Social Requirements for Designing Self-Adaptive Privacy Schemes in Cloud

The Interrelation of Social Identity with Self Disclosure Practices

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

Abstract— **This paper examines the self-presentation and self-disclosure 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' 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; self-disclosure practices; social requirements.

I. INTRODUCTION

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 [1]. 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 [2]. Organizations and individuals should carefully evaluate their specific requirements and consider the appropriate privacy measures and service-level agreements when adopting cloud services [3]. Towards these requirements and measures, the notion of social identity has been indicated as an important factor that influences individuals' privacy preferences and concerns [4]. 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 [5]. 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 [6]. Different social groups may have varying attitudes towards self-presentation and self-disclosure practices [7]. 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 [8]. 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 [9].

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 [10]. 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 [11]. 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 [12]. Recent studies have focused on developing algorithmic implementations of such self-privacy adaptation methods that pay attention to users' individual attributes or context [13][14] and not on groups' norms, while other work concentrates on the user interface mechanism to adopt such adaptations in order to be protected [15].

Therefore, supporting that not only individuals' social attributes should be examined but social groups as well, this paper examines critical issues about users' social groups within cloud services related to their self-presentation and self-disclosure practices. Specifically, we aim to identify relevant determinants, based on each social group, of self-disclosure 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' 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' self-presentation and self-disclosure 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 [5], the following foundational research question has been formulated to guide our study: RQ *"Is belonging in a social group affecting users' self-presentation and self-disclosure practices?"* 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 [16], 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. 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 [17]. 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. 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 [18] - [21] 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 [22]. 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 [23]. 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 the following Table 1, are associated with their level of social capital [24], 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: Companionships 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%), 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 [25]. 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 2, as follows.

TABLE II. SOCIAL GROUPS' DISCLOSURE PRACTICES

SELF-PRESENTATION AND INFORMATION DISCLOSURE		
Groups	***Disclosure Practices***	**Media & Services** ***Instagram, Messenger, Facebook Google services, What's up***
Companion-ship	personal information	***Messenger:*** $X^2(1) =6.844, p=0.009, \varphi_c = 0.157$
	photos of myself	***Instagram:*** $X^2(1) =11.024, p=0.001, \varphi_c = 0.200$
		Messenger: $X^2(1) =6.517, p=0.011, \varphi_c = 0.154$
	about my friends	***Messenger:*** $X^2(1) =3.957, p=0.047, \varphi_c = 0.120$
	about my job	***Messenger:*** $X^2(1) =5.227, p=0.022, \varphi_c = 0.138$
	about my hobbies	***Instagram:*** $X^2(1) =10.663, p=0.001, \varphi_c = 0.197$
		Messenger: $X^2(1) =5.632, p=0.018, \varphi_c = 0.143$
	about my daily activities	***Instagram:*** $X^2(1) =10.115, p=0.001, \varphi_c = 0.191$
		Messenger: $X^2(1) =6.479, p=0.011, \varphi_c = 0.153$
	my location	***Instagram:*** $X^2(1) =4.082, p=0.043, \varphi_c = 0.122$
	I tag others in the photos I share	***Instagram:*** $X^2(1) =5.520, p=0.019, \varphi_c = 0.141$
Professional	about my job	***Messenger:*** $X^2(1) =7.917, p=0.005, \varphi_c = 0.169$
	religious views	***Messenger:*** $X^2(1) =5.553, p=0.018, \varphi_c = -0.142$
	a short cv in my profile	***Instagram:*** $X^2(1) =5.470, p=0.019, \varphi_c = - 0.141$
	I tag others in the photos I share	***Instagram:*** $X^2(1) =5.549, p=.018, \varphi_c = -0.142$
Political	about my family	***Messenger:*** $X^2(1) =4.953, p=0.026, \varphi_c = 0.134$
	about my friends	***Facebook:*** $X^2(1) =3.936, p=0.047, \varphi_c = 0.119$
	about my job	***Messenger:*** $X^2(1) =6.415, p=0.011, \varphi_c = 0.152$
	about my hobbies	***Facebook:*** $X^2(1) =8.561, p=0.003, \varphi_c = 0.176$
	I tag others in the photos I share	***Facebook:*** $X^2(1) =7.527, p=0.006, \varphi_c = 0.165$
Trade union	photos of myself	***Instagram:*** $X^2(1) =4.502, p=0.034, \varphi_c = -0.128$
	about my hobbies	***Facebook:*** $X^2(1) =6.686, p=0.010, \varphi_c = 0.156$
		Instagram: $X^2(1) =5.633, p=0.018, \varphi_c = -0.143$
	my location	***Instagram:*** $X^2(1) =7.107, p=0.008, \varphi_c = -0.160$

SELF-PRESENTATION AND INFORMATION DISCLOSURE		
Groups	***Disclosure Practices***	**Media & Services** ***Instagram, Messenger, Facebook Google services, What's up***
	I tag others in the photos I share	***Instagram:*** $X^2(1)$ =8.209, p=0.004, φ_c = -0.172
Gender equality	personal information	***Messenger:*** $X^2(1)$ =4.871, p=0.027, φ_c = 0.133
	about my family	***Messenger:*** $X^2(1)$ =15.645, p=0.000, φ_c = 0.238
	about my friends	***Messenger:*** $X^2(1)$ =9.468, p=0.002, φ_c = 0.185
	about my daily activities	***Messenger:*** $X^2(1)$ =5.639, p=0.018, φ_c = 0.143
	contact information	***Facebook:*** $X^2(1)$ =5.563, p=0.018, φ_c = 0.142
Religious	information about my hobbies	***Facebook:*** $X^2(1)$ =5.076, p=0.024, φ_c = 0.136
Voluntary	photos of myself	***Instagram:*** $X^2(1)$ =4.410, p=0.036, φ_c = -0.126
		What's up: $X^2(1)$ =4.226, p=0.040, φ_c = 0.124
	about my job	***Facebook:*** $X^2(1)$ =8.503, p=0.004, φ_c = 0.176
	about my hobbies	***Messenger:*** $X^2(1)$ =4.735 p=0.030, φ_c = 0.131
	my daily activities	***Facebook:*** $X^2(1)$ =4.720, p=0.030, φ_c = 0.131
	contact information	***Google services:*** $X^2(1)$ =3.878, p=0.049, φ_c = 0.119
	I tag others in the photos I share	***Facebook:*** $X^2(1)$ =4.268, p=0.039, φ_c =0.124
Sport	personal information	***Messenger:*** $X^2(1)$ =4.467, p=0.035, φ_c = 0.127
	about my friends	***Instagram:*** $X^2(1)$ =4.484, p=0.034, φ_c = 0.127
	about my hobbies	***Facebook:*** $X^2(1)$ =5.774, p=0.016, φ_c = 0.145
		Instagram: $X^2(1)$ =8.501, p=0.004, φ_c = 0.175
	my daily activities	***Messenger:*** $X^2(1)$ =5.480, p=0.019, φ_c = 0.141
	my location	***Instagram:*** $X^2(1)$ =6.245, p=0.012, φ_c = 0.150
	I tag others in the photos I share	***Instagram:*** $X^2(1)$ =4.086, p=0.043, φ_c =0.122
Leisure	personal information	***Google services:*** $X^2(1)$ =3.972, p=0.046, φ_c = 0.120
	photos of myself	***Facebook:*** $X^2(1)$ =4.667, p=0.031, φ_c = 0.130
		Instagram: $X^2(1)$ =4.730, p=0.030, φ_c = 0.131
	about my hobbies	***Facebook:*** $X^2(1)$ =7.015, p=0.008, φ_c = 0.159
	I update my status	***Facebook:*** $X^2(1)$ =4.634, p=0.031, φ_c = 0.130
Cultural	about my family	***Messenger:*** $X^2(1)$ =4.405, p=.0036, φ_c = 0.126
	about my sexuality	***Messenger:*** $X^2(1)$ =11.908, p=0.001, φ_c = 0.208
	religious views	***Messenger:*** $X^2(1)$ =9.344, p=0.002, φ_c = 0.184
	about my political views	***Messenger:*** $X^2(1)$ =8.041, p=0.005, φ_c = 0.171
	my location	***Messenger:*** $X^2(1)$ =8.671, p=0.003, φ_c = 0.177
	contact information	***Instagram:*** $X^2(1)$ =3.863, p=0.049, φ_c = - 0.118
		Messenger: $X^2(1)$ =3.888, p=0.049, φ_c = 0.119
Scientific	about my job	***Facebook:*** $X^2(1)$ =9.700, p=0.002, φ_c = 0.187
	about my hobbies	***Instagram:*** $X^2(1)$ =4.189, p=0.041, φ_c = -0.123
	about my daily activities	***Messenger:*** $X^2(1)$ =4.597, p=0.032, φ_c = -0.129
Environmental	personal information	***Messenger:*** $X^2(1)$ =4.182, p=0.041, φ_c = -0.123
Human Support	photos of myself	***Facebook:*** $X^2(1)$ =7.492, p=0.007, φ_c = 0.164
Technological Interest	photos of myself	***Instagram:*** $X^2(1)$ =8.102, p=0.004, φ_c = -0.171
	about my hobbies	***Instagram:*** $X^2(1)$ =4.825, p=0.028, φ_c = -0.132
	about my daily activities	***Instagram:*** $X^2(1)$ =5.751, p=0.016, φ_c = -0.144

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 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).

IV. DISCUSSION AND CONCLUSION

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 [26]. 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 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 [27]. In this regard, the identification of social groups' self-disclosure 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 [28], 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 [29], 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' self-disclosure practices into the concept of "privacy by design" methodologies, such as the extended PriS framework for cloud computing services [30] 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 self-disclosure 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. In this respect, the defining of the self-disclosure practices can influence the establishment of privacy defaults in cloud platforms. In Figure 1, these 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.

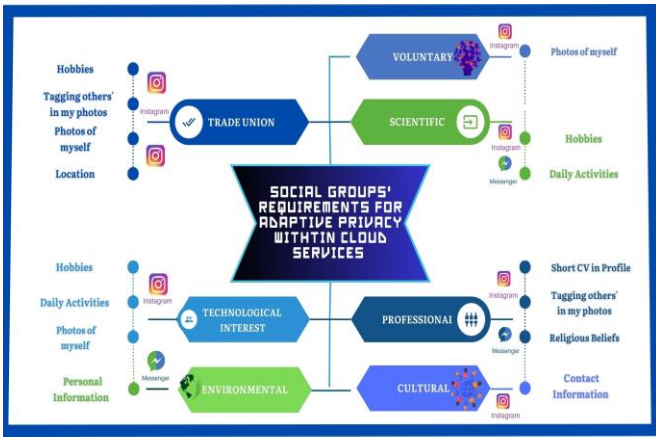

Figure 1. Social Requirements for Self-Adaptive Privacy Schemes in Cloud based on Social Groups' self disclosure practices.

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.

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. Cook et al., "Internet of Cloud: Security and Privacy Issues", in Cloud Computing for Optimization: Foundations, Applications, and Challenges. Studies in Big Data, B. Mishra, H. Das, S. Dehuri and A. Jagadev, Eds., Cham: Springer, pp. 271-301, 2018. doi:10.1007/978-3-319-73676-1_11.

[2] D. Peras and R. Makovec, “A conceptualization of the privacy concerns of cloud users”, Information and Computer Security, vol. 30, no. 5, pp. 653-671, Mar. 2022, doi:10.1108/ICS-11-2021-0182.

[3] A. Tsouplaki, “Internet of Cloud: The Need of Raising Privacy and Security Awareness”, Proc. International Conference on Research Challenges in Information Science, RCIS 2023, Springer , May 2023, pp. 542-550, doi:10.1007/978-3-031-33080-3_36.

[4] A. Kitsiou, E. Tzortzaki, C. Kalloniatis, and S. Gritzalis, “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. Academic Press, pp. 9-32, 2020.

[5] M. Hogg, D. Abrams, and M. Brewer, “Social identity: The role of self in group processes and intergroup relations”, Group Process and Intergroup Relations, vol. 20, no. 5, pp. 570–581, Jan. 2017, doi:10.1177/1368430217690909.

[6] E. E. Hollenbaugh, “Self-presentation in social media: Review and research opportunities”, Review of communication research, vol. 9, pp. 80-98, Jan. 2021, doi: 10.12840/ISSN.2255-4165.027.

[7] K. Vgena, A. Kitsiou, and C. Kalloniatis, “Understanding the role of users’ socio-location attributes and their privacy implications on social media”. Information and Computer Security, vol. 30, no. 5, pp. 705-729, May 2022, doi:10.1108/ICS-12-2021-0211.

[8] T. Dienlin, P. K. Masur, and S. Trepte, “A longitudinal analysis of the privacy paradox”. New Media and Society, vol. 25, no. 5, pp.1043-1064, June 2021, doi:10.1177/14614448211016316.

[9] 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, no. 2, pp. 1-25, Jan. 2021, doi:10.3390/fi13020023.

[10] M. Belk, C. Fidas, E. Athanasopoulos, and A. Pitsillides, “Adaptive and Personalized Privacy and Security (APPS 2019): Workshop Chairs’ Welcome and Organization”. Proc. Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization (UMAP'19 Adjunct), ACM, June 2019, pp. 191–192, doi: 10.1145/3314183.3324963.

[11] B. P. Knijnenburg, “Privacy? I Can’t Even! Making a Case for User-Tailored Privacy”, IEEE Security and Privacy, vol. 15, no.4, pp. 62–67, Jan, 2017, doi:10.1109/MSP.2017.3151331.

[12] A. Kitsiou, E. Tzortzaki, C. Kalloniatis, and S. Gritzalis, “Self Adaptive Privacy in Cloud Computing Environments: Identifying the Major Socio-Technical Concepts”, in Computer Security, S. K. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, Eds. Cham, Switzerland: Springer, pp. 117-132, 2020.

[13] I. Saini, S. Saad and A. Jaekel, “A context aware and traffic adaptive privacy scheme in vanets”. Proc. IEEE 3rd Connected and Automated Vehicles Symposium (CAVS), IEEE, Dec.2020, pp. 1-5, doi: 10.1109/CAVS51000.2020.9334559.

[14] F. Schaub, B. Könings, and M. Weber, “Context-adaptive privacy: Leveraging context awareness to support privacy decision making”, IEEE Pervasive Computing, vol. 14, no. 1, pp. 34–43, Jan - March, 2015, doi:10.1109/MPRV.2015.5.

[15] M. Namara, H. Sloan and B.P. Knijnenburg, The Effectiveness of Adaptation Methods in Improving User Engagement and Privacy Protection on Social Network Sites. [Online]. Available from: https://nru.uncst.go.ug/handle/123456789/4540 [retrieved: 10, 2023].

[16] M. Chalikias, P. Lalou, and A. Manolessou, Research Methodology and Introduction to Statistical Data Analysis via IBM SPSS STATISTICS. [Online]. Available from: https://repository.kallipos.gr/handle/11419/5075 [retrieved: 10, 2023].

[17] S. Bentley et. al., “Social Identity Mapping Online”. J. of Personality and Social Psychology, vol. 118, no. 2, pp. 213-241, Feb. 2020, doi: 10.1037/pspa0000174.

[18] M. J. Hernández-Serrano, P. Renés-Arellano, R. Campos Ortuño, and B. González-Larrea, “Privacy in social networks: analysis of the Spanish teenagers’ digital self-presentation risks”. Revis. Lat. de Comunic. Soc., vol.79, pp. 133-154, Nov. 2021, doi: 10.4185/RLCS-2021-1528.

[19] 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, no.1, pp. 70–85, Jan. 2015, doi:10.1080/21582041.2014.980840.

[20] 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, no. 9, pp. 249-267, Aug. 2022, doi:10.3390/fi14090249.

[21] 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, April 2014, doi:10.1016/j.chb.2013.07.015.

[22] A. Kitsiou, E. Tzortzaki, C. Kalloniatis, and S. Gritzalis, “Measuring Users’ Socio- contextual Attributes for Self-adaptive Privacy Within Cloud-Computing Environments” in Trust, Privacy and Security in Digital Business, S. Gritzalis, E. R. Weippl, G. Kotsis, A. M. Tjoa and I. Khalil Eds. Cham, Switzerland: Springer, pp. 140-155, 2021.

[23] E. R. Babbie, The Practice of Social Research. Hamshire, UK: Cengage Learning, 2021.

[24] P. Bourdieu, “The Forms of Capital” in Handbook of Theory and Research for the Sociology of Education, J. Richardson Ed. New York: Greenwood, pp. 241-258, 1985.

[25] R. Jenkins, Social Identity. London, UK: Routledge/Taylor and Francis Group, 2008.

[26] N. Ní Bhroin et al., “The privacy paradox by proxy: Considering predictors of sharenting”, Media and Communication, vol. 10, no. 1, pp. 371-383, March 2022, doi: 10.17645/mac.v10i1.4858.

[27] K. Feher, “Digital identity and the online self: Footprint strategies–An exploratory and comparative research study”, Journal of information science, vol. 47, no. 2, pp. 192-205, April 2021, doi:10.1177/0165551519879.

[28] S. Gritzalis, M. Sideri, A. Kitsiou, E. Tzortzaki and C. Kalloniatis,“Sustaining Social Cohesion in Information and Knowledge Society: The Priceless Value of Privacy”, in Recent Advances in Core Technologies in Informatics – Selected Papers in Honor of Professor Nikolaos Alexandris, G. Tsihrintzis and M. Virvou Eds. Vol. 14, Springer Learning and Analytics in Intelligent Systems, pp.177 - 198, 2020.

[29] A. Kitsiou et al., “Self-Adaptive Privacy in Cloud Computing: An overview under an interdisciplinary spectrum”. Proc. 26th Pan-Hellenic Conference on Informatics (PCI '22), ACM, Nov. 2022, pp. 64–69, doi: 10.1145/3575879.3575968.

[30] C. Kalloniatis, “Incorporating privacy in the design of cloud-based systems: A conceptual meta-model”, Information and Computer Security, vol. 25, no. 5, pp. 614–633, Nov. 2017, doi:10.1108/ICS-06-2016-0044.