Sustaining Social Cohesion in Information and Knowledge Society: The Priceless Value of Privacy

Gritzalis Stefanos[1], Sideri Maria[2], Kitsiou Angeliki[3], Tzortzaki Eleni[4], Kalloniatis Christos[5]

[1] Professor, Lab. of Systems Security, Dept. of Digital Systems, University of Piraeus, GR 18532, Piraeus, Greece, sgritz@unipi.gr
[2] Laboratory Teaching Staff, Privacy Engineering and Social Informatics Lab., Dept. of Cultural Technology and Communication, University of the Aegean, GR 81100, Lesvos, Greece, msid@aegean.gr
[3] Post-Doc Researcher, Privacy Engineering and Social Informatics Lab., Dept. of Cultural Technology and Communication, University of the Aegean, GR 81100, Lesvos, Greece, a.kitsiou@aegean.gr
[4] PhD Researcher, Lab. of Information and Communication Systems Security, Dept. of Information and Communications Systems Engineering, University of the Aegean, GR 83200, Samos, Greece, etzortzaki@aegean.gr
[5] Associate Professor, Privacy Engineering and Social Informatics Lab., Dept. of Cultural Technology and Communication, University of the Aegean, GR 81100, Lesvos, Greece, chkallon@aegean.gr

ABSTRACT. Within Information and Knowledge Society the concept of Privacy has been enriched including aspects related to digital life, while the right to online Privacy gains more and more attention daily due to several cases of privacy breaches. Privacy is associated with the control, access and use or misuse of personal information by others, including governments, companies and other users as well. Social Network Sites as a part of digital space have altered the way that people communicate and have contributed to the construction of online social networks. During online interaction, users disclose information about them or others, while at the same time they express their concerns about Privacy infringement that may come up due to self-disclosure practices, not restricting or reversing though their disclosure behavior. Thus "Privacy paradox" phenomenon is recorded since users cannot balance between Privacy concerns and their need for disclosure. Privacy's circumvention destabilizes the trust between social actors, increases the feelings of insecurity and puts into risk social cohesion which is a prerequisite for the sustainability of our society. Legislation as well as technology may protect us, but sometimes they are not user friendly and sufficient. Users should protect themselves and other people in order to preserve their Privacy as a fundamental human right. In this paper, based on a literature review, we present the issue of Privacy in Social Network Sites focusing on factors that affect people's Privacy concerns and behavior while relating these to social cohesion.

KEYWORDS: privacy, privacy paradox, privacy protective behavior, Social Network Sites, human rights, social cohesion

1. INTRODUCTION

In 1992, [1] in his book titled "Risk Society: Towards a New Modernity" notes that technology and science within modern societies' development produce new forms of risks unknown in previous ages to which we are constantly required to respond. So, the Risk Society, as described by [1], raises itself the risks that threaten its existence. These risks are not limited to specific forms alone (e.g. environmental) but include a whole series of interrelated changes within contemporary social life (e.g. financial crisis, social inequalities, job insecurity, declining tradition influence, human rights jeopardy). In addition, risks are not restricted to one country only, but affect all countries and all social classes having global consequences. However, risks do not automatically lead to societies' destruction, since [1] incorporates in the concept of risk the ability to predict a future disaster in time, which can lead to the disaster's prevention. Nevertheless, even in this case, deterrence is not definitive, as the globalized post-modern society suffers from four systemic defections that amplify risk reproduction; exceeding limits, weakness in control, inadequate compensation for the damage caused and lack of knowledge and awareness regarding the risks. In this way risks rebound.

In the frame above, the concept of sustainability has emerged in order to address the risks that society produces with reference to physical, social, economic and cultural level. The concept of sustainability has been broadened from its original frame, paying nowadays attention synthetically and simultaneously to all three pillars; economy, environment, society. Referring to the field of society, sustainability includes the proposal and the promise for social cohesion maintenance. Social cohesion as a state expresses the extension and quality regarding relationship intensity between the members of a society, recording the degree of synergy between the social subjects. Synergy leads both to the establishment and strengthening of the social consciousness and its manifestation through expressions of social solidarity.

For better understanding the concept of social cohesion, the study of social networks as multidimensional systems of communication and shaping of human practice and social identity [2] is required. Social networks are related to a person's social relationships, their characteristics and the way that people perceive and evaluate these relationships. Social networks are characterized by their extent, density, bonding, homogeneity, contact frequency between members, duration and reciprocity [3]. The emotional, psychological or financial support that people can acquire through their social networks constitutes the social support. This is linked to factors that affect quality of life, such as life satisfaction and sense of well-being [4], while lack of social support and exclusion from networks are considered to reduce people's abilities to form their social identity, receive emotional support or material help and gain access to services and information [5]. In this respect, people's participation in social networks and human rights' respect within these are prerequisite for achieving and maintaining social cohesion in the frame of social sustainability and development both for the present and the future.

Several evolutions in the Information and Knowledge Society are inextricably linked to the processes of social development. Digital social networks for example

coexist with offline social networks altering contemporary social life. In this frame, Social Networking Sites (SNSs), that have replaced many forms of offline social activities (e.g. communication, leisure activities, services provision) being tools of both private and public communication [6] are a place that intersects public and private practices. Promoting the social interconnection between users, facilitating and encouraging users' communication within and beyond the direct contacts of their networks [7], SNSs constitute, on the one hand, an appropriate field of social development, while on the other hand their usage raises multiple issues regarding human rights both at individual and social level.

The evolutions having taken place within Information and Knowledge Society highlight the necessity for human rights protection at digital level as well [8]. In this frame, the issue of privacy and its protection - not being a new social phenomenon though - takes a foreground place in the scientific community among IT, legal and social scientists, following a multidisciplinary approach. What is private and how private is intertwined with the public is an issue that is rooted in the very beginning of human presence. We should note that the distinction between private and public is related to the social context in which it occurs, underlining though that the social and cultural factors that determine the concept of privacy do not remain stable, altering thus the perceptions regarding private and public. Nevertheless, as noted by [9], after the technological evolution "*the classical concept of privacy has been greatly enriched*" (p. 508). Considering that within Information Society the relationships between the different information managers are complex, the distinction between private and public is even more obscure [10, 11].

The safeguarding of individual rights in the 18th and 19th centuries allowed the formulation of the right to privacy which is directly linked to the freedom of a person from all forms of control / surveillance and insult. At the same time, the legal introduction of the right to privacy has consistently led to the introduction of a constitutional protection obligation. So, theoretically, we live in a world where privacy is now legally enforceable and self-evident in every form of social practice, such as the use of SNSs. Is this real?

This paper addresses the right to privacy in online networks framed on Social Networking Sites. Section 2 refers to privacy in SNSs, focusing on the way SNSs have become a part of contemporary reality having effect on human experiences. This Section addresses also the Privacy Paradox phenomenon as the state of contradiction between privacy attitude and privacy behavior, includes subsections regarding the factors that affect users' disclosure practices and privacy concerns, while it also records measures that should be taken for privacy protection. Section 3 underlines that the right to privacy is one of the most endangered human rights in the context of globalization and emergence of the Information and Knowledge Society. Privacy violation affects social cohesion and puts thus into danger the whole society.

2. THE RIGHT TO PRIVACY IN INFORMATION SOCIETY. THE CASE OF SOCIAL NETWORKING SITES

Information holds a key role within Information Society. In this frame, control of information produces new conflicts that raise unique global risks [12] regarding individual rights, protection of personal data, and security of information. These risks come up because the social, economic and political functions of states directly depend on information circulating in information systems, while also depending on private sector [13-15] which due to the competition rules cannot provide security guarantees for the democratic orientation of the states. As a result, national governments challenge the control of information, establishing, limiting and applying laws that balance public and private interests [13, 16]. In this frame the terms for privacy protection are being renegotiated globally. It is understood, thus, that the above-mentioned risks "*do not derive from external phenomena but from human decisions and actions*" [1] (p. 50) concerning the control and use of information according to the visible and latent interests of social groups they serve.

A series of recent incidents, as that of the Snowden case in 2013 or of Cambridge Analytica in 2018, confirm that despite the constitutional requirements for privacy, governments or politicians in cooperation with companies use internet-based information and organize mass-tracking programs for citizens. Hundreds of millions of data are collected, while governments and private organizations / service providers refuse that they collect and distribute citizens' data.

Within a society where on one hand information is disseminated through every possible internet source becoming accessible to all and legislation has established general principles for privacy protection on the other, while the states have different starting points of legal culture, the interpretations of privacy become more and more obscure [16]. The regulatory framework for privacy protection is multidimensional concerning both the application of international law conventions, national regulations, decisions by independent authorities that manage information issues, and rules of private sector bodies through self-regulation [17]. Within this complex frame, keeping in mind that citizens are constantly expressing their anxiety about who has access to their data, it is particularly interesting to consider how citizens perceive themselves in online networks and take care to ensure their privacy -if they do so-, acknowledging it as an indefeasible right.

2.1 Users privacy experiences in Social Networking Sites

Social media are the outcome of the technological development during the last decades. Beyond a technological phenomenon, social media constitute a social phenomenon since their effect on human daily reality is catalytic. This is evidenced by the growing number of users, the new applications and the multiple environments to which they have exploited.

Social Networking Sites (SNSs) -one of the categories of social media- dominate in almost all human activities, facilitating the interaction between people, the online procurement of goods and services, business transactions, communication between the state and the citizens, the development of communities. In this context of

ubiquitous presence of SNSs, social subjects adapt to a new "reality", the digital reality that operates within the framework of social action, but often shaping its own norms.

To participate in a SNS, the user has to build a profile that represents, in a way he/she chooses, the digital persona adopting specific methods to present and control his/her image. Users share a large amount of information in a variety of forms, such as personal data, photos, thoughts, experiences and preferences -sometimes true, sometimes false- leaving their digital footprint in every function. At the same time, this process raises users' anxiety regarding their privacy and the security of their data even though they voluntarily provide personal information and / or carelessly consent to its collection. SNSs provide users the facility to create new relationships or to preserve pre-existing, to self-present, to explore photos and profiles of other users, to activate post-communication forms such as commenting on messages posted or to have fun [18-22]. [23] has pointed out that the specific nature of SNSs creates intimacy feelings that encourage the information flow within them allowing users to feel that they can maintain relationships not only at personal level but at professional also, as noted by [24].

SNSs are currently the most dynamically developing personal networking tool [6], as they contribute to the promotion of online interpersonal interactions based on the norms of daily interaction, allowing both the expression of personal identity, and community building [25]. In this frame it is clear that SNSs usage leads to the increase of users' material and symbolic resources simultaneously reconstructing the social status since SNSs constitute the modern practice of participation in social networks in the Information Society. In this frame, the establishment of a collective digital culture, built on reciprocity and trust which are crucial for social development and sustainability is recommended. But what is the price?

Although users believe they can control the information they share, controlling thus their privacy, [26] point out that today information is not under the control of individuals, but of organizations that hold it. In the context above, users experience or learn about incidents ranging from personal data violation to online personalized advertisements. Violations of users' privacy may arise, in addition to those known as a result of the operation of governments and companies, by other users also due to the multiple forms of unwanted or uncontrolled information disclosure, regardless the number of persons to whom it is disclosed, since information can be easily found and copied. Incidents regarding violation or misuse of personal information raise users' privacy concerns and anxiety about their visibility and vulnerability in digital environments. Users experience the feeling of intrusion into their personal lives, the concern that one knows their habits and preferences, controls their behavior and guides their daily practices. These anxieties will grow even more as the technological advances of mobile devices are moving fast forward [27]. Despite these, the number of SNSs users continues to grow steadily, because SNSs bear a form of glamor resulting from the combination of the possibilities they offer for self-presentation and social interconnection, as [25] argues.

Privacy is a multidimensional concept and is perceived by people in different ways defined by a variety of parameters. [27] note that the literature provides five

variables of privacy, including: "*perceived ability to control submitted information*", "*use of information*", "*notice*", "*perceived privacy*" and "*privacy protection behavior*" (p. 430).

2.1.1. Privacy Paradox

In order to understand the concept of privacy in digital environments, most of the studies [28-31] use the definitions of Westin and Altman. According to Westin, privacy is defined as one's right to determine what information is accessible, to whom and when, while in Altman's view privacy is determined as the selective control of individuals on others' access to their information, forming thus a social and dynamic process targeting the achievement of optimization in the relationship between information disclosure and withdrawal [28-29, 31].

The relationship between privacy on SNSs and information disclosure is a multidimensional issue [32-35]. [28] has recorded the tense in the relation between users' desire and need to protect their privacy and their desire to disclose personal information, which may lead them to underestimate the privacy risks resulting from personal information disclosure. As underlined by [36] this relationship "*is characterized by a constant tension between secrecy and transparency. On the one hand, individuals are afraid of threats to their personal autonomy and freedoms stemming from a global data processing by governments and undertakings, while on the other hand they voluntarily proceed to the disclosure of personal data (eg by posting names, photographs, dates of birth, marital status….)*" (p. 642).

Referring to privacy in Web in general, [28] points out that its ideal achievement is based on a balanced relationship between individuals' needs for social interaction and personal information disclosure and their needs for privacy. So, as it happens with privacy in real life, SNSs' users need to balance their concerns regarding their visible content on a Web site to a variety of audiences with their desire to enjoy privileges because of their interactions in them [30]. According to [37], the balance between privacy and self-disclosure is the core of human behavior and determines interpersonal relationships. The choice of more or less privacy changes according to wishes, social goals and specific context, influencing thus the ways in which interpersonal boundaries in relationships are being negotiated.

However, what has been observed in a number of researches is that SNSs users do not always manage to balance these needs. Several studies have dealt with the issue of privacy concerns impact on users' behavior and have comparatively examined the stated attitude and the actual behavior demonstrating that although users are interested in their privacy on SNSs and have concerns regarding the security of personal information [38-40] or feel vulnerable to privacy violations [30], these concerns are not followed, for example, by disclosing less information or changing privacy settings. Consequently, people fail, as [41] explains, to turn their privacy concerns into privacy protection behaviors. In this way an inconsistency or discrepancy is revealed between views and attitudes on one hand and behavior on the other with reference to the informational privacy.

"Privacy paradox" [40, 42] finally emerges as the state of contradiction between privacy attitude and privacy behavior. In a recent literature review paper, [43] notes that although this is the dominant dichotomy when referring to privacy paradox,

researchers have also compared privacy concerns with privacy behavior. Even though these two constructs are related, they are also fundamentally different, as "*privacy concerns could be quite generic and, in most cases, are not bound to any specific context, whilst privacy attitudes refer to the appraisal of specific privacy behaviours*" [43] (p. 123). Furthermore, [43] underlines that several studies investigate privacy intention instead of privacy behavior ignoring that often privacy intentions do not lead to protective behavior. [40] attempting to interpret the "privacy paradox" explain that this discrepancy is likely to be based on users' trust towards service providers and other users if users consider providers to be honest with them (Cheung et al., 2015) or if they recognize similarities between themselves and other users [44].

2.1.2 Factors affecting personal information disclosure

What impels people in online spaces such SNSs to reveal information about themselves and others, even though they really know or suspect that information is accessible? How could one interpret the fact that we often reveal more information during our online interactions with others than in our face to face communication? Many researches have attempted to uncover the factors that influence the decision-making process to disclose personal information on SNSs.

[27] have investigated the relationship between information disclosure and three important dimensions; control over personal information, user awareness, and security / privacy alerts. Information control is recognized as a key element in the perception of risk [45-46] that derives from information disclosure. [47] verified the hypothesis that the increased control individuals think they have regarding sharing and access to their information will also increase their willingness to disclose sensitive information, and if this increase is high, users will end up being more vulnerable, despite the fact that technologies are designed to protect them. So, [47] conclude that the perceived ability of people to control certain dangers shields their awareness or turns their attention to other dangers they cannot control.

Many researches have focused on users' general lack of awareness regarding the usage of their information by SNSs and third parties, including governments also [48-49]. [50] argue that awareness of the consequences resulting from privacy breaches predicts disclosure. The positive correlation between user awareness and information disclosure has been also supported by [27] who argue that when users have a better knowledge about the use of personal information, they are more likely to reveal more information. This finding is particularly for user awareness programs.

The low level of knowledge has been shown to be related to the tendency or temptation to reveal personal information in order to gain small benefits [51-53]. [41] predicts that in the future, in larger social environments, there will be a privacy protection gap "*given that knowledgeable users understand why their online privacy matters while less knowledgeable users may be easily persuaded to trade their privacy for transient benefits"* (p. 40). Digital literacy on the contrary seems to have positive effects on online privacy protection [54-56] being recorded as a prerequisite for the understanding of technical terms such as cookies and data mining [55-56]. In this context, researches such as those of [57] and [56] have focused on users' lack of ability, knowledge and privacy protection skills identifying this situation through

the theory of cognitive deficiency. [58] referring to users' privacy literacy notes that it "*encompasses an informed concern for their privacy and effective strategies to protect it*" (p. 51), while [59] claim that "*online privacy literacy can be defined as a combination of factual or declarative knowledge ('knowing that') and the procedural ('knowing how') knowledge about privacy*" (p. 339). The first one refers to users' knowledge of the technical aspects regarding their data protection, the relevant laws and directives, while the second to their ability to use strategies in order to regulate their privacy and protect their data.

Self-disclosure has been also studied with reference to social influence [60-61] and online trust [62-63], revealing that both factors increase self-disclosure while, on the contrary, perceptions regarding the risk for privacy breach reduce it. In this frame, the influence by friends' practices regarding privacy settings or the social pressure that users receive from their social environment in order to participate in SNSs seem to affect disclosure behaviors. [64] referring to the contribution of social factors, during a research addressed to students, has shown that they cannot avoid participating in Facebook, which acts as a social norm for their everyday life, although they have made progress regarding the personal information they reveal and share. As [31] point out *"(perceived) social norms seem to play an important role in determining personal and spatial access restriction to user profiles as well as the amount and the kind of information individuals provide within SNSs"* (p. 185). An important factor that also affects disclosure is people's need to adapt to the expectations of a group or community in order to avoid exclusion, indicating specific behavior that is determined mainly by their own representation of the group's expectations [65]. In this frame, one's need to feel being part of a group (sense of belonging) can limit privacy concerns.

Other approaches emphasize on the incentives that trigger users' disclosure behaviors. Social capital, social support, maintaining communication with others, starting new relationships, self-promotion and entertainment/fun have been recognized as such motivations for users' operation on SNSs [66-71, 44]. [72] report that Facebook users disclose personal information in order to acquire social capital benefits, while [73] underline that in order to achieve these benefits disclosure needs to be permanent. In the frame above, self-disclosure is perceived as a privacy transaction, since users believe they will receive a reward if they reveal personal information and thus behave in the opposite direction of protecting their privacy [74-75]. The choice to disclose or conceal personal information constitutes thus an act of balancing between the perceived benefits and the perceived costs [44].

Empirical researches in the field of psychology associate the control of information communicated and the information disclosure with personality treats, such as the need for popularity and self-esteem. For example, [76] have shown that Facebook users who disclose a large amount of information are possessed by a tension for self- promotion. They also demonstrated that those using Facebook for the creation of digital communities are the ones who reveal the most essential personal information and appear to be socially extroversial, while for both categories of users it was pointed out that the number of posts grew when they experienced periods of low self-esteem [76]. The reasons that lead to these behaviors, apart from

psychological factors, include reduced social cohesion and lack of satisfaction resulting from users' offline relationships as well.

The level of information sensitivity has also been reported as a factor for users' willingness to disclose information. [77] and [28] have shown that information sensitivity raises the belief in risk while decreasing the desire for disclosure. So, users are more cautious when they reveal sensitive information in relation to less sensitive one. A recent research however, regarding Greek Universities students' Facebook communities [78] showed that within these communities, University students felt that they could share even the most inner information about their sexual life, thus limiting the concept of privacy.

The structure of SNSs has also a crucial role regarding users' information disclosure, as shown by [79] in the case of Facebook. In many cases, a user in order to use the services of a SNS, has to reveal information according to SNS's operating preconditions [79-80, 38]. [31] note that providers, through technical features, try to maximize the amount of information they receive from users to make Websites more dynamic and attractive in order to make a profit. The high intensity usage of SNSs also leads to disclosure behaviors [68]. Finally, the state of anonymity has also been recognized as a factor influencing disclosure reducing thus privacy concerns [74, 81].

Personal information disclosure, consciously or not, is ultimately a common practice among users involving heterogeneous audiences with different social relationships within users' networks. Although disclosure can be made either with full publicity and to unknown users or to specific individuals within users' network [28], the information is very easy to be found, copied, expanded and shared in both cases [82]. As [28] points out users who reveal personal information are often not sure who and how many people are included amongst the audiences at which the revelations have been made due to the temporal and spatial segregation that exists in relationships developed between these audiences.

2.1.3. Privacy concerns

Most researches regarding privacy concerns or related protection behaviors focus on individual level [52, 83-84]. [85] have highlighted the impact of cultural values on users' privacy concerns and the way they may affect self-disclosure, noting that they also influence the assessment regarding the sensitivity of the personal information communicated. In this frame, researches [86-87, 53] have focused at country level investigating how individuals from different cultural contexts evaluate privacy and respond to privacy concerns and privacy issues.

[41] in their study regarding the factors of privacy concerns have included the dimension of perceived risk for other users, using the concept of comparative optimism as reported by [88]. Comparative optimism refers to the state of belief that the individual is more protected than others, mostly compared to more vulnerable others or groups. This situation may arise either from the underestimation of personal risk or from overestimating the vulnerability of others regarding online privacy violation, but in both cases it refers to knowledge about privacy protection [54].

Privacy, as already stated in the previous sub-section, is directly related to the control of personal information. [47] underline that a distinction should be made between the act of voluntary information disclosure, the access and the use or misuse of information, emphasizing thus that the resulting cost depends on access and use / misuse of information, which people fail to conceive as they focus on the first level of control (release of information). In this frame, previous researches have shown that lower estimated control over personal information is associated with higher privacy concerns [89], while in other cases it has been pointed out that those who are indifferent to privacy feel that they have control over the information they reveal [40]. These findings verify [47] argument that "*perceived control over release or access of personal information can cause people to experience an illusory sense of security and, thus, release more information. Vice versa, lack of perceived control can generate paradoxically high privacy concerns and decrease willingness to disclose, even if the associated risks of disclosure may be lower*"(p. 342).

Privacy concerns also relate to the security of SNSs, as demonstrated by [40]. [90] explain that businesses trying to convince customers about the security of their personal data have introduced new techniques -self-regulatory transparency mechanisms- that provide alerts and include privacy statements and privacy seals. However, former researches have shown that privacy seals can increase the willingness to disclose information [91], thus putting aside privacy concerns. It seems, therefore, that privacy concerns are affected by users' confidence in privacy settings.

Age seems to be also an important factor in privacy concerns. As [92] explains, people belonging to different age groups vary in their perception of privacy and the way they can manage it. [93] reports that young people are willing to experiment with SNSs and this can lead them to behave inconsiderably or recklessly, while other researches have shown that young people have a higher level of privacy awareness [94-95, 64]. Older people usually have more difficulty to understand and implement privacy settings and this turns them into potential high-risk users [96]. [97] investigated the use of Facebook, privacy concerns and the application of privacy settings in the three stages of adulthood (18-25, 25-40, 40-65) revealing differences between the three groups. Specifically, groups aged 25-40 and 40-65 years old are more vulnerable in terms of privacy protection than those of 18-25 years, who are recorded as d conscious users with reference to privacy. Those aged 40-65 had greater privacy concerns than other age groups, although they admitted they were less likely to use privacy settings.

Gender constitutes a variable whose impact has been investigated in relation to privacy perceptions and privacy concerns. For example, [98] and [40] have shown that men are less concerned about online privacy, [99] that women are generally more risk-averse, while other researchers [100-102] did not identify significant differences between gender in relation to privacy perception. With reference to teenagers, [103] recorded no difference in privacy concerns between boys and girls, although the latter were more likely to have their profiles private and adopt privacy protection strategies to avoid victimization.

SNSs users' privacy concerns are related not only to the protection of their personal information disseminated to others who could exploit this, but also related to the protection and management of their image in the frame of the relationships that they have developed within their network [30]. The extent to which these concerns are positive making users more cautious both in terms of quantity and quality of information they publish either for themselves or for others will ultimately determine the extent to which they will protect themselves from the potential problems that will arise from the exploitation of information.

2.2 Privacy protection in Social Networking Sites

Several proposals have been made in order to ensure that personal information circulated on Internet and social media is kept safe, not accumulated and used by others -no matter who they are- without the explicit consent of the users. In this context, it is suggested that legislation should be strengthen in order to regulate the technological planning of data collection and the control of data acquired [36]. The European Commission in 2012 reformulated the European Union Data Protection Directive (1995) proposing the establishment of "the right to be forgotten", "privacy by default" and "privacy by design" in order to enhance privacy protection [104].

Referring to the providers, [60] highlight the need to introduce "*more social features that foster users' interactions over the Social Networking Sites, such as person profile customization or news feed notification services*", while they also propose that service providers "can integrate intuitive privacy indices, showing users the level of privacy protection to alert them about the potential risks of self-disclosure in SNSs" (p. 293). [105] state that users could be helped to confront privacy issues if the configured information systems provide them with mechanisms and interfaces enabling them to understand their function and if these mechanisms become integrated into users' practices, values and sensitivities.

From a more technical point of view, software engineers consider privacy in a more technical sense mainly as a set of specific requirements that need to be fulfilled in order for a system or service to become privacy aware. In previous works [106-108] a method that assists software engineers in eliciting and modeling privacy requirements during system design is presented. Our findings show that for increasing users' privacy it is of vital importance to understand factors that overcome the close boundaries of an information system and its technical abilities (fulfilled requirements) as privacy is a multifaceted concept that is related to user's social and behavioral characteristics. Creating trustworthy systems and services that fulfill specific security and privacy requirements taken into consideration external non-technical factors is a solution towards this direction [109].

In addition to legislation's provisions and providers' obligations, it is important to activate users and enhance their awareness to use strategies in order to mitigate the risks resulting from disclosure to unwanted audiences [29- 30]. These strategies relate both to personal information disclosure behaviors and the use of privacy control techniques provided by the Web sites. In the frame of the first dimension, users choose the type of information they record in their profile or the updates they share in their Status [30], control the network of their Friends [29, 110],

retain different profiles, do not accept friend requests from strangers, delete comments or remove photos [111-112]. [79] research, from 2005 to 2011, investigated Facebook users' behavior regarding personal information disclosure options, showing that the amount of information users choose to disclose to their friends has grown despite existing privacy concerns, while disclosure of information to profiles of strangers has decreased. With reference to the second dimension, that of technical control, users in order to protect their privacy use privacy settings [29-30]. [113] record that the Facebook privacy control techniques allow users to successfully manage privacy threats from unknown external audience but provide poor choices in relation to risk reduction arising from the existing Friends network. As pointed out by [79], Facebook, in recent years, in order to encourage the disclosure of personal information has changed the default settings when new users register on the Site.

Finally, educational programs aiming at raising users' awareness regarding potential risks driving from self-disclosure on SNSs and adopting relevant protection behaviors are particularly important as shown in several researches [114-117]. Specifically, long term educational interventions are shown to have a significant impact on students' attitude, increasing both privacy awareness and concerns through acknowledging risks in SNSs and confronting them. Awareness increase leads users/students to adopt privacy protective behavior either by using personal strategies or employing technical mechanisms [118].

3. ENSURING SOCIAL COHESION IN INFORMATION AND KNOWLEDGE SOCIETY

The digital revolution led to a new reality that essentially altered not only the way people perceive the social environment, but also social environment itself. Communication with friends, creation of new relationships, search for support from others, need to present oneself -sometimes even in the form of projection-, participation in communities of common interest, products and services' market, transactions with the state and other organizations are all fields mediated by the digital technology of SNSs. Indeed, social media and specifically SNSs have shaped new norms and practices in modern society, transforming among others the form of human interaction. The fundamental elements of users experiences on SNSs -in the sense that [119] refers to experiences as "relationships of power and forms of relationship between the Self and Others"- point out that within Information Society multiple aspects of social reality are being remodeled and redefined in particularly obscure and inconspicuous ways [1]. The flood of information [120] opens the path for more knowledge and individual and social rights on the one hand, while on the other it sets under negotiation concepts such as privacy and security.

In the context of SNSs, users "*when creating the personal information they want to share with others, they decide at the same time how they wish to be perceived by other members of the community*" [121] (p. 6), while providers with sophisticated techniques gather and process large amounts of information either by themselves or providing it

to others (governments). Thus, as [120] points out, people's exposure to a "*flood of information*" raises conflicts about security, predictability, sense of belonging, stable personal identity, cohesion, unmediated experiences.

Within this flood, "*the distinction limits between personal data and personal data accessible to public are equally indistinguishable, which suggests that the possibilities of using and misusing personal data multiply*" [16] (p. 38). In this respect, the exercise of the power regarding personal data management runs throughout the social body, without being clear the conditions of enforcement and compulsion. The increase of control over individuals serves the purpose of safeguarding the well-being of social media large companies. As a result, besides the role of the state that changes [122], companies are increasingly involved in power, exercising ideological and political control [15]. This issue further reinforces [119] thesis on the development of "problem-making" when considering the protection of privacy and its effects on social cohesion, especially in the context of Information Society, by cultivating practices that pose problems on every political and social choice.

In this context, many researches on social media [123-126] use the "Panoptikon", a framework for monitoring prisoners developed by Jeremy Bentham in the late 18th century. "Panoptikon" extends into cyberspace. Potentially everyone can be seen by everybody. This reality alters the concept of privacy while users often have the illusion of privacy which makes difficult to delimit the kind of information they should be share [51]. This personalized exercise of power clearly illustrates the danger already identified by [127] regarding social systems of high differentiation, where the exercise of social control is pushed "*to the most intricate sphere of the meaning*" (p. 85) of the social actors, while simultaneously dominant established collective values are constructed. Through the operation of social media companies, specific interests are built up as values in relation to privacy and these are reproduced over the years, ending up in their encapsulation and integration by the community.

Although all may espouse these dominant values at the theoretical level, at empirical and experiential levels this may not happen [128]. [129] argues that there are differences between users' representations regarding how they feel about privacy and how they really react to its violation. So, although users have embraced or agreed to the general value of privacy protection, they may take actions that contradict it accordingly to the effort to achieve the goals they have set in defending their individual interests. Underlining the phenomenon recorded as "Privacy Paradox" [51, 83, 130] which refers to the differentiation between the intention of social subjects to disclose personal information and the actual disclosure behavior, mediated by privacy concerns, it is important to note that the perception of privacy shows significant variations between socio-cultural systems [131-132]. Users, according to the assessment of the situation they make through social media usage, show the extent to which they have incorporated the value of privacy protection and whether they are prepared to defend it through practices and actions in social media, in each case the value is specialized, goes beyond its abstract context and concerns specific purposes and interests. It should be noted that, even if there is complete consensus on the value of privacy protection, it is impossible to have full consensus

on its evaluations. These evaluations result in the formulation of criteria of action directly linked to specific situations, but the criteria cannot appeal to all social media users, given the diversity that characterizes them.

The possibility of privacy violation is one of the greatest risks in the globalized environment of the Information Society [133], since it includes the lack of respect for the individuals and for their right to privacy as well as the control exercise over him/her, while at the same time creates significant opportunities and challenges for the delimitation of collective values and social behaviors in relation to privacy protection.

Thus, beyond the obvious responsibility of third parties, whoever those are that violate national and international conventions on the protection of human rights, we must think on the role of individuals / users in the process of revealing their information. Regardless the need to communicate with others, to join a team and gain benefits and despite the obvious and recorded privacy concerns, users themselves generate the risk, not only for themselves but also for others too and potentially for the whole society, given their criteria of action and the collective representation that we all are somehow connected. Users' intention and need to interact with others even if they have to reveal personal information and their disclosure behavior constitute parts of a recurrent process of privacy risks generation. In this frame privacy risks re-occur as a result of the four systemic defections that contribute to the risk reproduction according to [1].

Based on [1] thesis that the concept of risk involves the possibility of timely forecasting that can lead to the prevention of future disaster, the role of users regarding their self-protection is of major importance, leading to a new form of social development in Information Society, within which one of the basic principles is the personal responsibility. After all, as [119] records from the moment when certain relations of power develop there are synchronically resistance possibilities too, which need to be equally resourceful, dynamic and productive.

The users' concerns and their anxieties with regard to privacy protection prove that they recognize the risk, while the strategies and techniques of protection they adopt show that they try to avert the risk. In this frame, social development ensure is based on a shift in intervention; from repressive to preventative intervention with an emphasis on users' awareness. As a matter of fact, this is a form of personal development that, as recorded by [134], collectively ensures social progress. On this basis, in order to make social development sustainable, its planning should be based on citizens' actions which will perpetuate and maintain it through participation and democracy, always taking into account the environmental constraints and the clear knowledge of their needs [135].

However, as [1] argues, prevention is not final as post-modern society suffers from four systemic defects that contribute to risk reproduction. Thus, in any case where users exceeding the limits are unable to control information they publish for themselves or others and to control who and how can access and use this information or users underestimate the harm that can come up for themselves or others while often overestimating the perceived control over information, the risk for the members of society recurs. In this respect, the results of the [136] and [137]

studies who argue that the co-responsibility of public and private organizations brings more effective measures for social development need to be applied in terms of privacy protection also.

Nevertheless, according to the cognitive approach for social development planning, its production processes consist of overlapping interventions designed by experts and those benefited [138], requiring everyone's participation in the effort to improve the quality of life and social autonomy [139]. As [9] notes "*the concepts of society and privacy are completely interrelated, since without society there would be no need and demand for privacy*" (p. 507).

Privacy protection has been recognized as an important principle in all modern democracies [140] and its preservation has been identified as a major need [141]. In this context, social development principles based on privacy protection in social media can focus on users' personal development, their development as members of digital communities emphasizing on knowledge addressing to users' needs and goals for privacy protection, on practices assessment and on users' demand for social media providers adaption to their needs as well.

4. REFERENCES

[1] Beck U.: *Risk Society. Towards a New Modernity*. Sage, London, (1992).

[2] Chtouris, S.: *Rational symbolic networks - Global States and national hobbit*. Nisos Publ., Athens (2004) (in Greek).

[3] Berkman, L.F., Glass, T.: Social integration, social networks, social support and health. In: Berkman, L. F., Kawachi, I. (eds). *Social Epidemiology*, pp. 158-162. Oxford University Press, New York. (2000).

[4] Breeze, E., Grundy C., Fletcher A. *Inequalities in quality of life among people aged 75 years and over in Great Britain*. University of Sheffield, UK (2001). http://www.growingolder.group.shef.ac.uk/GOProgSumms.pdf. Accessed Jan 2019.

[5] Walker K., Macbride A., Vachon M.L.S.: Social support networks and the crisis of bereavement. *Social Science and Medicine* **11**, 34-41 (1997).

[6] Lin, K.Y., Lu, H.P.: Why people use social networking sites: an empirical study integrating network externalities and motivation theory. *Comput. Hum. Behav*. **27**(3), 1152–1161 (2011).

[7] Pai, P., Arnott, D. C.: User adoption of social networking sites: Eliciting uses and gratifications through a means–end approach. *Computers in Human Behavior* **29**(3), 1039-1053 (2013).

[8] Gritzalis, S.: Enhancing Web Privacy and Anonymity in the Digital Era. *Information Management and Computer Security* **12**(3), 255-288 (2004).

[9] Mitrou, L.: Privacy protection in Information and Communication Technology - The legal dimension. In: Lambrinoudakis, C., Mitrou, L., Gritzalis, S., Katsikas, S. (eds). *Privacy and Information and Communication Technologies - Technical and Legal Issues,* pp. 505-551. Papasotiriou Publ., Athens (2010) (in Greek).

[10] Jones, T. & Newburn T.: *Private Security and Public Policing*. Clarendon, Oxford (1998).
[11] Marx, G.T.: Murky Conceptual Waters: The Public and the Private. *Ethics and Information Technology* **3**(3), 157-169 (2001).
[12] Panousis, J.: *Symbolic constructions of reality*. Entelecheia Publ., Athens (2004) (in Greek).
[13] Kitsiou, A.: *The social construction of crime in Information Society: the paradigm of free software movement*. Ph.D. thesis. Department of Sociology, University of the Aegean (2014) (in Greek).
[14] Kallas, J.: *Information Society and the role of social sciences*. Nefeli Publ., Athens (2006) (in Greek).
[15] Cebrian J.L.: *The network*. Stachi, Athens (2000) (in Greek).
[16] Mitrou, L.: *Law in Information Society.* Sakkoulas Publ., Athens (2002) (in Greek).
[17] Simon, E.: Introduction to the legal frame of Information Society. In: R. Pinter (ed.) *Information Society, Studies on Information Society. From theory to political practice*. Gondolat, Budapest (2008)
[18] Lee, K. T., Noh, M. J., Koo, D. M.: Lonely people are no longer lonely on social networking sites: The mediating role of self-disclosure and social support. *Cyberpsychology, Behavior and Social Networking* **16**(6), 413-418 (2013).
[19] Bryant, E. M., Marmo, J., Ramirez, A. Jr.: A functional approach to social networking sites. In: Wright, K. B., Webb, L. M., (Eds). *Computer-mediated communication in personal relationships*, pp. 3-20. Peter Lang, New York (2011).
[20] Kim, J., Lee J.R.: The Facebook paths to happiness: effects of the number of Facebook friends and self-presentation on subjective wellbeing. *CyberPsychology, Behavior and Social Networking* **14**, 359–364 (2011).
[21] Pempek, T. A., Yermolayeva, Y. A., Yermolayeva, S. L.: College students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology* **30**, 227–238 (2009).
[22] Bargh J.A, McKenna K.: The Internet and social life. *Annual Review of Psychology* **55**, 573–590 (2004).
[23] Pearson, E.: All the worldwide web's a stage: the performance of identity in online social networks. *First Monday* **14**(3) (2009). http://firstmonday.org/article/view/2162/2127. Accessed Dec 2018
[24] Trusov, M., Bucklin, R. E., Pauwels, K.: Effects of word-of-mouth versus traditional marketing: Findings from an internet social networking site. *Journal of Marketing* **73**, 90–102 (2009).
[25] Papacharissi, Z. (Ed.): *A networked self: Identity, community, and culture on social network sites*. Routledge, New York (2011).
[26] Conger, S., Pratt, J.H. & Loch, K.D.: Personal information privacy and emerging technologies. *Information Systems Journal* **23**(5), 401-417 (2013).
[27] Benson, V., Saridakis, G. & Tennakoon, H.: Information disclosure of social media users. Does control over personal information, user awareness and security notices matter?. *Information Technology & People* **28**(3),426-441 (2015).
[28] Taddicken, M.: The 'Privacy Paradox in the Social Web: The Impact of Privacy Concerns, Individual Characteristics and the Perceived Social Relevance on

Different Forms of Self-Disclosure, *Journal of Computer-Mediated Communication* **19**(2), 248-273 (2014).

[29] Stutzman, F., Vitak, J., Ellison, N. B., Gray, R., Lampe, C.: Privacy in Interaction: Exploring Disclosure and Social Capital in Facebook. In: *Proceedings of the Sixth International Conference on Weblogs and Social Media* pp. 330-337. AAAI org, Ireland, Dublin (2012).

[30] Ellison, N., Vitak, J., Steinfield, C., Gray, R., Lampe, C.: Negotiating privacy concerns and social capital needs in a social media environment. In: Trepte, S., Reinecke, L. (Eds). *Privacy online: Perspectives on privacy and self- disclosure in the social web*, pp. 19-32. Springer, Heidelberg (2011).

[31] Ziegele, M., Quiring, O.: Privacy in Social Network Sites. In: Trepte, S., Reinecke, L. (Eds). *Privacy online: Perspectives on privacy and self- disclosure in the social web*, pp. 175-189. Springer, Heidelberg (2011).

[32] Rains, S. A., Brunner, S. R.: The Outcomes of Broadcasting Self-Disclosure Using New Communication Technologies Responses to Disclosure Vary Across One's Social Network. *Communication Research* **45**(5), 659–687 (2015).

[33] Bazarova, N. N., Choi, Y. H.: Self-disclosure in social media: Extending the functional approach to self-disclosure motivations and characteristics on social network sites. *Journal of Communication* **64**, 635-657 (2014).

[34] 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* pp. 3287-3296. ACM, Paris, France (2013).

[35] Walton, S. C., Rice, R. E.: Mediated disclosure on Twitter: The roles of gender and identity in boundary impermeability, valence, disclosure, and stage. *Computers in Human Behavior* **29**, 1465-1474 (2013).

[36] Buschel, I., Mehdi, R., Cammilleri, A., Marzouki, Y., Elger, B.: Protecting human health and security in digital Europe: how to deal with the "privacy paradox"? *Sci. Eng. Ethics* **20**, 639–658 (2014).

[37] Petronio, S.: *Boundary of privacy: Dialectics of disclosure*. State University of New York Press, Albany (2002).

[38] Nguyen, M., Bin, Y.S., Campbell, A.: Comparing online and offline self-disclosure: a systematic review. *Cyberpsychol. Behav. Soc. Netw*. **15**(2), 103–111 (2012).

[39] boyd, d. m., Hargittai, E.: Facebook privacy settings: Who cares?. *First Monday*, **15**(8), (2010). https://firstmonday.org/article/view/3086/2589 Accessed Jan 2019.

[40] Acquisti, A., Gross, R.: Imagined communities: Awareness, information sharing, and privacy on The Facebook. In: Danezis, G., Golle, P. (eds). *Proceedings of the 6th Workshop on Privacy Enhancing Technologies (PET '06)* pp. 36-58. Robinson College, Cambridge, UK (2006).

[41] Baek, Y.M.: Solving the privacy paradox: a counter-argument experimental approach. *Comput. Hum. Behav*. **38**, 33–42 (2014).

[42] Dienlin, T., Trepte, S.: Putting the social (psychology) into social media is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *Eur. J. Soc. Psychol*. **45**, 285–297 (2015).

[43] Kokolakis, Sp.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security* **64**, 122-134 (2017).
[44] Krasnova, H., Spiekermann, S., Koroleva, K., Hildebrand, T.: Online social networks: why we disclose. J. *Inf. Technol*. **25**, 109–125 (2010)
[45] Klein, W. M., Kunda, Z.: Exaggerated self-assessments and the preference for controllable risks. *Organizational Behavior and Human Decision Processes* **59**, 410-427 (1994).
[46] Nordgren, L.F., Van Der Pligt, J., Van Harreveld, F.: Unpacking perceived control in risk perception: The mediating role of anticipated regret. *Journal of Behavioral Decision Making* **20**(5), 533-544 (2007).
[47] Brandimarte, L., Acquisti, A., Loewenstein, G.: Misplaced confidences: privacy and the control paradox. *Soc. Psychol. Pers. Sci*. **4**(3), 340–347 (2012)
[48] Bertot, J.C., Jaeger, P.T, Grimes, J.M.: Using ICTs to create a culture of transparency: e-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly* **27**(3), 264-271 (2010).
[49] Bertot, J.C., Jaeger, P.T., Hansen, D.: The impact of polices on government social media use: issues, challenges, and recommendations. *Government Information Quarterly* **29**(1), 30-40 (2012).
[50] Christofides, E., Muise, A., Desmarais, S.: Information disclosure and control on Facebook: are they two sides of the same coin or two different processes?. *CyberPsychology & Behavior* **12**(3), 341-345 (2012).
[51] Barnes, S.B.: A privacy paradox: social networking in the United States. *First Monday*, **11**(9), (2006). https://firstmonday.org/article/view/1394/1312_2 Accessed Jan 2019.
[52] Gross, R., & Acquisti, A.: Information revelation and privacy in online social networks. In: Proceedings of the *ACM Workshop on Privacy in the Electronic Society* pp. 71-80. ACM, Virginia, USA (2005).
[53] Smith, H.J., Dinev, T., Xu, H.: Information privacy research: an interdisciplinary review. *MIS Quarterly* **35**(4), 989-1015 (2011).
[54] Baek, Y.M., Kim, E. Bae, Y.: My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior* **31**, 48–56 (2014).
[55] Hargittai, E.: An update on survey measures of web-oriented digital literacy. *Social Science Computer Review* **27**(1), 130–137 (2009).
[56] Park, Y.J.: Digital literacy and privacy behavior online. *Commun. Res*. **40**(2), 215–236 (2011)
[57] Debatin, B., Lovejoy, J.P., Horn, A.K., Hughes, B.N.: Facebook and online privacy: attitudes, behaviors, and unintended consequences. *J. Comput. Med. Commun*. **15**, 83–108 (2009).
[58] Debatin, B.: Ethics, privacy, and self-restraint in social networking. In: Trepte, S., Reinecke, L. (Eds). *Privacy online: Perspectives on privacy and self- disclosure in the social web*, pp. 47-60. Springer, Heidelberg (2011).
[59] Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M., Hennhofer, A., Lind, F.: Do people know about privacy and data protection strategies?

Towards the "Online Privacy Literacy Scale" (OPLIS). In: Gutwirth, S., Leenes, R., de Hert, P. (eds.) *Reforming European data protection law*, pp. 333–365. Springer, Heidelberg (2015).

[60] Cheung, C., Lee, Z. W. Y., Chan. T. K. H.: Self-disclosure in social networking sites. *Internet Research* **25**(2), 279 – 299 (2015).

[61] Zhou, T.: Understanding online community user participation: a social influence perspective". *Internet Research* **21**(1), pp. 67-81 (2011).

[62] Posey, C., Lowry, P.B., Roberts, T.L., Ellis, T.S.: Proposing the online community self- disclosure model: the case of working professionals in France and the UK who use online communities. *European Journal of Information Systems* **19**(2), 181-195 (2010).

[63] Dwyer, C., Hiltz, S., Passerini, K.: Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In*: Proceedings of 13th Americas Conference on Information Systems, AMCIS 2007, paper 339.* https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1849&context=amcis2007 Accessed Jan 2019.

[64] Tufekci, Z.: Facebook, youth and privacy in networked publics. In: *Proceedings of the Sixth International Conference on Weblogs and Social Media*, pp. 338-35. AAAI org, Dublin, Ireland (2012).

[65] Ragnedda, M.: Social control and surveillance in the society of consumers. *Int. J. Sociol. Anthropol.* **3**(6), 180–188 (2011).

[66] Ellison, N. B., Steinfield, C., Lampe, C.: The benefits of Facebook ''friends'': Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication* **12**(4), 1143–1168 (2007).

[67] Taddicken, M., Jers, C.: The uses of privacy online: trading a loss of privacy for social web gratifications? In: Trepte, S., Reinecke, L. (eds.) *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, pp. 143–158. Springer, Heidelberg (2011).

[68] Trepte, S. & Reinecke, L.: The reciprocal effects of social network site use and the disposition for self-disclosure: A longitudinal study. *Computers in Human Behavior* **29**(3), 1102-1112 (2013).

[69] Cheung, C. M. K., Chiu, P.-Y., Lee, M. K. O.: Online social networks: Why do students use Facebook?. *Computers in Human Behavior* **27**(4), 1337–1343 (2011).

[70] Utz, S., Kramer, N.: The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 3(2) (2009). https://cyberpsychology.eu/article/view/4223/3265 Accessed Jan 2019

[71] boyd, d., Heer, J.: Profiles as Conversation: Networked Identity Performance on Friendster. In: *Proceedings of the Hawai'i International Conference on System Sciences (HICSS-39)*. IEEE, Kauai (2006).

[72] Steinfield, C., Ellison, N., Lampe, C., Vitak, J.: Online social network sites and the concept of social capital. In : Lee, F. L., Leung, L., Qiu, J. S., Chu, D. (eds.). *Frontiers in New Media Research*, pp. 115-131. Routledge, New York (2012).

[73] Valkenburg, P. M., Peter, J.: The effect of instant messaging on the quality of adolescents' existing friendships: A longitudinal study. *Journal of Communication* **59**, 79–97 (2009).
[74] Jiang, Z.J., Heng, C.S., Choi B.C.: Research note-privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research* **24**(3), 579-595 (2013).
[75] Xu, H., Luo, X.R., Carroll, J.M, Rosson, M.B.: The personalization privacy paradox: An exploratory study of decision-making process for location-aware marketing. *Decision Support Systems* **51**(1), 42-52 (2011).
[76] Hollenbaugh, E. E., Ferris, A. L.: Facebook self-disclosure: Examining the role of traits, social cohesion, and motives. *Computers in Human Behavior* **30**, 50-58 (2014).
[77] Malhotra, N.K., Kim, S.S., Agarwal, J.: Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research* **15**(4), 336-355 (2004).
[78] Sideri, M., Kitsiou, A., Kalloniatis, C., Gritzalis, S.: Privacy and facebook universities students' communities for confessions and secrets: the greek case. In: Katsikas, S.K., Sideridis, A.B. (eds.) *e-Democracy 2015. CCIS*, vol. 570, pp. 77–94. Springer, Cham (2015).
[79] Stutzman, F., Gross, R., Acquisti, A.: Silent listeners: the evolution of privacy and disclosure on facebook. *J. Priv. Confid*. **4**(2), 7–41 (2013)
[80] Gibbs, J. L., Ellison, N. B., Lai, C.-H.: First comes love, then comes Google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research* **38**(1), 70–100 (2011).
[81] Okdie, B. M.: *Blogging and self-disclosure: The role of anonymity, self-awareness and audience size*. Ph.D. dissertation. Department of Psychology in the Graduate School, University of Alabama (2011).
[82] Papacharissi, Z., Gibson, P. L.: Fifteen minutes of privacy: Privacy, sociality, and publicity on social network sites. In: Trepte, S., Reinecke, L.(Eds). *Privacy online: Perspectives on privacy and self- disclosure in the social web*, pp. 75-89. Springer, Heidelberg (2011).
[83] Norberg, P.A., Horne, D., Horne, D.: The privacy paradox: personal information disclosure intentions versus behaviors. *J. Consum. Aff.* **41**(1), 100–126 (2007).
[84] Tufekci, Z.: Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society* **28**, 20–36 (2008).
[85] Alashoor, T., Keil, M., Liu, L. & Smith, H. J.: How Values Shape Concerns about Privacy for Self and Others. In Carte, T., Heinzl, A., Urquhart, C. (eds). *Proceedings of the Thirty Sixth International Conference on Information Systems, ICIS 2015*. AIS Electronic Library, Atlanta (2015).
[86] Krasnova, H., Veltri, N. F., Günther, O.: Self-disclosure and privacy calculus on social networking sites: The role of culture: Intercultural dynamics of privacy calculus. *Business and Information Systems Engineering* **4**(3), 127-135 (2012).
[87] Lowry, P.B., Cao, J., Everard, A.: Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: the

case of instant messaging in two cultures. *Journal of Management Information Systems* **27**(4), 163-200 (2011),

[88] Helweg-Larsen, M., Shepperd, J. A.: Do moderators of the optimistic bias affect personal or target risk estimates? A review of the literature. *Personality and Social Psychology Bulletin* **5**(1), 75–95 (2001).

[89] Hoadley, C.M., Xu, H., Lee, J.J., Rosson, M.B.: Privacy as information access and illusory control: The case of the Facebook news feed privacy outcry. *Electronic Commerce Research and Applications* **9**(1), 50–60 (2010).

[90] Acquisti, A., John, L. K., Loewenstein, G.: What is privacy worth?, *The Journal of Legal Studies* **42**(2), 249-274 (2013).

[91] Hui, K.-L., Teo, H.-H., Lee, S.-Y. T.: The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly* **31**(1), 19-33 (2007).

[92] Steijn, W. M. P.: *Developing a sense of privacy: An investigation into privacy appreciation among young and older individuals in the context of social network sites*. Dissertation. Tilburg University (2014) https://pure.uvt.nl/ws/portalfiles/portal/7737309/Steijn_Developing_05_09_2014_emb_tot_06_09_2015.pdf Accessed Dec 2018.

[93] boyd, D.: What does the Facebook experiment teach us? *The Message* (2014). https://medium.com/message/what-does-the-facebook-experiment-teach-us-c858c08e287f Accessed Jan 2019

[94] Livingston, S.: Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media Society* **10**(3), 393–411(2008).

[95] Raynes-Goldie, K.: Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook'. *First Monday* **15**(1), (2010). https://firstmonday.org/article/view/2775/2432 Accessed Jan 2019.

[96] Brandtzæg, P. B., Lüders, M., Skjetne, J. H.: Too many Facebook "friends"? Content sharing and sociability versus the need for privacy in social network sites. *International Journal of Human-Computer Interaction* **26**, 1006–1030 (2010).

[97] Van den Broeck, E., Poels, K., Walrave, M.: Older and Wiser? Facebook Use, Privacy Concern, and Privacy Protection in the Life Stages of Emerging, Young, and Middle Adulthood. *Social Media and Society*, July-Dec., 1 –11 (2015).

[98] Sheehan, K.: An Investigation of gender differences in on-line privacy concerns and resultant behavior. *Journal of Interactive Marketing* **13**, 24–38 (1999).

[99] Jensen, C., Potts, C., Jensen, C.: Privacy practices of Internet users: Self- reports versus observed behavior. *International Journal of Human–Computer Studies* **63** (1–2), 203–227 (2005).

[100] Ackerman, M.S., Cranor, L.F., Reagle, J.: Privacy in e-commerce: examining user scenarios and privacy preferences. In: *Proceedings of the ACM Conference on Electronic Commerce*, pp. 1-8. ACM, Denver, U.S.A (1999).

[101] Sheehan, K. B.: Toward a typology of Internet users and online privacy concerns. *The Information Society* **18**, 21–32 (2002).

[102] Yao, M.Z., Rice, R.E., Wallis, K.: Predicting user concerns about online privacy. *J. Am. Soc. Inf. Sci. Technol*. **58**, 710–722 (2007).

[103] Feng, Y., Xie, W.: Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior* **33**, 153–162 (2014).
[104] Cecere, G., Le Guel, F., Soulié, N.: Perceived Internet privacy concerns on social networks in Europe. *Technological Forecasting & Social Change* **96**, 277–287 (2015).
[105] Nguyen, D.H., Mynatt, E.D.: *Privacy mirrors: understanding and shaping socio-technical ubiquitous computing systems*. Georgia Institute of Technology, USA (2002).
[106] Kavakli, E., Kalloniatis, C., Loucopoulos, P., Gritzalis, S.: Incorporating Privacy Requirements into the System Design Process: The PriS Conceptual Framework. *Internet Research* **16**(2), 140-158 (2006).
[107] Kalloniatis, C., Kavakli, E., Gritzalis, S.: PriS Methodology: Incorporating Privacy Requirements into the System Design Process. In: Mylopoulos, J., Spafford, G. (Eds.). *Proceedings of the SREIS 2005 13th IEEE International Requirements Engineering Conference – Symposium on Requirements Engineering for Information Security* pp. 1-9. IEEE, France, Paris (2005).
[108] Kalloniatis, C., Kavakli, E., Gritzalis, S.: Addressing privacy requirements in system design: The PriS method. *Requirements Engineering Journal* **13**(3), 241-255 (2008).
[109] Pavlidis M., Mouratidis, H., Kalloniatis, C., Islam, S., Gritzalis, S.: Trustworthy Selection of Cloud Providers based in security and privacy requirements: Justifying trust assumptions. In: Furnell, S., Lambrinoudakis, C. (Eds). Proceedings of *10th International Conference on Trust, Privacy and Security in Digital Business*, pp. 185-198. Springer, Czech, Prague (2013).
[110] Kramer, N.C., Haferkamp, N.: Online Self-Presentation: Balancing Privacy Concerns and Impression Construction on Social Networking Sites. In: Trepte, S., Reinecke, L.(Eds). *Privacy online: Perspectives on privacy and self- disclosure in the social web*, pp. 127-141. Springer, Heidelberg (2011).
[111] Litt, E.: Understanding social network site users' privacy tool use. *Computers in Human Behavior* **29**, 1649-1656 (2013).
[112] Young, A.L, Quan-Haase, A.: Privacy Protection Strategies on FACEBOOK, Information. *Communication & Society* **16**(4), 479-500 (2013).
[113] Johnson, M., Egelman, S., Bellovin, S.M.: Facebook and privacy: it's complicated. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS 2012)*, pp. 1–15. ACM, Washington (2012).
[114] Vanderhoven, E., Schellens, T., Valcke, M.: Exploring the usefulness of school education about risks on social network sites: a survey study. *J. Media Liter. Educ*. **5**(1), 285–294 (2013)
[115] Vanderhoven, E., Schellens, T., Valcke, M.: Educating teens about the risks on social network sites: an intervention study in secondary education. *Communicar Sci. J. Media Educ*. **43**(XXII), 123–131 (2014)
[116] Vanderhoven, E., Schellens, T., Vanderlinde, R., Valcke, M.: Developing educational materials about risks on social network sites: a design-based research approach. *Educ. Tech. Res. Dev*. **64**, 459–480 (2016)

[117] Del Rey, R., Casas, J.A., Ortega, R.: The ConRed program, an evidence-based practice. *Communicar Sci. J. Media Educ.* **39**(XX), 129–137 (2012)
[118] Sideri, M., Kitsiou, A., Tzortzaki, E., Kalloniatis, C., Gritzalis, S.: "I have learned that I must think twice before…". An educational intervention for enhancing students' privacy awareness in Facebook. In: Katsikas, S., Zorkadis, V. (eds). *Proceedings of the 7th International Conference, E-Democracy 2017,* pp. 79-94. Springer, Cham (2017).
[119] Foucault, M.; *Power, Knowledge, Ethics*. Ipsilon, Athens (1987) (in Greek).
[120] Eriksen, T.H.: *Tyranny of the Moment. Fast and Slow Time in the Information Age*. Pluto Press, London (2001).
[121] Jakala M., Berki, E.: Communities, Communication and Online Identities. In: Warburton, St., Hatzipanagos, St. (eds). *Digital Identity and Social Media*, pp. 1-13. IGI Global, USA (2013).
[122] Lampropoulou, E.: *Internal Security and Control Society*. Kritiki Publ., Athens (2001) (in Greek).
[123] Norris, C.: From personal to digital: CCTV, the panopticon and the technological mediation of suspicion and social control. In: Lyon D. (ed.). *Surveillance and Social Sorting: Privacy Risk and Automated Discrimination*, pp. 249-281. Routledge, London (2003).
[124] Lyon, D.: *The Electronic Eye: The Rise of Surveillance Society-Computers and Social Control in Context*. Wiley, UK (2013).
[125] Kandias, M., Mitrou, L., Stavrou, V., Gritzalis, D.: Which side are you on? A new panopticon vs. privacy. In: *Proceedings of 2013 International Conference on Security and Cryptography (SECRYPT)*, pp. 1-13. IEEE, Reykjavik, Iceland (2013).
[126] Mitrou, L., Kandias, M., Stavrou, V., Gritzalis, D.: Social media profiling: a panopticon or omniopticon tool?. In: *Proceedings of the 6th Biannual Surveillance and Society Conference*, pp. 1-15. Spain, Barcelona (2014).
[127] Melucci, A.: *Social Theory in the Information Era*. Trotta Editorial (2002).
[128] Daskalakis E.: *Criminology of social reaction: traditions*. Sakkoulas Publ., Athens (1985) (in Greek)
[129] Viégas, F.B.: Blogger's expectations of privacy and accountability: an initial survey. *J. Comput.-Mediated Commun*. **10**(3), 1–31 (2005).
[130] D'Souza, G., Phelps, J. E.: The Privacy Paradox: The Case of Secondary Disclosure. *Review of Marketing Science* **7**, 1-29 (2009).
[131] Solove, D.J.: A taxonomy of privacy. *Law Rev*. **154**(3), 477–560 (2006).
[132] Islam, M.B., Watson, J., Iannella, R., Geva, S.: *What I Want for my Social Network Privacy*. NICTA, Australia (2014).
[133] Beldad, A., De Jong, M., Steehouder, M.: I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior* **27**(6), 2233-2242 (2011).
[134] Midgley, J.: *Social development. The developmental perspective in social welfare.* Sage, London (1995).
[135] Holmberg, J. (ed.): *Making development sustainable*. Island Press, Washington D.C. (1992).

[136] Streeck, W.: Productive Constraints: On the Institutional Conditions of Diversified Quality Production. In: Street, W. (ed). *Social Institutions and Economic Performance*, pp. 1-40. Sage, London (1992).
[137] Cooke, Ph., Morgan, K.: *The Associational Economy*. Oxford University Press, Oxford (1998).
[138] Uphoff, N.: *Local institutional development: an analytic sourcebook with cases.* Kumarian, West Hartford (1986).
[139] Salmen, L. F.: *Listen to the people. Participant-observer evaluation of development projects.* Oxford University Press, Washington (1987).
[140] Henderson, S.E.: Expectations of privacy in social media. *Mississippi Coll. Law Rev*, **31**, 227-24. (2012).
[141] Cohen, J.E.: What privacy is for. *Harvard Law Rev*. **126**(7), 1904–1933 (2013).