# A Set of Social Requirements for Self-adaptive Privacy Management Based on Social Groups' Belonging

Angeliki Kitsiou, Maria Sideri, Aikaterini – Georgia Mavroeidi, Katerina Vgena,
Eleni Tzortzaki, Michail Pantelelis, Stavros Simou and Christos Kalloniatis
*Privacy Engineering and Social Informatics Laboratory, Department of Cultural Technology and Communication,*
*University of the Aegean, Mytilene, Greece*
{a.kitsiou, msid, kmav, kvgena, etzortzaki, mpantel, ssimou, chkallon}@aegean.gr

***Abstract*—This paper examines the privacy representations and privacy management practices of cloud services users that relate to the social group they belong to, through a quantitative survey addressed to the student population of three Universities in Greece, England, and Spain. Findings provide valuable insights regarding social identity-based users' privacy practices and indicate important information for the design of self-adaptive privacy schemes within cloud services, setting specific social requirements based on users' social groups belonging.**

***Keywords*-adaptive privacy; privacy management; social requirements.**

## I. Introduction

This paper examines critical issues about users' social groups within cloud services related to their privacy management practices, as an extension of our previous paper presented in IARIA CONGRESS in 13–17 November 2023 in Valencia, concentrating only on self-presentation and self-disclosure practices [1]. Cloud services have significantly expanded in current society, transforming the way individuals and organizations store, access, and manage their data and applications. They often offer integration and interoperability capabilities, allowing different applications and systems to communicate and work together seamlessly, indicating the new notion of the Internet of Cloud [2]. This facilitates the exchange of data and information across platforms, enabling real-time collaboration, sharing, and communication among several team members regardless of their physical locations. Thus, the potential challenges and concerns associated with the expansion of cloud services are immense, such as data privacy and security, vendor lock-in and regulatory compliance [3]. Organizations and individuals should carefully evaluate their specific requirements and consider the appropriate privacy measures and service-level agreements when adopting cloud services [4]. Towards these requirements and measures, the notion of social identity has been indicated as an important factor that influences individuals' privacy preferences and concerns [5]. Social identity refers to the way individuals perceive themselves in relation to various social groups they belong to. The forming of these groups can include factors, such as nationality, ethnicity, gender, religion, profession, or interests [6]. Cloud services provide individuals with opportunities to express and project their social identities to others through profiles, content sharing, and interactions. People often join groups or follow pages related to their social identities, fostering a sense of belonging and connection. In this regard, social identity plays a key role in how individuals present themselves and manage their online image within cloud services [7]. Different social groups may have varying attitudes towards self-disclosure and privacy management practices [8]. However, the nature of self-disclosure on cloud services raises privacy concerns, as individuals need to consider the potential risks associated with sharing personal information publicly [9]. Respectively, the variety of attitudes within cloud services concerns privacy as well, such as prioritizing the protection of personal information or embracing a more open approach. People may strategically disclose or withhold personal information in order to shape their online identity and project a desired image that aligns with their social identity and the desired/intended impression they want to create. They may share personal milestones, hobbies, achievements, opinions, or emotions, while choosing to keep other aspects of themselves and their lives private. Social identity can shape the norms and expectations around privacy within specific social groups. Group members may have shared understandings of what information is appropriate to share, the level of privacy they expect, and the consequences of privacy breaches. These group norms and the values associated with them can shape members' privacy preferences and may influence individuals' privacy management practices and decisions [10].

Privacy management, in this context, involves considering what information to disclose and how it aligns with individuals' social identity and desired impression. Users may employ privacy settings and controls to manage their self-disclosure and control who can access their shared content. Towards this, self-adaptive privacy measures and techniques have been indicated as an effective approach. Self-adaptive privacy in cloud computing refers to the ability of cloud systems to dynamically adjust privacy measures based on specific requirements and preferences of individual users or organizations. It involves tailoring privacy controls, mechanisms, and policies to meet the unique privacy needs of different users and data types [11]. In this regard, self-adaptive privacy aims at empowering users by giving them greater control over their privacy. It provides users with visibility into how their data is being handled within the cloud, offering transparency into privacy practices, and enabling informed decision-making [12]. Considering that privacy management is changing based on users' social groups, several social factors and attributes play a significant role in self-adaptive privacy approaches. These factors influence the design, implementation, and acceptance of self-adaptive privacy mechanisms and practices. Thus, as previous research indicates, these factors are usually hard to be identified or are neglected during systems' design [13]. Recent studies have focused on developing algorithmic implementations of such self-privacy adaptation methods that pay attention to users' individual attributes or context [14], [15] and not on groups' norms, while other work concentrates on the user interface mechanism to adopt such adaptations in order to be protected [16].

Therefore, individuals' social attributes should be examined in relation to their social group's belonging [1]. Thus, in this paper, we aim to identify more determinants, based on each social group, of privacy management practices within the cloud. To gather the required data, a survey was conducted among the students of three Universities in Greece, England, and Spain. The findings from this study contribute to valuable insights regarding users' privacy practices based on their belonging to a group and provide important information for the design of usable and self-adaptive privacy features within the cloud, since they promote specific privacy requirements based on users' social identity and groups, considering adaptation on a basis of group privacy management. Section II presents the research field, the methodology followed, and the implemented instrument. In Section III, the results of our survey are outlined, indicating users' privacy management practices. Section IV discusses and concludes the main findings, raising future research directions and practical implications.

## II. Methodology

Supporting the arguments above suggesting that social identity pertains to how individuals shape their attitudes and behaviors within various domains of activity [6], the following foundational research question has been formulated to guide our study: RQ *"Is belonging in a social group affecting users' privacy management?"*. To address that, the research population selected for this study included the students of three Universities in Greece, England, and Spain: University of the Aegean, University of Bournemouth, and University of Malaga, respectively. The survey was administered to undergraduate, postgraduate, and doctoral students. Due to its diverse nature in terms of geographical location and demographics, the research population holds significant potential for providing respected insights regarding users' disclosure practices within cloud-based services. It focuses on the domain of social media as the aforementioned cloud environments have been pointed out in the study as the handiest in users' everyday online practices. To ensure access to a substantial portion of the research population and facilitate the generalizability of results [17], a quantitative approach was chosen, and a structured questionnaire was developed. The researchers opted for the Hellenic Statistical Authority's categorizations when determining the values for measuring users' socio-demographics across their survey in order to ensure reliability, representativeness, and transparency. 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 Cloud Services. All items were compiled from previous literature and, in particular, participants were asked to identify the groups to which they belong within cloud services using a social identity taxonomy that aligns with the work of [18]. This taxonomy encompassed a range of group categories, including 15 types of groups, such as leisure groups, well-being groups, professional groups, and other user-indicated groups. 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, such as privacy concerns, privacy risks, and privacy behaviors, it was important these measures to be incorporated in our instrument. Furthermore, the nature of self-disclosure on cloud services raises privacy concerns, as individuals need to consider the potential risks associated with sharing of personal information publicly. Respectively the variety of attitudes within cloud services concerns privacy as well, such as prioritizing the protection of personal information or embracing a more open approach. Therefore, the questionnaire that was developed for the data collection, included wider sections, concerning users' social identity, users' self-disclosure and privacy management, along with their respective items. For example, in order to ensure the reliability and validity of our instrument, a comprehensive review of the literature for self-presentation and self-disclosure practices was conducted. This review allowed us to incorporate validated metrics from previous studies [19]–[22] on self-presentation and information disclosure into our instrument. These concerned 15 items, as follows: *"I share personal information, I share photos of myself, I share information about my family, I share information about my friends, I share information about my job, I share information about my hobbies, I share information about my daily activities, I share information regarding my sexuality, I share religion-related views, I share information about my political views, I state my location, I update my status, I include contact information (e.g. email, links to other profiles, personal web pages, mobile number, postal address), I have included a short cv in my profile, I tag others in the photos I share"*.

Moreover, the instrument included a set of six questions aiming at capturing participants' socio-demographic characteristics based on previous work [23]. These questions encompassed gender, age, family structure, educational level, professional experience, and monthly income. By incorporating these questions in the final part of the instrument, participants had the time required to complete it more effectively. Prior to distributing the questionnaire to the research population, a pilot study was conducted with a sample of 60 students from the three universities. The purpose of this pilot study was to test the instrument for its form, language, clarity, difficulty level, and responsiveness to respondents' interests, leading to the necessary revisions to the questionnaire items. The survey was conducted using Google Forms, which allowed for direct distribution via email. In the introductory note of the survey, the purpose, procedure, and ethical considerations were clearly explained, adhering to established research ethics and standards [24]. The collected data was then recoded and processed using IBM SPSS Statistics 28 (SPSS28).

## III. Results

Out of the 368 responses received, thorough checks for completeness were performed, resulting in 280 valid responses being included in the analysis. The survey involved more women than men, while a small percentage declared a different gender. Despite the distribution of ages, the majority was in the age group of 18–32. Regarding family structure, the nuclear form dominates, while it is quite interesting that some of the responders preferred not to provide an answer. Most of the participants held a Master's diploma, and 92% of the respondents have professional experience of at least 1–5 years. The majority declared a relatively low monthly income, ranging from 301 to 800€. Participants' individual attributes, presented in detail in Table I, are associated with their level of social capital [25], setting the standard for a better understanding of users' self-categorization procedure in order to formulate their social identity and define their perceptions and willingness to belong to a social group.

TABLE I. Respondents' demographics.

| | *Sample Socio-Demographics* | |
|---|---|---|
| | ***Value*** | ***Percentage%*** |
| ***Gender*** | Male | 37.5% |
| | Female | 61.8% |
| | Other | 0.7% |
| ***Age*** | 18–32 | 58.9% |
| | 33–47 | 28.6% |
| | >48 | 12.1% |
| ***Family Form*** | Nuclear Family | 61.8% |
| | Large Family | 7.5% |
| | Single-Parent Family | 11.8% |
| | Other Form | 9.3% |
| | Prefer not answering | 9.3% |
| ***Educational Level*** | ICD4 | 36.8% |
| | Bachelor | 23.2% |
| | MSc | 35.7% |
| | PhD | 3.6% |
| ***Professional Experience*** | 1 to 5 | 43.6% |
| | 6 to 10 | 17.5% |
| | 11 to 15 | 9.6% |
| | 16 to 20 | 8.9% |
| | 21 to 25 | 6.4% |
| | >26 | 5.7% |
| ***Monthly Income*** | 301–800€ | 40.7% |
| | 801–1000€ | 16.1% |
| | 1001–1500€ | 20.7% |
| | 1501–2000€ | 6.1% |
| | 2001–3000€ | 3.2% |

The findings of our survey indicate that participants declare belonging to various social groups when adopting cloud services, namely: Companionship group (33.9%), Professional group (11.3%), Political group (3.1%), Trade union group (2.4%), Voluntary group (8.1%), Sport group (7.7%), Leisure group (11.7%), Cultural group (5.9%), Human Support group (1.5%), Scientific group (2.9%), Environmental group (2.3%), Mutual Support group (1.1%), Religious group (2.0%), Technological Interest group (3.1%) and Gender equality group (3.2%). Previous research has already suggested that individuals who possess multiple social identities are shaping their behaviors, respectively, within specific contexts [26].

Moreover, in order to check if participation in a specific group is associated to participants' stated reasons for social media and cloud services usage, chi-square test for two nominal variables was used. Statistically significant results are shown in Table II. According to this table, there is an association between the variables of companionship, professional, voluntary, sport, leisure, cultural and scientific groups, and specific reasons of use. In all other cases of groups (political, trade union group, human support, environmental, mutual support, religious, technological interest and gender equality group) no statistically significant results came up. Considering that $\phi_c$ (Phi) takes values between 0 and +/-1, the strength of association of the nominal by nominal relationships is positive in all cases, although low (from 0.129 to 0.166).

The reasons for using social media and cloud services across different social groups are also differentiated. The practice of presenting oneself on platforms like Instagram, Messenger, and Facebook is significantly associated with companionship group. This indicates that individuals may use these platforms to connect with others and establish relationships.

Professionals are more likely to use social media and cloud services for professional activities, as indicated by the statistically significant associations. This suggests that platforms like Google services and WhatsApp may be used for work-related communication and collaboration. Similar to the professional group, individuals interested in sports and scientific activities also tend to use social media and cloud services for professional purposes. Members of voluntary groups show a significant association with using social media and cloud services for professional activities as well. People in leisure groups use social media to seek emotional relationships, partnerships, and job opportunities, serving as avenues for both personal and professional interactions within the leisure context. Individuals interested in cultural activities tend to use them, not only for professional reasons, but also for political activities.

In this regard and in order to check whether participation in a specific social group is associated with specific self-presentation and information disclosure practices, the chi-square test for two nominal dichotomous variables was used. Results are shown in Table III, as follows.

Results show that there are statistically significant associations between the nominal variables of "*group participation*"and "*self-presentation and information disclosure practices*", highlighting that the group in which one chooses to participate is related to the practices that she/he chooses or

TABLE II. SOCIAL GROUPS AND REASONS FOR SOCIAL MEDIA AND CLOUD SERVICES USAGE.

| **Groups** | **Practices** | **Media & Services**<br>***Instagram, Messenger, Facebook, Google services, What's up*** |
|---|---|---|
| **Companionship** | Present myself | $\chi^2(1)$=4.869, $p$=0.027, $\phi_c$=0.133 |
| **Professional** | For professional activities | $\chi^2(1)$=6.936 $p$=0.008, $\phi_c$=0.159 |
| **Sport** | Look for friendships | $\chi^2(1)$=7.589 $p$=0.006, $\phi_c$=0.166 |
| **Scientific** | For professional activities | $\chi^2(1)$=6.235 $p$=0.013, $\phi_c$=0.151 |
| **Voluntary** | For professional activities | $\chi^2(1)$=4.580 $p$=0.032, $\phi_c$=0.129 |
| **Leisure** | Look for emotional relationship | $\chi^2(1)$=4.911 $p$=0.027, $\phi_c$=0.134 |
| | Look for partnerships | $\chi^2(1)$=6.565 $p$=0.010, $\phi_c$=0.155 |
| | Look for job | $\chi^2(1)$=*4.761 p=0.029,* $\phi_c$=*0.132* |
| **Cultural** | For professional activities | $\chi^2(1)$=5.599 $p$=0.018, $\phi_c$=0.143 |
| | For professional activities | $\chi^2(1)$=5.377 $p$=0.020, $\phi_c$=0.140 |

avoids for self-presentation. Most of the associations were revealed for users' self-presentation and information disclosure practices on Messenger (25 associations) and Instagram (22 associations), less on Facebook (15 associations) and few (1-2) on What's Up and Google services. These results are not surprising, considering that the cumulative percent of participants using "once daily"and "several times daily"Messenger, Instagram and Facebook are, according to the results of the research, high (78.3%, 70.2% and 61.9%, respectively).

The majority of associations were positive with the exception of fifteen (15) negative revealed in the case of participating in specific types of groups (mainly trade-union, professional, technological interest, scientific, voluntary, cultural, environmental) and for specific social media, mostly Instagram and less Messenger. Although the negative associations refer to nine (9) different practices, more negative associations were revealed for practices including photos sharing ("I share photos of myself"and "I tag others in the photos I share") and for practices referring to hobbies and daily activities information sharing. This finding implies that the aforementioned practices are considered rather inappropriate by people participating in professional groups or groups that serve specific interests. Moreover, results revealed that those participating in companionship groups use more self-disclosure practices compared to others participating in other type of groups, which is explicable considering the more open goal of participation and the expected benefits from self-disclosure. Results also revealed that the self-presentation practices more used (or avoided) by people according to the type of group they belong, and the media context, were that of sharing information about hobbies (12 associations, 3 of them negative) and photos sharing of oneself (9 associations, 3 of them negative).

TABLE III. SOCIAL GROUPS' SELF-PRESENTATION AND INFORMATION DISCLOSURE PRACTICES.

| **Groups** | **Disclosure Practices** | **Media & Services**<br>***Instagram, Messenger, Facebook, Google services, What's up*** |
|---|---|---|
| **Companionship** | Personal information | ***Messenger:***<br>$\chi^2(1)$=6.844, $p$=0.009, $\phi_c$=0.157 |
| | Photos of myself | ***Instagram:***<br>$\chi^2(1)$=11.024, $p$=0.001, $\phi_c$=0.200 |
| | | ***Messenger:***<br>$\chi^2(1)$=6.517, $p$=0.011, $\phi_c$=0.154 |
| | About my friends | ***Messenger:***<br>$\chi^2(1)$=3.957, $p$=0.047, $\phi_c$=0.120 |
| | About my job | ***Messenger:***<br>$\chi^2(1)$=5.227, $p$=0.022, $\phi_c$=0.138 |
| | About my hobbies | ***Instagram:***<br>$\chi^2(1)$=10.663, $p$=0.001, $\phi_c$=0.197 |
| | | ***Messenger:***<br>$\chi^2(1)$=5.632, $p$=0.018, $\phi_c$=0.143 |
| | About my daily activities | ***Instagram:***<br>$\chi^2(1)$=10.115, $p$=0.001, $\phi_c$=0.191 |
| | | ***Messenger:***<br>$\chi^2(1)$=6.479, $p$=0.011, $\phi_c$=0.153 |
| | My location | ***Instagram:***<br>$\chi^2(1)$=4.082, $p$=0.043, $\phi_c$=0.122 |
| | I tag others in the photos I share | ***Instagram:***<br>$\chi^2(1)$=5.520, $p$=0.019, $\phi_c$=0.141 |
| **Professional** | About my job | ***Messenger:***<br>$\chi^2(1)$=7.917, $p$=0.005, $\phi_c$=0.169 |
| | Religious views | ***Messenger:***<br>$\chi^2(1)$=5.553, $p$=0.018, $\phi_c$=-0.142 |
| | A short cv in my profile | ***Instagram:***<br>$\chi^2(1)$=5.470, $p$=0.019, $\phi_c$=-0.141 |
| | I tag others in the photos I share | ***Instagram:***<br>$\chi^2(1)$=5.549, $p$=.018, $\phi_c$=-0.142 |
| **Political** | About my family | ***Messenger:***<br>$\chi^2(1)$=4.953, $p$=0.026, $\phi_c$=0.134 |
| | About my friends | ***Facebook:***<br>$\chi^2(1)$=3.936, $p$=0.047, $\phi_c$=0.119 |
| | About my job | ***Messenger:***<br>$\chi^2(1)$=6.415, $p$=0.011, $\phi_c$=0.152 |
| | About my hobbies | ***Facebook:***<br>$\chi^2(1)$=8.561, $p$=0.003, $\phi_c$=0.176 |
| | I tag others in the photos I share | ***Facebook:***<br>$\chi^2(1)$=7.527, $p$=0.006, $\phi_c$=0.165 |
| **Technological Interest** | Photos of myself | ***Instagram:***<br>$\chi^2(1)$=8.102, $p$=0.004, $\phi_c$=-0.171 |
| | About my hobbies | ***Instagram:***<br>$\chi^2(1)$=4.825, $p$=0.028, $\phi_c$=-0.132 |
| | About my daily activities | ***Instagram:***<br>$\chi^2(1)$=5.751, $p$=0.016, $\phi_c$=-0.144 |

*Continues...*

Furthermore, in order to check if participating in a specific group relates to perceptions about beliefs in privacy rights, privacy concerns, comfortability with information collection, privacy control, attitude towards collaborative privacy management and self-disclosure cost-benefit evaluation, a Mann-Whitney test for to independent samples (those participating in a group vsthose not participating) was used. Kolmogorov-Smirnov test of normality firstly applied didn't show normal distribution for these variables, which is a prerequisite for using a T-test. To run the Mann-Whitney test the total score of the statements included in the variables above has been calculated. The results of Mann Whitney tests are shown in Table IV, revealing statistically significant differences ($p$ <0.05) between those who declared their participation into some of the groups.

Results revealed significant differences in several aspects of privacy-related perceptions among participants in different groups compared to non-participants. Firstly, individuals who participated in the Companionship group exhibited statistically significant differences in their perceptions of privacy control compared to non-participants. Similarly, participants in the Political group showed significant differences in privacy control compared to those not in the group. Moreover, both the Companionship and Political groups displayed significant differences in collaborative privacy management compared to non-participants. This suggests that group participation influences individuals' attitudes towards managing privacy collaboratively. Additionally, individuals associated with the Trade Union group showed significantly different perceptions of privacy control compared to non-participants. In terms of specific interest groups, participants in the Sport group displayed significant differences in collaborative privacy management compared to non-participants. Similarly, individuals in the Cultural group exhibited significant differences in their approach to collaborative privacy management. Lastly, participants in the Gender Equality group had significantly different beliefs in privacy rights compared to non-participants. Furthermore, participants in sport groups overall had significantly different self-disclosure cost-benefit evaluations compared to non-ones.

In order to check also if participation in a group is related to self-protection strategies, chi-square test for two nominal variables was again used. Results are shown in Table V. As revealed there is an association between the variables of companionship, professional, voluntary, leisure, scientific, environmental, religious, technological interest and gender equality group, and specific self-protection strategies. In all other cases of groups (political, trade union group, sport, cultural, human support and mutual support) no statistically significant results came up. The strength of association of the nominal by nominal relationships is positive in 8 cases and negative in 7 (marked in Italics), but low in all cases.

Results indicate that individuals who often adjust their privacy settings are more likely to belong to social groups centered around companionship. This indicates a proactive approach to managing privacy concerns within this context. Participants who do not restrict access to the content they upload are associated with professional social groups. This suggests

TABLE III. SOCIAL GROUPS' SELF-PRESENTATION AND INFORMATION DISCLOSURE PRACTICES (CONT.).

| Groups | Disclosure Practices | Media & Services<br>*Instagram, Messenger, Facebook, Google services, What's up* |
|---|---|---|
| **Trade Union** | Photos of myself | ***Instagram:***<br>$\chi^2(1)$=4.502, $p$=0.034, $\phi_c$=-0.128 |
| | About my hobbies | ***Facebook:***<br>$\chi^2(1)$=6.686, $p$=0.010, $\phi_c$=0.156 |
| | | ***Instagram:***<br>$\chi^2(1)$=5.633, $p$=0.018, $\phi_c$=-0.143 |
| | My location | ***Instagram:***<br>$\chi^2(1)$=7.107, $p$=0.008, $\phi_c$=-0.160 |
| | I tag others in the photos I share | ***Instagram:***<br>$\chi^2(1)$=8.209, $p$=0.004, $\phi_c$=-0.172 |
| **Gender equality** | Personal information | ***Messenger:***<br>$\chi^2(1)$=4.871, $p$=0.027, $\phi_c$=0.133 |
| | About my family | ***Messenger:***<br>$\chi^2(1)$=15.645, $p$=0.000, $\phi_c$=0.238 |
| | About my friends | ***Messenger:***<br>$\chi^2(1)$=9.468, $p$=0.002, $\phi_c$=0.185 |
| | About my daily activities | ***Messenger:***<br>$\chi^2(1)$=5.639, $p$=0.018, $\phi_c$=0.143 |
| | Contact information | ***Facebook:***<br>$\chi^2(1)$=5.563, $p$=0.018, $\phi_c$=0.142 |
| **Religious** | Information about my hobbies | ***Facebook:***<br>$\chi^2(1)$=5.076, $p$=0.024, $\phi_c$=0.136 |
| **Voluntary** | Photos of myself | ***Instagram:***<br>$\chi^2(1)$=4.410, $p$=0.036, $\phi_c$=-0.126 |
| | | ***What's up:***<br>$\chi^2(1)$=4.226, $p$=0.040, $\phi_c$=0.124 |
| | About my job | ***Facebook:***<br>$\chi^2(1)$=8.503, $p$=0.004, $\phi_c$=0.176 |
| | About my hobbies | ***Messenger:***<br>$\chi^2(1)$=4.735 $p$=0.030, $\phi_c$=0.131 |
| | My daily activities | ***Facebook:***<br>$\chi^2(1)$=4.720, $p$=0.030, $\phi_c$=0.131 |
| | Contact information | ***Google services:***<br>$\chi^2(1)$=3.878, $p$=0.049, $\phi_c$=0.119 |
| | I tag others in the photos I share | ***Facebook:***<br>$\chi^2(1)$=4.268, $p$=0.039, $\phi_c$=0.124 |
| **Scientific** | About my job | ***Facebook:***<br>$\chi^2(1)$=9.700, $p$=0.002, $\phi_c$=0.187 |
| | About my hobbies | ***Instagram:***<br>$\chi^2(1)$=4.189, $p$=0.041, $\phi_c$=-0.123 |
| | About my daily activities | ***Messenger:***<br>$\chi^2(1)$=4.597, $p$=0.032, $\phi_c$=-0.129 |

*Continues...*

TABLE III. Social Groups' Self-Presentation and Information Disclosure Practices (cont.).

| Groups | Disclosure Practices | Media & Services<br>*Instagram, Messenger, Facebook, Google services, What's up* |
|---|---|---|
| **Sport** | Personal information | ***Messenger:***<br>$\chi^2(1)$=4.467, $p$=0.035, $\phi_c$=0.127 |
| | About my friends | ***Instagram:***<br>$\chi^2(1)$=4.484, $p$=0.034, $\phi_c$=0.127 |
| | About my hobbies | ***Facebook:***<br>$\chi^2(1)$=5.774, $p$=0.016, $\phi_c$=0.145 |
| | | ***Instagram:***<br>$\chi^2(1)$=8.501, $p$=0.004, $\phi_c$=0.175 |
| | My daily activities | ***Messenger:***<br>$\chi^2(1)$=5.480, $p$=0.019, $\phi_c$=0.141 |
| | My location | ***Instagram:***<br>$\chi^2(1)$=6.245, $p$=0.012, $\phi_c$=0.150 |
| | I tag others in the photos I share | ***Instagram:***<br>$\chi^2(1)$=4.086, $p$=0.043, $\phi_c$=0.122 |
| **Leisure** | Personal information | ***Google services:***<br>$\chi^2(1)$=3.972, $p$=0.046, $\phi_c$=0.120 |
| | Photos of myself | ***Facebook:***<br>$\chi^2(1)$=4.667, $p$=0.031, $\phi_c$=0.130 |
| | | ***Instagram:***<br>$\chi^2(1)$=4.730, $p$=0.030, $\phi_c$=0.131 |
| | About my hobbies | ***Facebook:***<br>$\chi^2(1)$=7.015, $p$=0.008, $\phi_c$=0.159 |
| | I update my status | ***Facebook:***<br>$\chi^2(1)$=4.634, $p$=0.031, $\phi_c$=0.130 |
| **Cultural** | About my family | ***Messenger:***<br>$\chi^2(1)$=4.405, $p$=.0036, $\phi_c$=0.126 |
| | About my sexuality | ***Messenger:***<br>$\chi^2(1)$=11.908, $p$=0.001, $\phi_c$=0.208 |
| | Religious views | ***Messenger:***<br>$\chi^2(1)$=9.344, $p$=0.002, $\phi_c$=0.184 |
| | About my political views | ***Messenger:***<br>$\chi^2(1)$=8.041, $p$=0.005, $\phi_c$=0.171 |
| | My location | ***Messenger:***<br>$\chi^2(1)$=8.671, $p$=0.003, $\phi_c$=0.177 |
| | Contact information | ***Instagram:***<br>$\chi^2(1)$=3.863, $p$=0.049, $\phi_c$=-0.118 |
| | | ***Messenger:***<br>$\chi^2(1)$=3.888, $p$=0.049, $\phi_c$=0.119 |
| **Environmental** | Personal information | ***Messenger:***<br>$\chi^2(1)$=4.182, $p$=0.041, $\phi_c$=-0.123 |
| **Human Support** | Photos of myself | ***Facebook:***<br>$\chi^2(1)$=7.492, $p$=0.007, $\phi_c$=0.164 |

a willingness to share professional information openly. Those who do not accept friendship requests from strangers are more likely to belong to groups advocating for gender equality. This behavior aligns with cautious online practices regarding social connections. Individuals familiar with platform mechanisms for self-protection tend to belong to religious groups. This indicates a sense of awareness and possibly guidance within religious communities regarding online safety. Members who have left privacy settings at default are linked to voluntary groups. This suggests a lack of awareness or concern about privacy implications within this group. Changing initial privacy settings and adjusting them frequently are common practices among individuals in leisure-oriented groups. Additionally, they tend to consider contextual factors when sharing information, reflecting a balanced approach to privacy management. Moreover, changing initial privacy settings and using limited profile options are prevalent among individuals in scientific groups. This indicates a proactive stance towards safeguarding privacy, possibly influenced by professional or research-related considerations. Usage of limited profile options is associated with environmental groups, suggesting a conscious effort to control the visibility of personal information. Finally, those who frequently adjust privacy settings often belong to groups interested in technology. This behavior may stem from a deeper understanding of online privacy risks and a proactive approach to mitigating them.

## IV. Discussion and Conclusion

Our analysis highlights the diverse motivations driving the use of social media and cloud services across different social groups, ranging from personal connections and professional networking to cultural interests and political activities. These findings underscore the multifaceted nature of online engagement and the varying needs of different user demographics. The results suggest that group participation influences various aspects of individuals' perceptions and behaviors related to privacy. Depending on the specific group, individuals may exhibit different attitudes towards privacy control, collaborative privacy management, beliefs in privacy rights, and self-disclosure -cost-benefit evaluation. These findings highlight the importance of considering group dynamics when examining privacy-related behaviors in social contexts. The findings also underscore the influence of group participation on individuals' perceptions and behaviors related to privacy and self-disclosure. As the findings above indicate, social belonging in a group affects users' self-disclosure practices and, respectively, influences their privacy preferences. Self-disclosure on cloud services contributes to users' digital footprints, leaving a trace of their activities, interests, and interactions [27]. Thus, findings highlighted that users who share a similar social identity based on companionship, feel more comfortable disclosing personal information and photos within cloud services and particularly within social media. However, other users emphasizing certain aspects of their identity, mostly the professional based ones, and downplaying the others, declared to be mindful of their social identity presentation and self-disclosure on social media, considering

TABLE IV. SOCIAL GROUPS' PRIVACY ATTITUDES.

| Variables/Groups | Companionship | Political | Trade union | Sport | Cultural | Environmental | Gender equality |
|---|---|---|---|---|---|---|---|
| **Privacy Control** | $U$=1715.000<br>$p$=0.006 | $U$=2033.500<br>$p$=0.016 | $U$=1491.000<br>$p$=0.009 | | | | |
| **Collaborative Privacy Management** | $U$=1542.000<br>$p$=0.001 | $U$=1828.000<br>$p$=0.003 | | | $U$=4111.000<br>$p$=0.039 | $U$=1573.000<br>$p$=0.047 | |
| **Beliefs In Privacy Rights** | | | $U$=1591.000<br>$p$=0.023 | | | | |
| **Self Disclosure Cost Benefit** | | | | $U$=5190.000<br>$p$=0.034 | | | |

the potential consequences and impacts on their privacy, well-being, and relationships. Evidently, previous research has shown that this digital footprint can have implications for reputation management, online perception, and potential consequences in both personal and professional contexts [28]. What is more the analysis highlights how self-protection strategies vary across different social groups, reflecting varying levels of awareness, concern, and proactive behavior regarding online privacy and security.

In this regard, the identification of social groups' privacy management practices on the cloud can have a significant impact on the design and implementation of self-adaptive privacy schemes, in order for users to be aware of privacy settings, critically evaluate the information shared, and maintain a balance between online and offline identities which can contribute to a more positive and authentic online presence. Considering that social groups' norms serve as guidelines for users and societies to navigate privacy boundaries and expectations, contributing to the preservation of personal autonomy, dignity, and trust [29], the identification of the practices that lead to specific group-based needs is of great importance. Since self-adaptive privacy in cloud services seeks to strike a balance between data utility and privacy protection, by tailoring privacy measures to users' needs and dynamically adapting to changing circumstances [30], users' empowerment can be enhanced when self- adaptive privacy schemes from the beginning of the design take into account groups preferences and the balance between maintaining privacy and participating in social interactions within one's social identity networks. Furthermore, incorporating the understanding of social groups' privacy management practices into the concept of "privacy by design"methodologies, such as the extended PriS framework for cloud computing services [31] that should be used for designing self-adaptive privacy schemes, can help ensure that privacy considerations are embedded in the development process of cloud services.

Despite the limitations of our survey, concerning the weak strength of association of the nominal-by-nominal relationships ($\phi$ coefficient takes values between $0$ and $+/-1$), our results indicate the diversity of privacy management practices across different social groups, providing a guide for specific social requirements that could be integrated from the initial design stages of self-adaptive privacy schemes. It is indicated that the users within Cloud exhibit several key characteristics. Firstly, they are heterogeneous, representing diverse social identities that reflect both their individual norms and their interactions within social networks. Secondly, they are socially interrelated, as they share personal information to gain symbolic benefits and resources from their online networks. Thirdly, they prioritize privacy, holding privacy rights in high regard and expressing significant concerns about privacy when using the services. Despite this, they have a limited level of trust regarding the use of their personal information. Lastly, they demonstrate collaborative behavior, co-managing their personal information with other users and sometimes sharing information about others without their explicit consent.

In this respect, the defining of the privacy management practices can influence the establishment of privacy defaults in cloud platforms. Therefore, the identification of specific social privacy related requirements are presented in the following tables and figure as follows:

Based on the significant associations between group participation and reasons for social media and cloud services usage presented, the social requirements for privacy protection can be identified, as presented in Table VI.

These requirements underscore the importance of context-specific privacy protections that accommodate the diverse reasons for social media and cloud services usage within different groups, ensuring that users can engage in various activities while maintaining control over their personal information. In Figure **??**, the self-disclosure practices are visualized by group and cloud service, aiming to aid the self-adaptive privacy schemes designed to be aligned with the preferences of social groups by setting initial privacy defaults that reflect their common practices and expectations.

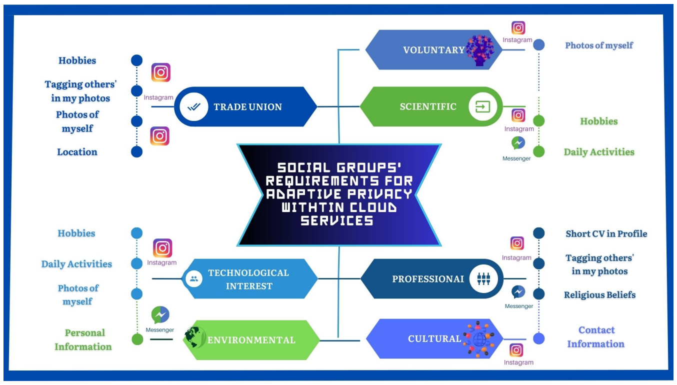

Figure 1. Social Requirements for Self-Adaptive Privacy Schemes in Cloud based on Social Groups' self disclosure practices.

Furthermore, considering that privacy control, collabora-

TABLE V. SOCIAL GROUPS' SELF-PROTECTION STRATEGIES.

| Groups | Practices | Media & Services<br>*Instagram, Messenger, Facebook, Google services, What's up* |
|---|---|---|
| **Companionship** | Often adjust privacy settings | $\chi^2(1)$=6.498, $p$=0.011, $\phi_c$=-0.155 |
| **Professional** | Do not restrict access to the content I upload | $\chi^2(1)$=4.833, $p$=0.028, $\phi_c$=-0.133 |
| **Gender equality** | Do not accept friendship requests from strangers | $\chi^2(1)$=9.079, $p$=0.003, $\phi_c$=-0.182 |
| | Untag myself from others' photos | $\chi^2(1)$=3.921, $p$=0.048, $\phi_c$=0.120 |
| **Religious** | Familiar with the mechanisms provided by the platform to protect myself | $\chi^2(1)$=4.732, $p$=0.030, $\phi_c$=0.132 |
| **Voluntary** | Have let privacy settings at default | $\chi^2(1)$=4.166, $p$=0.041, $\phi_c$=0.124 |
| | Untag myself from others' photos | $\chi^2(1)$=6.121, $p$=0.013, $\phi_c$=-0.150 |
| **Leisure** | Have changed initial privacy settings | $\chi^2(1)$=5.876, $p$=0.015, $\phi_c$=0.147 |
| | Often adjust privacy settings | $\chi^2(1)$=4.881, $p$=0.027, $\phi_c$=0.134 |
| | Carefully consider the context (where am I) when I provide information | $\chi^2(1)$=5.940, $p$=0.015, $\phi_c$=0.148 |
| **Scientific** | Have changed initial privacy settings | $\chi^2(1)$=4.947, $p$=0.026, $\phi_c$=-0.135 |
| | Use a limited profile option | $\chi^2(1)$=5.420, $p$=0.020, $\phi_c$=-0.141 |
| | Have excluded contact information from my profile | $\chi^2(1)$=5.200, $p$=0.023, $\phi_c$=-0.138 |
| **Environmental** | Use a limited profile option | $\chi^2(1)$=3.865, $p$=0.049, $\phi_c$=0.119 |
| **Technological Interest** | Often adjust privacy settings | $\chi^2(1)$=4.212, $p$=0.040, $\phi_c$=0.124 |

TABLE VI. SOCIAL REQUIREMENTS FOR SELF-ADAPTIVE PRIVACY SCHEMES IN CLOUD BASED ON SOCIAL GROUPS' REASONS FOR USING SOCIAL MEDIA AND CLOUD SERVICES.

| SR | Description |
|---|---|
| SR 1 | Tailor privacy settings and controls to accommodate the diverse reasons for social media and cloud services usage across different groups, ensuring that individuals can present themselves and seek various types of relationships without compromising their privacy. |
| SR 2 | Implement privacy measures that support professional activities on social media platforms, acknowledging the need for privacy while engaging in career-related networking and interactions. |
| SR 3 | Provide privacy features that align with the voluntary nature of group participation, respecting users' autonomy and preferences in sharing information within these contexts. |
| SR 4 | Recognize the privacy needs of individuals engaging in sports-related groups, ensuring that privacy controls enable users to maintain their privacy while participating in sports-related discussions and activities. |
| SR 5 | Develop privacy mechanisms that cater to leisure and cultural group participation, acknowledging the importance of privacy in recreational and cultural exchanges online. |
| SR 6 | Implement privacy measures that support scientific activities and discussions on social media platforms, safeguarding the privacy of individuals engaging in scientific research and collaborations. |

TABLE VII. SOCIAL REQUIREMENTS FOR SELF-ADAPTIVE PRIVACY SCHEMES IN CLOUD BASED ON SOCIAL GROUPS' PRIVACY ATTITUDES.

| SR | Description |
|---|---|
| SR 1 | Implement mechanisms for collaborative privacy management within online groups to empower users in controlling the information they share about others. |
| SR 2 | Cultivate a culture of respect for privacy rights within online groups, emphasizing the importance of privacy and providing education on privacy-related issues. |
| SR 3 | Enhance users' understanding of the importance of privacy control and of costs and benefits of self-disclosure within online communities, to enable informed decision-making regarding personal information sharing. |

tive privacy management, beliefs in privacy rights and self-disclosure cost-benefit evaluation impact on users' disclosure behavior regarding the risks they uptake for themselves and other, as well as that the level of privacy control and collaborative privacy management should be high when participating in social groups in order users to protect themselves and others, we propose the requirements, as presented in Table VII.

Finally, as far as the self-protection strategies concerns, the following requirements are presented in the Table VIII.

Since the insights into social groups' self-disclosure practices can inform the design process, this knowledge can enable in particular the design of contextual privacy settings. These settings can dynamically adjust privacy levels based on the specific context or situation, taking into account groups' preferences in order, for example, to be more restrictive for the information of the professional groups, while more permissive for companionship or leisure groups. Finally, the provided insights into the self-disclosure practices can enhance the transparency and consent mechanisms in the self-adaptive privacy schemes. Users can be provided with clear and understandable information about how their data will be used, shared, and stored on the cloud, allowing them to make informed decisions and providing meaningful consent based on their social group norms. Therefore, users will be provided with control and agency over their information and with respect to their individual privacy preferences, reducing the risk of unintentional oversharing or undersharing.

TABLE VIII. SOCIAL REQUIREMENTS FOR SELF-ADAPTIVE PRIVACY SCHEMES IN CLOUD BASED ON SOCIAL GROUPS' SELF PROTECTION STRATEGIES.

| SR | Description |
|---|---|
| SR 1 | Users participating in companionship groups should be able to easily change their initial privacy settings, ensuring control over their online information. |
| SR 2 | Professionals engaging in online communities should have the ability to adjust privacy settings frequently, allowing them to tailor their online presence according to their professional needs and preferences. |
| SR 3 | Volunteers involved in online platforms should be provided with a limited profile option, empowering them to manage their privacy settings effectively while participating in various activities. |
| SR 4 | Individuals engaging in leisure groups should have the option to untag themselves from others' photos easily, granting them control over their online image and associations. |
| SR 5 | Users interested in scientific communities should be familiar with the mechanisms provided by the platform to protect their privacy, enabling them to make informed decisions about their online activities. |
| SR 6 | Environmental enthusiasts should have the capability to exclude contact information from their profile, safeguarding their privacy while actively participating in environmental initiatives. |
| SR 7 | Participants in religious groups should be empowered to carefully consider the context when providing information online, ensuring that their actions align with their religious beliefs and values. |
| SR 8 | Those with technological interests should be able to avoid accepting friendship requests from strangers, enhancing their online security and privacy. |

## ACKNOWLEDGMENT

H.F.R.I. Hellenic Foundation for Research & Innovation The research project was supported by the Hellenic Foundation for Research and Innovation (H.F.R.I.) under the '2nd Call for H.F.R.I. Research Projects to support Faculty Members & Researchers' (Project Number: 2550).

## REFERENCES

[1] A. Kitsiou, M. Sideri, A.-G. Mavroeidi, K. Vgena, eleni Tzortzaki, M. Pantelelis, S. Simou, and C. Kalloniatis, "Social requirements for designing self-adaptive privacy schemes in cloud," in *The 2023 IARIA Annual Congress on Frontiers in Science, Technology, Services, and Applications*, vol. ISBN:978-1-68558-089-6, IARIA, 2023.

[2] A. Cook, M. Robinson, M. A. Ferrag, L. A. Maglaras, Y. He, K. Jones, and H. Janicke, *Internet of Cloud: Security and Privacy Issues*, pp. 271–301. Springer International Publishing, 2018.

[3] D. Peras and R. Mekovec, "A conceptualization of the privacy concerns of cloud users," *Information & Computer Security*, vol. 30, pp. 653–671, Apr. 2022.

[4] A. Tsouplaki, *Internet of Cloud (IoC): The Need of Raising Privacy and Security Awareness*, pp. 542–550. Springer Nature Switzerland, 2023.

[5] A. Kitsiou, E. Tzortzaki, C. Kalloniatis, and S. Gritzalis, "Chapter 2 - towards an integrated socio-technical approach for designing adaptive privacy aware services in cloud computing," in *Cyber Influence and Cognitive Threats* (V. Benson and J. Mcalaney, eds.), pp. 9–32, Academic Press, 2020.

[6] M. A. Hogg, D. Abrams, and M. B. Brewer, "Social identity: The role of self in group processes and intergroup relations," *Group Processes & Intergroup Relations*, vol. 20, pp. 570–581, Mar. 2017.

[7] H. Erin E., "Self-presentation in social media: Review and research opportunities," *Review of Communication Research*, vol. 9, pp. 80–98, 2021.

[8] K. Vgena, A. Kitsiou, and C. Kalloniatis, "Understanding the role of users' socio-location attributes and their privacy implications on social media," *Information & Computer Security*, vol. 30, pp. 705–729, May 2022.

[9] T. Dienlin, P. K. Masur, and S. Trepte, "A longitudinal analysis of the privacy paradox," *New Media & Society*, vol. 25, pp. 1043–1064, June 2021.

[10] A. Kitsiou, E. Tzortzaki, C. Kalloniatis, and S. Gritzalis, "Identifying privacy related requirements for the design of self-adaptive privacy protections schemes in social networks," *Future Internet*, vol. 13, p. 23, Jan. 2021.

[11] M. Belk, C. Fidas, E. Athanasopoulos, and A. Pitsillides, "Adaptive and personalized privacy and security (apps 2019): Workshop chairs' welcome and organization," in *Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization*, UMAP '19, ACM, June 2019.

[12] B. P. Knijnenburg, "Privacy? I can't even! making a case for user-tailored privacy," *IEEE Security & Privacy*, vol. 15, no. 4, pp. 62–67, 2017.

[13] A. Kitsiou, E. Tzortzaki, C. Kalloniatis, and S. Gritzalis, *Self Adaptive Privacy in Cloud Computing Environments: Identifying the Major Socio-Technical Concepts*, pp. 117–132. Springer International Publishing, 2020.

[14] I. Saini, S. Saad, and A. Jaekel, "A context aware and traffic adaptive privacy scheme in vanets," in *2020 IEEE 3rd Connected and Automated Vehicles Symposium (CAVS)*, IEEE, Nov. 2020.

[15] F. Schaub, B. Könings, and M. Weber, "Context-adaptive privacy: Leveraging context awareness to support privacy decision making," *IEEE Pervasive Computing*, vol. 14, pp. 34–43, Jan. 2015.

[16] M. Namara, H. Sloan, and B. P. Knijnenburg, "The effectiveness of adaptation methods in improving user engagement and privacy protection on social network sites," *Proceedings on Privacy Enhancing Technologies*, vol. 2022, pp. 629–648, Nov. 2021.

[17] M. Chalikias, P. Lalou, and A. Manolesou, "Research methodology and introduction to statistical data analysis via ibm spss statistics," 2016.

[18] S. V. Bentley, K. H. Greenaway, S. A. Haslam, T. Cruwys, N. K. Steffens, C. Haslam, and B. Cull, "Social identity mapping online.," *Journal of Personality and Social Psychology*, vol. 118, pp. 213–241, Feb. 2020.

[19] M. J. Hernandez-Serrano, P. Renés-Arellano, R. Campos Ortuño, and B. González-Larrea, "Privacidad en redes sociales: análisis de los riesgos de auto-representación digital de adolescentes españoles," *Revista Latina de Comunicación Social*, pp. 133–154, Nov. 2021.

[20] M. Aresta, L. Pedro, C. Santos, and A. Moreira, "Portraying the self in online contexts: context-driven and user-driven online identity profiles," *Contemporary Social Science*, vol. 10, pp. 70–85, Jan. 2015.

[21] K. Vgena, A. Kitsiou, C. Kalloniatis, and S. Gritzalis, "Determining the role of social identity attributes to the protection of users' privacy in social media," *Future Internet*, vol. 14, p. 249, Aug. 2022.

[22] Z. Jordán-Conde, B. Mennecke, and A. Townsend, "Late adolescent identity definition and intimate disclosure on facebook," *Computers in Human Behavior*, vol. 33, pp. 356–366, Apr. 2014.

[23] A. Kitsiou, E. Tzortzaki, C. Kalloniatis, and S. Gritzalis, *Measuring Users' Socio-contextual Attributes for Self-adaptive Privacy Within Cloud-Computing Environments*, pp. 140–155. Springer International Publishing, 2020.

[24] E. R. Babbie, *The Practice of Social Research*. Boston, MA: Cengage, fifteenth ed., 2021.

[25] P. Bourdieu, *The Forms of Capital*, ch. 15, pp. 241–258. New York, USA: Greenwood, 1986.

[26] R. Jenkins, *Social Identity*. Routledge/Taylor and Francis Group, May 2008.

[27] N. Ní Bhroin, T. Dinh, K. Thiel, C. Lampert, E. Staksrud, and K. Ólafsson, "The privacy paradox by proxy: Considering predictors of sharenting," *Media and Communication*, vol. 10, pp. 371–383, Mar. 2022.

[28] K. Feher, "Digital identity and the online self: Footprint strategies – an exploratory and comparative research study," *Journal of Information Science*, vol. 47, pp. 192–205, Oct. 2019.

[29] S. Gritzalis, M. Sideri, A. Kitsiou, E. Tzortzaki, and C. Kalloniatis, *Sustaining Social Cohesion in Information and Knowledge Society: The Priceless Value of Privacy*, pp. 177–198. Springer International Publishing, June 2020.

[30] A. Kitsiou, M. Pantelelis, A.-G. Mavroeidi, M. Sideri, S. Simou, A. Vgena, E. Tzortzaki, and C. Kalloniatis, "Self-adaptive privacy in cloud computing: An overview under an interdisciplinary spectrum," in

*Proceedings of the 26th Pan-Hellenic Conference on Informatics*, PCI 2022, ACM, Nov. 2022.

[31] C. Kalloniatis, “Incorporating privacy in the design of cloud-based systems: a conceptual meta-model,” *Information & Computer Security*, vol. 25, pp. 614–633, Nov. 2017.