky behaviors, since the other group members do not take approval for disclosing information. As [62] argues, it is often unclear who and how many people are included in the groups, which disclose such information. Furthermore, it is also unclear who accesses and stores users' data, which are often analyzed by unauthorized parties [86]. Personal information disclosures of a user for other users, regardless other users' consent, like sharing friends, family, colleagues and other connections contact lists, enables SNs and third companies to misuse such information and circumvent users' privacy rights provided with GDPR, such as to know, to restrict processing, to not be subject of automated decision-making, leading to untrustworthy web services. Therefore, capturing the collaborative process of privacy management within SNs should be a great deal for the design of self-adaptive privacy schemes. The monitoring process of self-adaptive privacy systems should not focus only to the user itself, but also to its social environment and its interconnections, in order to provide the proper features, since privacy protection within SNs presupposes a group-level coordination.

Drawing up, therefore, on the results of our survey regarding their social attributes, privacy perceptions and management, indicatively the following privacy related requirements should be taken under consideration at the early design of self-adaptive privacy schemes within SNs, in order to support effectively their operations for monitoring, analysis and implementation:

i. Adults SNs users, with high cultural and financial capital, value privacy in a high level and they indicate higher perceived privacy concerns regarding the ways of their personal information is handled and they cannot foresee or of the ways these can be misused. In this respect, self-adaptive privacy schemes should offer users proper justification and awareness about the privacy decision that they undertake.

ii. Adults SNs users, despite their belonging to several social groups within SNs, they more often participate and communicate with Family and Friends groups. Since the belonging in these groups includes emotional involvement and a further level of trust among the members, self-adaptive privacy preserving schemes should provide users with the proper features that detect threats before disclosing information based on this frequent communication and trust among the group members within SNs.

iii. Adult SNs users perceive their belonging to political groups within SNs of great importance. In this regard, self-adaptive privacy schemes should utilize framework models to identify these users' SNs environments and to provide the features that determine the value of such groups, so as to diagnose the privacy related threats.

iv. Adults SNs users, despite the general low to medium level of social capital investment within SNs, give more emphasis in the bonding social capital and in particular in the resources provided for job references. Consequently, when users disclose information for such benefits, self-adaptive privacy schemes should provide them with the possibility of selective information disclosure.

v. Adults SNs users find SNs untrustworthy and they perceive highly the value of their information for these providers. In this regard, self-adaptive protection schemes should be adapted to the interoperability of SNs technologies and the structure of their systems, providing users with justifications regarding the SNs role on privacy risks, in order to take the right privacy decisions.

vi. Adults SNs users perceive a low level of privacy control within SNs, and therefore self-adaptive privacy preserving schemes should provide them with further control capabilities and choices, in order to enhance their privacy awareness as well.

vii. Adults SNs users co-manage personal information with other users within SNs due to belonging to multiple social groups, leading often to privacy implications. Self-adaptive privacy schemes should be able to analyze this co-management and to detect threats before information disclosure, calculating users' benefits in comparison to information disclosure costs.

In the following scenario case, we may focus on an adult female user of Facebook, which belongs in a Family group, in a Friends group, and in political group, while seeking for a job and she has made a lot of applications. In that way, the user is characterized by multiple social identities, such as being a Mother, a Wife, a Political party member, and Unemployed. The user, despite of her privacy concerns, discloses personal information during executing everyday tasks in her daily routine for each one of these identities in her profile, since she has a low degree of privacy awareness of how this information is used. In some cases, other members of her groups disclose her personal information, uploading her photos for instance. Since her profile is open to all, this indicates the revelation of her privacy normativity within Facebook. Everyone is able to follow the user and to have knowledge for her social places or backgrounds, such as her house, her leisure with friends, her activities with the political party. Furthermore, everyone can pay special attention in the way that her social identities are utilized or dropped accordingly.

Therefore, her privacy normativity can include all the anticipated activities, while being present at a specific place, accordingly to the identity, such as eating or home keeping, while using the Mother identity within the family group or her political activities (e.g., participating in a demonstration), while using her political identity. At the same time, since she is seeking for a job, she has asked for job references from her groups' members. However, the direct or indirect disclosure of her information while online can lead to a number of subsequent privacy implications. The privacy implications may happen, when, for instance, an employer in which she has sent an application, will visit her profile and through various ways of her communicating information in Facebook, such as posting photographs, hash tagging places, time description of posts or check-ins, evaluates her activities, and he/she decides not to hire her, because he/she disagrees with her political action or because she has three children. Therefore, privacy implications may appear due to users' social need for sharing information and low privacy awareness that encourage unveiling her identity along with additional information (photographs or hashtags) which may lead to her detectability and observability by unwanted parties. Thus, since a self-adaptive privacy protection scheme could be utilized by the user that has considered these identified privacy related requirements, these implications can be prevented. In case the user, under her Mother identity, is ready to disclose information about her home and children or under her political identity is ready to disclose information for her political action, the self-adaptive privacy scheme is able to indicate users' environment and to identify that she has asked for job references. Therefore, it provides her with the proper justification and awareness about the privacy decision that she will undertake, since it can detect the threats and the privacy implications, before she discloses information. It can also provide user with justifications regarding the Facebook role on privacy risks, since her profile is open, in order to offer her the ability to take the right privacy decision. Furthermore, it is able to analyze the co-management of information sharing from other group members and to detect threats before information disclosure, giving her specific notifications. In this regard, it is of major importance that by identifying these privacy related requirements, user is given with further control capabilities and privacy choices, which, from our survey it is indicated that are lagging, while her privacy awareness is enhanced as well.

Furthermore, considering these privacy related requirements at the early stage of the self-adaptive privacy schemes design, will also enhance the implementation of the technical perspectives of PbD approach. These will support the satisfaction of several technical privacy requirements, such as Authentication, Authorization, Identification, Anonymity, Pseudonymity, Unlinkability, Data Protection, Unobservability, Undetectability, Isolation, Provenanceability, Traceability, Intervenability, and Accountability, which were introduced by the extended PriS framework for cloud computing services [87]. It 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.

5. Conclusions

All Social Networks platforms and their functions nowadays are based on cloud computing. Thus, privacy issues within SNs require specific attention, since they bring new types of threats that designers should be aware of when designing respective services.

Consequently, it is immense to further understand how technology and data collection, storage, and usage might affect users' security and privacy rights [88]. To that end, the safeguarding of users' privacy is realizing through the development of self-adaptive privacy preserving schemes, which are supposed to consider users' social and technological context. In this regard, information about users' social landscape within SNs allows a coherent interrelation with their privacy perceptions and behaviors, enabling consequently, a further investigation of the factors affecting self-adaptive privacy design. Up to this, our study, indicates that a targeted research design in this area is required in order to examine these factors under an interdisciplinary spectrum, so as to capture the relevant parameters that affect self-adaptive privacy design and its requirements within SNs. Therefore, based on an interdisciplinary research instrument that adopted constructs and metrics from both sociological and privacy literature, our study identified users' empirical social data, as well as their privacy views and management within SNs, leading to a pilot taxonomic analysis for self-adaptive privacy within SNs. Therefore, our study provides the ground for the development of targeted research models on self-adaptive privacy within SNs, while it allows a further understanding of how the self- adaptive related requirements can be identified, in order for suitable self-adaptive privacy schemes to the openness and the fluidity of SNs environments, to be designed.

The results of our survey, leveraging knowledge regarding users' social attributes and their perceived privacy management within SNs, led us to propose several privacy related requirements for this domain. In order to further establish our interdisciplinary approach, we formulated a case study scenario. In this case study scenario the user was presented to utilise her Facebook account under her plausible social identities, while possible privacy implications were identified. The importance of the identified self-adaptive privacy related requirements is underlined, since their non-satisfaction can impose more serious privacy implications, affecting user's real life. In this regard, our study will contribute researchers to provide insight for the development of the behavioral models that will enhance the optimal design of self-adaptive privacy preserving schemes in SNs, as well as designers to support the principle of PbD from a technical perspective. Despite the contribution of the study, specific limitations should be referred. For instance, the sociological notion of identity can prove to be even more multidimensional to identify, especially because different naming is used by different authors in order to be analyzed. The interdisciplinary approach of our research and case scenario could be expanded, including further technical constructs, such as security. Furthermore, the implementation on a real case study or experiments with volunteers could be very useful for conducting both a validating and testing process. Future research on this topic will focus on interdisciplinary approaches combining social attributes with technical privacy requirements, proposing a solid background towards addressing users' social context, and designing self-adaptive privacy protection schemes within SNs. In this regard, future research aims at the development of a specific social and technical privacy patterns in order for the operationalization of Self-Adaptive Privacy Systems to be achieved.

Author Contributions: A.K. contributed on the investigation of self-adaptive privacy protection schemes, writing of original draft, and the visualization of the work. E.T. contributed in the research elaboration and the analysis of the work. Assoc. C.K. contributed in the conceptualization of the idea as well as in supervision and writing—review and editing and S.G. contributed in the supervision and writing—review and editing of the paper. All authors have read and agreed to the published version of the manuscript.

Funding: 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)".

Data Availability Statement: Not Applicable, the study does not report any data.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

Social Networks	SNs
General Data Protection Regulation	GDPR
Privacy by Design	PbD
On line Social Identity Mapping	oSIM
Social Media	SM

References

1. Sideri, M.; Kitsiou, A.; Tzortzaki, E.; Kalloniatis, C.; Gritzalis, S. Enhancing University students' privacy literacy through an educational intervention. A Greek case-study. *Int. J. Electron. Gov.* **2019**, *11*, 333–360. [CrossRef]
2. Knijnenburg, B. Privacy in Social Information Access. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*; Springer: Cham, Switzerland, 2018; pp. 19–74, ISBN 978-3-319-90091-9.
3. Bazarova, N.N.; Choi, Y.H. Self-Disclosure in Social Media: Extending the Functional Approach to Disclosure Motivations and Characteristics on Social Network Sites. *J. Commun.* **2014**, *64*, 635–657. [CrossRef]
4. Toch, E.; Wang, Y.; Cranor, L.F. Personalization and privacy: A survey of privacy risks and remedies in personalization-based systems. *User Modeling User-Adapt. Interact.* **2012**, *22*, 203–220. [CrossRef]
5. Nissim, K.; Wood, A. Is privacy privacy? *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.* **2018**, *376*, 20170358. [CrossRef]
6. Thompson, J. Shifting Boundaries of Public and Private Life. *Theory Cult. Soc.* **2011**, *28*, 49–70. [CrossRef]
7. Martin, K. Understanding Privacy Online: Development of a Social Contract Approach to Privacy. *J. Bus. Ethics* **2015**, *137*. [CrossRef]
8. Vickery, J.R. 'I don't have anything to hide, but . . . ': The challenges and negotiations of social and mobile media privacy for non-dominant youth. *Inf. Commun. Soc.* **2015**, *18*, 281–294. [CrossRef]
9. De Wolf, R.; Pierson, J. Researching social privacy on SNS through developing and evaluating alternative privacy technologies. In Proceedings of the 16th ACM Conference on Computer-Supported Cooperative Work and Social Computing, San Antonio, TX, USA, 23–27 February 2013.
10. Kitsiou, A.; Tzortzaki, E.; Kalloniatis, C.; Gritzalis, S. Chapter 2—Towards an integrated socio-technical approach for designing adaptive privacy aware services in cloud computing. In *Cyber Influence and Cognitive Threats*; Benson, V., Mcalaney, J., Eds.; Academic Press: Cambridge, MA, USA, 2020; pp. 9–32, ISBN 978-0-12-819204-7.
11. Sujon, Z. The Triumph of Social Privacy: Understanding the Privacy Logics of Sharing Behaviors across Social Media. *Int. J. Commun.* **2018**, *12*, 3751–3771.
12. Cook, A.; Robinson, M.; Ferrag, M.A.; Maglaras, L.; He, Y.; Jones, K.; Janicke, H. Internet of Cloud: Security and Privacy issues. In *Cloud Computing for Optimization: Foundations, Applications, and Challenges*; Springer: Cham, Switzerland, 2017.
13. Bodriagov, O. Social Networks and Privacy. Doctoral Dissertation, KTH Royal Institute of Technology, Stockholm, Sweden, 2015.
14. Cavoukian, A. Privacy by design [leading edge]. *IEEE Technol. Soc. Mag.* **2012**, *31*, 18–19. [CrossRef]
15. Romanou, A. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Comput. Law Secur. Rev.* **2018**, *34*, 99–110. [CrossRef]
16. Lambrinoudakis, C. The General Data Protection Regulation (GDPR) Era: Ten Steps for Compliance of Data Processors and Data Controllers. In Proceedings of the 15th International Conference, Trust and Privacy in Digital Business, Regensburg, Germany, 5–6 September 2018; Springer: Cham, Switzerland, 2018; pp. 3–8, ISBN 978-3-319-98384-4.
17. Schaub, F.; Könings, B.; Dietzel, S.; Weber, M.; Kargl, F. Privacy context model for dynamic privacy adaptation in ubiquitous computing. In Proceedings of the UbiComp'12—2012 ACM Conference on Ubiquitous Computing, Pittsburgh, PA, USA, 5–8 September 2012; pp. 752–757.
18. Belk, M.; Fidas, C.; Athanasopoulos, E.; Pitsillides, A. Adaptive and Personalized Privacy and Security (APPS 2019): Workshop Chairs' Welcome and Organization. In Proceedings of the Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization, Larnaca, Cyprus, 9–12 June 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 191–192.
19. Namara, M.; Sloan, H.; Jaiswal, P.; Knijnenburg, B.P. The Potential for User-Tailored Privacy on Facebook. In *2018 IEEE Symposium on Privacy-Aware Computing (PAC)*; IEEE: New York, NY, USA, 2018; pp. 31–42.
20. Kumar, R.; Naik, M.V. Adaptive Privacy Policy Prediction System for User-uploaded Images on Content Sharing Sites. *Int. J. Eng. Technol.* **2018**, *5*, 148–154.
21. Qiuyang, G.; Qilian, N.; Xiangzhao, M.; Yang, Z. Dynamic social privacy protection based on graph mode partition in complex social network. *Pers. Ubiquitous Comput.* **2019**, *23*, 511–519. [CrossRef]
22. Leithardt, V.; Santos, D.; Silva, L.; Viel, F.; Zeferino, C.; Silva, J. A Solution for Dynamic Management of User Profiles in IoT Environments. *IEEE Lat. Am. Trans.* **2020**, *18*, 1193–1199. [CrossRef]
23. Kitsiou, A.; Tzortzaki, E.; Kalloniatis, C.; Gritzalis, S. Exploring Self Adaptive Privacy within Cloud Computing. In Proceedings of the 6th Workshop on the Security of Industrial Control Systems & of Cyber-Physical Systems, Guildford, UK, 14–18 September 2020; Katsikas, S., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Eds.; Springer LNCS Lecture Notes in Computer Science: Guildford, UK, 2020.

24. Beugnon, S.; Puteaux, P.; Puech, W. Privacy protection for social media based on a hierarchical secret image sharing scheme. In Proceedings of the 2019 IEEE International Conference on Image Processing (ICIP), Taipei, Taiwan, 22–25 September 2019; pp. 679–683. [CrossRef]
25. Kitsiou, A.; Tzortzaki, E.; Kalloniatis, C.; Gritzalis, S. Measuring Users' Socio-contextual Attributes for Self-adaptive Privacy Within Cloud-Computing Environments. In Proceedings of the International Conference on Trust and Privacy in Digital Business, Bratislava, Slovakia, 14–17 September 2020; pp. 140–155, ISBN 978-3-030-58985-1.
26. Chang, C.-H. New Technology, New Information Privacy: Social-Value-Oriented Information Privacy Theory. *SSRN Electron. J.* **2015**, *10*, 127. [CrossRef]
27. Wolf, R.; Willaert, K.; Pierson, J. Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Comput. Human Behav.* **2014**, *35*, 444–454. [CrossRef]
28. Xu, H.; Dinev, T.; Smith, H.; Hart, P. Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *J. Assoc. Inf. Syst.* **2011**, *12*, 1. [CrossRef]
29. Stutzman, F.; Vitak, J.; Ellison, N.; Gray, R.; Lampe, C. Privacy in Interaction: Exploring Disclosure and Social Capital in Facebook. In Proceedings of the International AAAI Conference on Web and Social Mediav, Dublin, Ireland, 4–7 June 2012.
30. Marwick, A.; Boyd, D. Networked privacy: How teenagers negotiate context in social media. *New Media Soc.* **2014**, *16*, 1051–1067. [CrossRef]
31. Hogg, M.; Abrams, D.; Brewer, M. Social identity: The role of self in group processes and intergroup relations. *Group Process. Intergroup Relat.* **2017**, *20*, 570–581. [CrossRef]
32. Bentley, S.; Greenaway, K.; Haslam, S.; Cruwys, T.; Steffens, N.K.; Haslam, C.; Cull, B. Social Identity Mapping Online. *J. Personal. Soc. Psychol.* **2019**, *118*, 213. [CrossRef]
33. Lin, N. *Social Capital: A Theory of Social Structure and Action*; Cambridge University Press: Cambridge, UK, 2001.
34. Bourdieu, P. The forms of social capital. *Forms Soc. Cap.* **1985**, *14*, 241–258.
35. Woo, J. The right not to be identified: Privacy and anonymity in the interactive media environment. *New Media Soc.* **2006**, *8*, 949–967. [CrossRef]
36. Chen, H.-T. Revisiting the Privacy Paradox on Social Media with an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management. *Am. Behav. Sci.* **2018**, *62*, 1392–1412. [CrossRef]
37. Williams, D. On and Off the 'Net: Scales for Social Capital in an Online Era. *J. Comput. Commun.* **2006**, *11*, 593–628. [CrossRef]
38. Hong, W.; Thong, J. Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Q.* **2013**, *37*, 275–298. [CrossRef]
39. Addae, J.; Brown, M.; Sun, X.; Towey, D.; Radenkovic, M. Measuring attitude towards personal data for adaptive cybersecurity. *Inf. Comput. Secur.* **2017**, *25*, 560–579. [CrossRef]
40. Smith, H.; Milberg, S.; Burke, S. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Q.* **1996**, *20*, 167–196. [CrossRef]
41. Malhotra, N.; Kim, S.; Agarwal, J. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Inf. Syst. Res.* **2004**, *15*, 336–355. [CrossRef]
42. Cho, H.; Knijnenburg, B.; Kobsa, A.; Li, Y. Collective Privacy Management in Social Media: A Cross-Cultural Validation. *ACM Trans. Comput. Interact.* **2018**, *25*, 1–33. [CrossRef]
43. Pernul, G.; Kolter, J. Collaborative Privacy Management. *Comput. Secur.* **2010**, *29*, 580–591. [CrossRef]
44. Deliri, S.; Albanese, M. Security and privacy issues in social networks. In *Data Management in Pervasive Systems*; Springer: Cham, Switzerland, 2015; pp. 195–209, ISBN 978-3-319-20061-3.
45. Saraiva, D.A.; Leithardt, V.R.Q.; de Paula, D.; Sales Mendes, A.; González, G.V.; Crocker, P. Prisec: Comparison of symmetric key algorithms for iot devices. *Sensors* **2019**, *19*, 4312. [CrossRef]
46. Kramer, R. Social Identity and Social Capital: The Collective Self at Work. *Int. Public Manag. J.* **2006**, *9*, 25–45. [CrossRef]
47. Todd, S.; Harris, K. What it means when your work is admired by others: Observations of employees of professional sport organizations. *J. Behav. Appl. Manag.* **2009**, *10*, 396–414. [CrossRef]
48. Papaioannou, T.; Tsohou, A.; Karyda, M. Shaping Digital Identities in Social Networks: Data Elements and the Role of Privacy Concerns. In *Computer Security*; Springer: Cham, Switzerland, 2020; pp. 159–180, ISBN 978-3-030-42047-5.
49. Jenkins, R. *Social Identity*, 3rd ed.; Routledge/Taylor & Francis Group: London, UK, 2008.
50. Nario-Redmond, M.; Biernat, M.; Eidelman, S.; Palenske, D. The Social and Personal Identities Scale: A Measure of the Differential Importance Ascribed to Social and Personal Self-Categorizations. *Self Identity* **2004**, *3*, 143–175. [CrossRef] [PubMed]
51. Scott, C. Communication and Social Identity Theory: Existing and Potential Connections in Organizational Identification Research. *Commun. Stud.* **2007**, *58*, 123–138. [CrossRef]
52. Rossler, B. *The Value of Privacy*; John Wiley & Sons: Hoboken, NJ, USA, 2004; ISBN 9780745631110/9780745631103/0745631118.
53. Schomakers, E.-M.; Lidynia, C.; Müllmann, D.; Ziefle, M. Internet users' perceptions of information sensitivity—Insights from Germany. *Int. J. Inf. Manag.* **2019**, *46*, 142–150. [CrossRef]
54. Acquisti, A.; Gross, R. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In *International Workshop on Privacy Enhancing Technologies*; Springer: Berlin/Heidelberg, Germany, 2006; Volume 4258, pp. 36–58.

55. Acquisti, A.; Brandimarte, L.; Loewenstein, G. Privacy and Human Behavior in the Information Age. In *The Cambridge Handbook of Consumer Privacy*; Selinger, E., Polonetsky, J., Tene, O., Eds.; Cambridge Law Handbooks—Cambridge University Press: Cambridge, UK, 2018; pp. 184–197.
56. Wang, Y.; Herrando, C. Does Privacy Assurance on Social Commerce Sites Matter to Millennials? *Int. J. Inf. Manag.* **2019**, *44*, 164–177. [CrossRef]
57. Smith, H.; Dinev, T.; Xu, H. Information Privacy Research: An Interdisciplinary Review. *MIS Q.* **2011**, *35*, 989–1015. [CrossRef]
58. Stutzman, F.; Gross, R.; Acquisti, A. Silent Listeners: The Evolution of Privacy and Disclosure on Facebook. *J. Priv. Confid.* **2013**, *4*, 7–41. [CrossRef]
59. Dienlin, T.; Trepte, S. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *Eur. J. Soc. Psychol.* **2014**, *45*, 285–297. [CrossRef]
60. Kamboj, S.; Sarmah, B.; Gupta, S.; Dwivedi, Y. Examining branding co-creation in brand communities on social media: Applying paradigm of Stimulus-Organism-Response. *Int. J. Inf. Manag.* **2018**, *39*, 169–185. [CrossRef]
61. Chen, H.; Beaudoin, C.; Hong, T. Teen online information disclosure: Empirical testing of a protection motivation and social capital model. *J. Assoc. Inf. Sci. Technol.* **2016**, *67*, 2871–2881. [CrossRef]
62. 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-Disclosure1. *J. Comput. Commun.* **2014**, *19*, 248–273. [CrossRef]
63. Jiang, Z.; Heng, C.; Choi, B. Research Note —Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Inf. Syst. Res.* **2013**, *24*, 579–595. [CrossRef]
64. Nissenbaum, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*; Stanford University Press: Palo Alto, CA, USA, 2010.
65. Knijnenburg, B. Simplifying Privacy Decisions: Towards Interactive and Adaptive Solutions. In *Decisions@ RecSys*; CEUR Workshop Proceedings: Hong Kong, China, 2013; Volume 1050.
66. Phan, N.H.; Wu, X.; Hu, H.; Dou, D. Adaptive Laplace Mechanism: Differential Privacy Preservation in Deep Learning. In Proceedings of the 2017 IEEE International Conference on Data Mining (ICDM), New Orleans, LA, USA, 18–21 November 2017; pp. 385–394.
67. Schaub, F.; Könings, B.; Lang, P.; Wiedersheim, B.; Winkler, C.; Weber, M. PriCal: Context-adaptive Privacy in Ambient Calendar Displays. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Seattle, WA, USA, 13–17 September 2014.
68. Pallapa, G.; Das, S.; Francesco, M.; Aura, T. Adaptive and context-aware privacy preservation exploiting user interactions in smart environments. *Pervasive Mob. Comput.* **2013**, *12*, 232–243. [CrossRef]
69. Martín, S.; Kung, A. Methods and Tools for GDPR Compliance through Privacy and Data Protection Engineering. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy Workshops, London, UK, 24–26 April 2018; pp. 108–111.
70. Weyns, D. Software Engineering of Self-Adaptive Systems: An Organised Tour and Future Challenges. In *Handbook of Software Engineering*; Cha, S., Taylor, R.N., Kang, K., Eds.; Springer: Cham, Switzerland, 2019; pp. 339–443.
71. Davis, C.H.F.; Deil-Amen, R.; Rios-Aguilar, C.; Gonzalez Canche, M.S. Social Media in Higher Education: A literature review and research directions. *SAGE Encycl. Online Educ.* **2012**, *39*, 1–30.
72. Spiliotopoulos, T.; Oakley, I. Understanding Motivations for Facebook Use: Usage Metrics, Network Structure, and Privacy. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Paris, France, 27 April–2 May 2013.
73. Steeves, V.; Regan, P. Young People Online and the Social Value of Privacy. *J. Inf. Commun. Ethics Soc.* **2014**, *12*, 298–313. [CrossRef]
74. Omoronyia, I. Reasoning with imprecise privacy preferences. In Proceedings of the 2016 24th ACM SIGSOFT International Symposium on Foundations of Software Engineering, Seattle, WA, USA, 13–19 November 2016; pp. 952–955.
75. Bailey, J. Some Meanings of 'the Private' in Sociological Thought. *Sociology* **2000**, *34*, 381–401. [CrossRef]
76. Wessels, B. Identification and the practices of identity and privacy in everyday digital communication. *New Media Soc.* **2012**, *14*, 1251–1268. [CrossRef]
77. Schaub, F.; Könings, B.; Weber, M. Context-adaptive privacy: Leveraging context awareness to support privacy decision making. *IEEE Pervasive Comput.* **2015**, *14*, 34–43. [CrossRef]
78. Wolf, R.; Heyman, R.; Pierson, J. Privacy by Design through a Social Requirements Analysis of Social Network Sites form a User Perspective. In *European Data Protection: Coming of Age*; Springer: Dordrecht, The Netherlands, 2013; pp. 241–265.
79. Kuhn, T.; Nelson, N. Reengineering Identity: A Case Study of Multiplicity and Duality in Organizational Identification. *Manag. Commun. Q.* **2002**, *16*, 5–38. [CrossRef]
80. Postmes, T.; Tanis, M.; Wit, B. Communication and Commitment in Organizations: A Social Identity Approach. *Group Process. Intergroup Relat.* **2001**, *4*, 227–246. [CrossRef]
81. Krasnova, H.; Spiekermann, S.; Koroleva, K.; Hildebrand, T. Online Social Networks: Why We Disclose. *J. Inf. Technol.* **2010**, *25*, 109–125. [CrossRef]
82. Costello, C.; McNiel, D.; Binder, R. Adolescents and Social Media: Privacy, Brain Development, and the Law. *J. Am. Acad. Psychiatry Law* **2016**, *44*, 313–321.
83. Becker, J.; Chen, H. *Measuring Privacy Risk in Online Social Networks*; University of California: Davis, CA, USA, 2009; Volume 2, pp. 1–8.

84. Acquisti, A.; Adjerid, I.; Brandimarte, L. Gone in 15 Seconds: The Limits of Privacy Transparency and Control. *Secur. Priv. IEEE* **2013**, *11*, 72–74. [CrossRef]
85. Bertot, J.; Jaeger, P.; Hansen, D. The Impact of Polices on Government Social Media Usage: Issues, Challenges, and Recommendations. *Gov. Inf. Q.* **2012**, *29*. [CrossRef]
86. Al-Rabeeah, A.A.N.; Hashim, M.M. Social Network Privacy Models: A Systematic Literature Review and Directions for Further Research. In Proceedings of the 3rd International Conference on Communication Engineering and Computer Science (CIC-COCOS'19), Tokyo, Japan, 29–30 April 2019.
87. Kalloniatis, C. Incorporating privacy in the design of cloud-based systems: A conceptual meta-model. *Inf. Comput. Secur.* **2017**, *25*, 614–633. [CrossRef]
88. Mican, D.; Sitar-Tăut, D.A.; Moisescu, O.I. Perceived usefulness: A silver bullet to assure user data availability for online recommendation systems. *Decis. Support Syst.* **2020**, *139*, 113420. [CrossRef]