International Journal of Media and Cultural Politics
Volume 6 Number 1
 doi: 10.1386/macp.6.1.81/1

TATJANA TARASZOW
Cyprus Neuroscience & Technology Institute

ELENA ARISTODEMOU
Cyprus Neuroscience & Technology Institute

GEORGINA SHITTA
Cyprus Neuroscience & Technology Institute

YIANNIS LAOURIS
Cyprus Neuroscience & Technology Institute

AYSU ARSOY
Eastern Mediterranean University

Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook™ profiles as an example

ABSTRACT

In the context of the European Safer Internet project 'EU Kids Online', the aim of this article is to address how young people deal with privacy issues in social networking

KEYWORDS

Facebook™
privacy

social networking sites
Safer Internet
online communications
youth
Web 2.0
interactive
gender differences
profile

sites, using Facebook™ as an example. The study on which it is based examined the type of personal and contact information young people disclose through their profiles. In addition, it assessed gender differences in the disclosure of personal and contact information. A hundred and thirty-one Facebook member profiles were observed, selected to fit the European Commission's youth age range of 13–30. Results suggested that most people regardless of gender enter full name, facial pictures, hometown and e-mail addresses in their profiles. However, males are more likely than females to disclose mobile phone number, home address and instant messaging (IM) screen names. Consistent with the past literature, youth, especially between the ages of 18 and 22, seem unaware of the potential dangers they are facing when entering real personal and contact information in their profiles while accepting 'friendship' requests from strangers. Recommendations for future research include investigating the levels of awareness young people have when disclosing information about themselves that can potentially harm them in more ways than one.

INTRODUCTION TO SOCIAL NETWORKING SITES

The number of web-based social networks, also known as social networking sites (SNSs), has increased exponentially within the last few years. boyd and Ellison (2007) define SNSs as web-based services that allow individuals to (1) construct a public or semi-public profile, (2) communicate with other users with whom they share a connection and (3) view and navigate through their own list of connections as well as those of others. Grounded in the concept of computer-based communities, Acquisti and Gross (2006: 2) describe SNSs as 'Internet-communities where individuals interact with others through profiles that represent their selves'. The existence of various characterizations suggests that there is no clear-cut definition for what SNSs are, but for the purposes of this article one was adapted from boyd and Ellison (2007). SNSs simplify communication by integrating digital communication and publishing, supporting an individual's construction of their digital identity and providing a single-point access to various communication tools, thus enabling communication across time and space (Dwyer et al. 2008). There are hundreds of SNSs, with diverse technological features, supporting a wide range of interests and practices, for example, based on common language or shared racial sexual, religious or nationality-based identities (boyd and Ellison 2007).

Members use SNSs for a number of purposes. The main motivation is communication, interaction and maintaining relationships (Dwyer et al. 2007). Popular activities include finding friends, dates and jobs; networking or looking for new acquaintances; extending one's network; updating others on activities and whereabouts; sharing information, photos, videos and music; receiving updates about events; inviting people to events; getting updates from friends; presenting an idealized presentation of oneself; sending messages privately and posting public testimonials (boyd and Ellison 2007; Dwyer et al. 2007).

CHARACTERISTICS OF SOCIAL NETWORKING SITES

The example of Facebook™ can be used to demonstrate the most common characteristics of SNSs.

Although SNSs have implemented a wide range of technical features, their main characteristic consists of visible profiles that display not only an 'articulated list of friends' (boyd and Ellison 2007), but also detailed personal

information. After joining an SNS, the new member needs to create a profile to 'type oneself into being' (Sundén 2003). To create the profile, the new member is asked to fill out forms with identifying information such as name, age/birthday, gender, hometown and/or location, religion, ethnicity, personal interests, contact information and an 'about me' section. Most SNSs also encourage users to upload a profile photo. Nobody is really forced to join an SNS, create a profile and reveal personal information. But can one, realistically speaking, remain unconnected? Besides the so-called basic information about oneself as described above, Facebook encourages its users to also publish contact details, details about personal interests and activities as well as details about educational background and work.

Another typical characteristic of SNSs is the connection of users with people they already know in real life, that is, existing friends, or to completely new people. All connections to other members are displayed in a list of friends/contacts/fans and are visible to anyone who has been allowed access to the profile. This list contains links to each friend's/contact's/fan's profile. The public display of connections is a crucial component of SNSs (boyd and Ellison 2007).

Most SNSs also provide a feature allowing visitors to leave messages on their friends'/contacts'/fans' profiles. At least one of the following three different mechanisms is offered to SNS members: (1) public messages, (2) private messages and (3) instant messages.

SNSs typically involve leaving public messages on a kind of blackboard, as well as leaving public comments on uploaded pictures, videos, etc. In Facebook, the public message board is called 'The Wall'. All messages published are visible to everyone who has access to the profile.

A private message in SNSs resembles an e-mail: the addressee is the only person who can read the message. In Facebook, the private message section is also organized like an e-mail account with an 'Inbox' to view and read the messages received, to mark messages as unread or to read and delete them; a 'Sent Messages' part to view the messages that the profile owner has sent; and a 'Compose Message' button to write new messages to be sent. A third communication possibility is instant messaging (IM), also known as chat. The receiver immediately receives messages sent in the form of chat so that a real-time conversation is possible.

With respect to privacy issues, different SNSs have different approaches. In some cases, user profiles are by default visible to anyone, as in Friendster™, Tribe.net™ and Hi5™. MySpace™ gives its users the option to choose between a 'public' or 'friends only' profile. When the research reported here started at the beginning of 2008, profiles on Facebook used to be by default visible to any other user unless the profile owner denied permission. A few months later, Facebook changed their settings and made profiles by default visible to friends only, with the option to change one's own profile into a public one. That change on Facebook privacy settings occurred after complaints the company received regarding violations of people's privacy rights.

CONCEPTS OF PRIVACY

As Wildemuth (2008) points out, there is no consensus about a universally accepted definition of privacy. However, four distinct concepts of privacy can be identified, which led Introna (1997) to conclude that privacy is a relative concept that should be seen as a continuum.

The first concept focuses on the full protection of any individual, which according to Warren and Brandeis (1890: 204) includes 'the right to privacy', where privacy is understood as the 'right to be let alone' (Warren and Brandeis 1890: 205). From quite early on, these authors had already noticed that a new discussion and definition of the nature and extent of this protection and privacy is necessary every now and then. Warren and Brandeis also called for a decision about whether and how the law will protect the right to privacy, mentioning unauthorized circulation of individuals' portraits as a contemporary example of invasion of that privacy. From a legal point of view, they argue that any invasion into the privacy that leads to mental suffering is a recognized source for lawful compensation. Moreover, the authors observe a new trend in technology development – 'mechanical devices' (Warren and Brandeis 1890: 205) as they call it – invading, even threatening, each individual's privacy, which leads to the need of another debate on privacy, including introducing protection from new technologies into the privacy concept. Although this was a remarkable perception regarding the nature of privacy at the end of the nineteenth century, this concept is less relevant to our discussion as we have today agreed on a right to privacy that is protected by law. Nevertheless, Warren and Brandeis laid the foundation for a concept of privacy that has come to be known as control over information about oneself.

The second concept is based on Westin's (1967) idea that privacy means one's control over one's own personal information. The author's definition of privacy therefore reads:

> Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.
>
> (Westin 1967: 7)

Westin, moreover, argues that individuals are continually engaged in a process of adjustment to find a balance between the desire for privacy and the desire for disclosure of one's self to others. New technology, according to Westin, alters this balance between privacy and disclosure. The author, however, does not elaborate how and in which direction the equilibrium is being changed through technology. Westin's concept not only includes the notion of loss of privacy in terms of losing one's control over one's personal information – a very important aspect to be considered as it is almost impossible to know when, how and to what extent others circulate one's own personal information in SNSs – but it also takes into account the balancing act individuals have to undertake when using new technologies, specifically SNSs. Nevertheless, the concept lacks a discussion of consequences for both the person losing his/her privacy and the person invading the privacy of somebody else (Wildemuth 2008).

The third concept focuses on privacy standing in competition with two very different ideas: the 'monitored' and the 'searchable' part of anyone's life (Lessing 1998). In his essay 'The Architecture of Privacy', Lessing defines the idea of the monitored part of one's day-to-day existence as the one that others can see, notice and respond to (e.g. as one walks down the street, one's behaviour is or can be monitored). The idea of the searchable part of one's life represents traces of information that one 'leaves' behind in the environment. For example, the scribbling in a diary leaves a record of one's thoughts; they can be searched. Objects in a house represent a record of what one possesses; they too can be searched. The recordings on a telephone answering machine

are a record of who called and what they said; they can be searched as well. The parts of one's digital life do not easily pass away. Instead, they remain to be reviewed – technology and law permitting.

According to Lessing (1998: 1), privacy is 'what's left after one subtracts, as it were, the monitored, and the searchable, from the balance of social life'. He continues, stating that 'life where less is monitored is a life more private' and 'life where less can be searched is a life more private' (Lessing 1998: 1). Looking at technology, more precisely, the Internet in general and SNSs in particular, individual life becomes more and more monitored as well as searchable as every activity online can be monitored and leaves a footprint or record. Any person – in a private capacity, in a commercial one, as part of the state or part of the police force – who has access to another person's profile in an SNS can monitor that person's activities as well as search for any personal information. Hence, Lessing's concept of privacy is of high relevance for the discussion and research on privacy in SNSs.

The fourth concept sees privacy as 'the immunity from the judgment of others' (Johnson 1992: 272), referring to those aspects of a person's life that are culturally recognized as being safe and protected from others' judgements. Johnson also associated privacy with blocking; his model stresses the blockage of illegitimate attitudes and judgements on the part of others. The author himself admits that his conception of privacy does not imply a clarification of which aspects of one's life are culturally recognized and therefore immune from the judgements of others. Applying Johnson's concept theoretically to new technologies, each technology most probably has its own culture and therefore its own type of immunity from the judgements of others – an idea that has yet to be explored through research.

All four concepts of privacy mark the vagueness and importance that such a concept includes. Present-day legislature, however, has managed to ensure some degree of privacy in everyday life, but the emergence of the Internet and new technologies call for revisiting the issue. New technologies, especially SNSs, arguably, undermine the people's right to privacy, which has taken so much effort to establish in the first place.

PRIVACY IN SOCIAL NETWORKING SITES AND IN FACEBOOK

Internet users, members of SNSs in particular, seem either not concerned about their privacy or not aware of the loss of privacy they suffer during their time online (Wildemuth 2008). Although consumers report that they are concerned about privacy issues (Stark and Hodge 2004), SNSs that encourage their users to reveal and exchange personal information are booming in popularity. At the same time as adults are concerned about the governmental and corporate invasion of privacy (e.g. through the central collection and storing of data about citizens and consumers), the teenagers and young adults freely disclose personal and private information on SNSs (Barnes 2006). Barnes (2006: 3) called this situation the 'privacy paradox', which led Dwyer (2007) to investigate what kind of attitudes individuals hold towards privacy when using SNSs. Dwyer (2007) concluded in her research that privacy is often not expected or undefined in SNSs. Barnes (2006) argues that the privacy paradox occurs when users, especially teenagers, are not aware of the nature of the Internet in general and SNSs in particular. Acquisti and Gross (2006) explain this phenomenon, however, as a disconnection between the users' desire to protect their privacy and their actual behaviour. When using SNSs, people divulge

personal information to strangers as well as to friends. Although the SNSs investigated in the past literature do not force users to reveal personal information, they actually encourage them to do so. That encouragement results in people really disclosing personal information without connecting it with their subsequent loss of privacy.

In comparison to other SNSs, Facebook stands out for both its vast membership and the quality of information in it; in fact, any information is personally identifiable (Acquisti and Gross 2006). As noted earlier, up until the beginning of 2008, by default, members' contact information and additional data – rarely available on other SNSs (e.g. personal interests, education, work) – was shown openly to every other member. Also, by default, members' profiles were searchable and readable by any other member. As privacy settings were by default set to 'public' (meaning they became available to the public and did not include restricted access) and access to the profiles from any Internet user was very easily achieved, Facebook was a totally open site. By default, any member of the social network could see everything that the other members were doing in Facebook due to the fact that Facebook assumed that all users want to share all of their information with their global networks (engtech 2007). Facebook's policy contradicted the current privacy laws that exist in all countries and offered access to its member's private information to the general public. At the end of 2007, Facebook had been urged to improve its privacy settings (Sophos 2007). The violation of privacy resulted in Facebook changing its default settings for privacy to ensure that disclosure of public information is only allowed when the users themselves decide to do so. Thus, by mid-2008, default privacy settings had been changed from Facebook administrators. Members' profiles, contact information and additional data are now visible, readable and searchable by friends only – unless otherwise chosen by each member.

According to researchers (Acquisti and Gross 2006; Gross and Acquisti 2005), an individual's privacy concerns are only a weak predictor of his/her membership in an SNS. In their studies, they showed that individuals concerned about privacy nevertheless join SNSs and reveal great amounts of personal information. Concurrently, some SNS members demonstrated significant misconceptions about the SNS's reach as well as the visibility of their profiles. Similarly, other studies showed teenagers being generally worried about privacy issues and setting their profile to private, yet revealing private information to several hundred people in their friends' list whom they have known only casually (Lenhart and Madden 2007; Livingstone 2008). Furthermore, Livingstone (2008) points out that although teenagers are strongly concerned about privacy online, their conception of privacy – based on being able to control which friend knows what about oneself – does not match the privacy settings of most SNSs. For all those reasons, not surprisingly, privacy and security concerns are being raised by researchers and the press (e.g. Acquisti and Gross 2006; boyd and Ellison 2007).

Various studies have shown that Facebook members reveal a great amount of personal information about themselves openly, while at the same time they are not aware of their privacy options or who can view their profile (Acquisti and Gross 2006; Lampe et al. 2007; Stutzmann 2006a, b). In a study of students from a freshmen class, Stutzmann (2005) found that out of 88% of freshmen who had an active Facebook profile, only 1–3% of them used privacy flags. Moreover, over time, the privacy use dropped from 3% to 1%. In an analysis of how much and which type of information freshmen are sharing with their

fellow students, Stutzmann (2006b) discovered that 75% of the student sample revealed their birthday, hometown, sexual orientation, relationship status and political orientation.

Preliminary results of the study reported here involving youth located in Cyprus showed that, similar to American students, Cypriot Facebook users are willing to share personal information: All Cypriot Facebook members published their real names, 97% revealed their gender, 97% published a facial profile picture of themselves (which identifies them), 51% indicated their hometown and 88% published their birth date (Taraszow et al. 2008). However, few of those Cypriot Facebook users were likely to disclose full contact details. Half of the sample revealed their personal e-mail addresses, but only a tiny minority revealed home address and cell phone number. According to the authors, these findings indicate that most youth are aware not only of the type of information they are publishing in Facebook, but also of the potential dangers related to publishing detailed contact information. The Statistical Service of the Republic of Cyprus (CyStat) in a recent survey on the use of computers and communications in Cypriot households (CyStat 2008) reported that 56.3% of all households own a computer with the vast majority of those being households with dependants. Moreover, for the first trimester of 2008, CyStat reports that 42.9% of all households had access to the Internet. By far, and with an increasing yearly percentage, the most common type of connection in households was DSL (76.2% of households with Internet access). As computer usage in Cyprus is still on the rise, the usage of mobile phones has reached 90.6%, which places Cyprus among the first countries in mobile usage across Europe (CyStat 2008). These statistics suggest that there may be more to come for Cyprus in relation to the use of the Internet, and especially the use of SNSs.

Finally, in another survey-based study, Acquisti and Gross (2006) investigated the type and quality of information revealed in Facebook. Similar to Stutzmann's (2006b) findings, 88% of the students published their birthdays, 58% their political views and 62% their sexual orientation. Surprisingly, many members were aware of the type of information they provide as the majority published their birthday (88%), but only a minority published their home phone number (11%), personal address (27%) or mobile phone number (41%), although the percentage of users who have published their mobile phone numbers is discussable. Moreover, the authors made the interesting observation that if particular information is provided, it is very likely to be of high quality, i.e. complete and accurate.

GENDER DIFFERENCES IN REVEALING PERSONAL INFORMATION

Finally, there is the question of gender differences in this field. Most of the literature on gender differences in SNSs focuses on gender identity (Manago et al. 2008), self-presentation (Magnuson and Dundes 2008) and personal interests such as friendship or dating (Thelwall 2008). Acquisti and Gross (2006) are an exception in that they examined usage differences between male and female Facebook members. Their results suggested that female members were less likely to disclose their sexual orientation, personal address and mobile phone number than male members. Yet this is a rare study. It is thus important to examine the type of information disclosed by users, especially young people, and assess whether males disclose different types of information than females do.

In the light of this literature review, the aim of the study reported in this article was to examine how young males and females deal with privacy issues in SNSs, using Facebook as an example. The study analyses gender differences in the amount and type of personal information young people disclose through their profiles. Specifically, usage was examined based on the following aspects: (1) the percentage of people using a public profile compared to those who have a private profile in relation to the default settings of Facebook; (2) the type of personal information disclosed to others such as profile name, profile image and birth date; (3) the type of contact information disclosed to others such as e-mail, telephone numbers, address and hometown.

THE STUDY

The Facebook profiles of 131 young people (68 females and 63 males) were observed for this study. Ages ranged from 14 to 29 years with a mean age of 21 years and 1 month (SD = 3.829). The age range was decided according to the European Commission's defined age range for youth, which is considered to be from 13 to 30 years. This broad age range was decided by the commission on the basis that activities funded could have people of that age range participate in their programmes. Even though it is a broad range of ages, the commission offers programmes aiming at the involvement of all young people, from the beginning of puberty to the end of young adulthood.

A guide sheet was prepared for the collection of the necessary information from each of the selected profiles. The sheet contained information on the general demographics needed for this study, such as gender and age. It also included sections on the personal information and contact information disclosed by members to the public and/or their friends. As far as personal information is concerned, the following data were recorded (for a full description of the list, refer to Appendix 1):

- Type of profile
- Profile name
- Profile picture
- Birth date

During the collection of the profile name, a note was made as to whether the Facebook user had used a real name, a partial name or a fake name (see Appendix 1). When assessing whether a real name was used or not, the 'real' referred to an actual name as it was not possible to know whether a particular name is a member's authentic name or not.

Since members have the option to publish contact information depending on their preferences, the following data were also recorded (for a full description of the list, refer to Appendix 2):

- E-mail address
- IM screen name
- Mobile phone number
- Other phone number
- Home address
- Hometown
- Website

A random sample of twenty profiles from all searchable members located in Cyprus was initially selected for the study, based on the age range defined as 'youth'. Specifically, from all Facebook members located in Cyprus, those who were aged 13–30 were selected. Following the age selection, twenty profiles were randomly selected to start the first phase of data collection. After recording the required information from these twenty profiles, a record of all their friends that matched the defined age range was made. The whole procedure was completed in four cycles, ending with the collection of information from 131 participants. It is important to note, however, that the participants in this study, that is, those young people whose Facebook profiles were examined, were not aware of this process (direct observation was performed) as it took place in the background with the data collectors not engaging in the participants' online activities.

The data were analysed using the Statistical Package for the Social Sciences (SPSS). Percentages were provided, showing which types of information are mostly revealed by young people to others through Facebook. The chi-square test was then used to examine differences in the disclosure of personal and contact information among males and females.

RESULTS

Before considering gender, some general results are outlined. With respect to the *type of profile*, the majority of the profiles studied were accessible only to friends, that is, they were not open to any Facebook member (76.3%), whereas a much smaller percentage of subjects made their profile publicly available (22.1%). Almost all subjects (89.3%) published a portrait *profile picture* of themselves from which one can identify their gender and approximate age. A few subjects (7.6%) chose to post a non-portrait image as their profile picture, for example, a group picture or joke image that is not related to a person, such as a cartoon or celebrity image. A minority of the sample did not provide any profile picture (2.3%). Moreover, the majority of the subjects published their real *names* (96.2%) in comparison to a partial name (3.8%) or a fake name (0.0%). Similarly, all participants (100%) disclosed their *birth date*; more particularly, the majority (99.2%) disclosed their full birth date providing information on date, month and year; a minority (0.8%) partly disclosed their birthday with information on date and month; none of the participants revealed absolutely nothing about their birthday. Figures 1–4 provide a summary of young people revealing personal information in Facebook.

As far as contact details are concerned, Figure 5 shows how many Facebook users disclose identity information in the form of contact details. The majority of the subjects in the sample publicly showed their *e-mail address* (64.1%). Fewer subjects revealed an *IM screen name* (10.7%). The same pattern applies to the revelation of *mobile phone number*: Only a few Facebook members published their mobile phone number (10.7%). Very few subjects published *another phone number* such as their landline or a second mobile number (2.3%). Similarly, only a minority (10.7%) of the participants revealed their *home address* on Facebook. Half of the sample indicated their *hometown* (54.2%) on Facebook. Furthermore, a small number of subjects revealed their *website* (5.3%).

Looking at the possible gender differences among Facebook users and their disclosure of personal and contact information, female and male young people were compared with respect to various elements. No significant difference was found with respect to having a public or non-public 'profile' between female

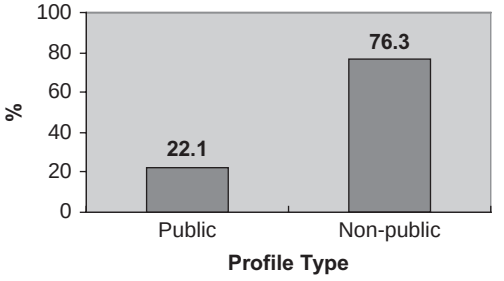

Figure 1: Percentages of young Facebook users having a public and non-public profile.

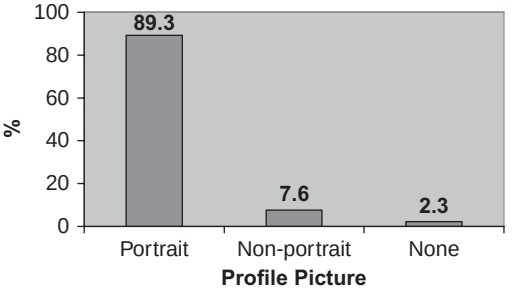

Figure 2: Percentages of young Facebook users' type of profile picture.

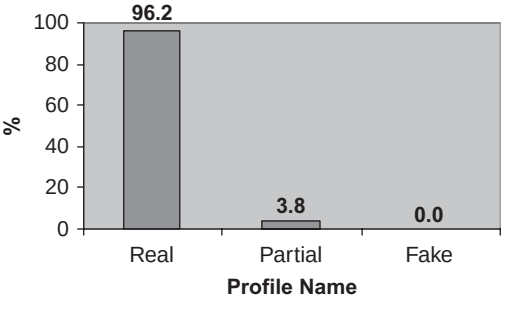

Figure 3: Percentages of young Facebook users' type of profile name.

and male users ($\chi^2 = 0.091$, $df = 1$, $p > .05$). This means, female (23.5%) and male (20.6%) Facebook users did not differ in their choice of having a public profile. Also, the chi-square test did not reveal any significant differences on the revelation of a portrait 'profile picture' among females and males ($\chi^2 = 4.34$, $df = 2$, $p > .05$). Specifically, both female (85.3%) and male (93.7%) Facebook members published mainly a portrait picture. With respect to the 'profile name', again female and male Facebook users did not significantly differ in publishing their real name ($\chi^2 = 0.14$, $df = 1$, $p > .05$). What this means is that both female (95.6%) and male (96.8%) users used mostly their real name as their profile name. Furthermore, results showed no significant difference in the disclosure of the 'birth date' among female and male Facebook members ($\chi^2 = 0.93$, $df = 1$, $p > .05$). The majority of both female (98.5%) and male (100%)

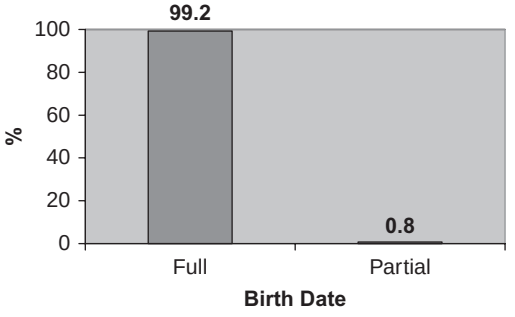

Figure 4: Percentages of young Facebook users' type of birth date.

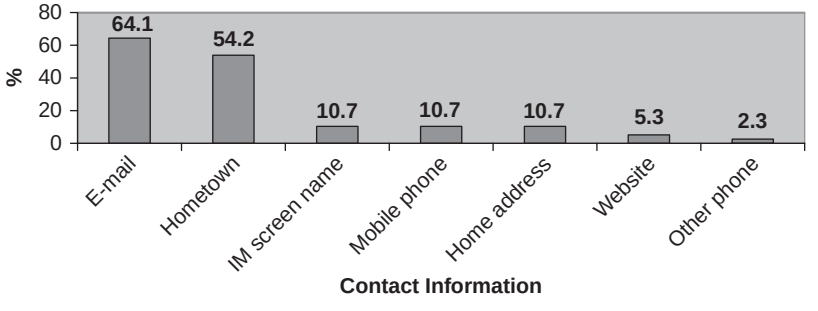

Figure 5: Percentages of young Facebook users revealing contact information in their profiles.

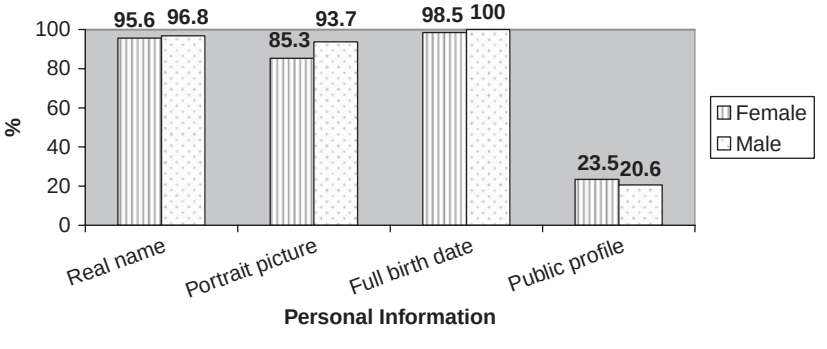

Figure 6: Percentages of female and male Facebook users with respect to disclosing personal information such as real name, portrait picture and full birth date, as well as to having a public profile.

users revealed their full birthday with date, month and year. Figure 6 demonstrates the disclosure pattern of personal information between female and male Facebook users.

As regards contact information data, the results showed that there was a significant difference among females and males in the disclosure of 'mobile number' ($\chi^2 = 5.99$, $df = 1$, $p < .05$). Specifically, what the results suggest is that males (17.5%) are more likely to disclose their mobile phone number than females (4.4%). Moreover, there was a significant difference between females

and males as regards the disclosure of their *e-mail address* ($\chi^2 = 2.82$, $df = 1$, $p < .1$). More male (71.4%) Facebook users revealed their e-mail address than female (57.4%) users did. In examining disclosure of some *other phone number*, again males (4.8%) differed from females (0.0%) in terms of being more likely to reveal another phone number ($\chi^2 = 3.37$, $df = 1$, $p < .1$). Likewise, there was a significant difference in the disclosure of *home addresses* among females and males, as more males (15.9%) revealed their address than females (5.9%) ($\chi^2 = 3.42$, $df = 1$, $p < .1$). In disclosing a personal *website*, results showed no significant difference among females (2.9%) and males (7.9%) ($\chi^2 = 1.62$, $df = 1$, $p>.05$). Female (8.8%) and male (12.7%) Facebook users also did not significantly differ in publishing their *IM screen names* ($\chi^2 = 0.57$, $df = 1$, $p > .05$). Neither female (50.0%) nor male (58.7%) Facebook members differed in disclosing their *hometown* ($\chi^2 = 0.84$, $df = 1$, $p > .05$). Figures 7 and 8 illustrate the differences in disclosure of contact information among female and male Facebook users.

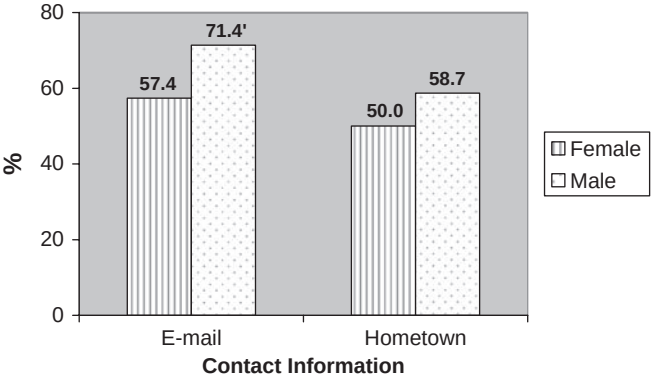

Figure 7: Percentages of female and male Facebook users with respect to disclosing e-mail address and hometown.
' indicates a trend of significant difference among males and females on the 10% level.

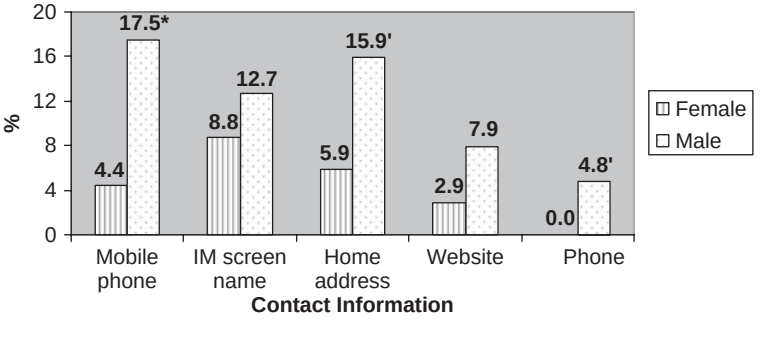

Figure 8: Percentages of female and male Facebook users with respect to disclosing mobile phone number, IM screen name, address, website and other phone number.
** indicates a significant difference between gender on 5% level.*
' indicates a trend of significant difference between gender on 10% level.

After finding that almost no significant gender differences were observable in the disclosure of contact information among young people on Facebook, and since some results were found to be only just statistically significant, a more detailed examination was conducted. Controlling for age, gender differences as regards the disclosure of contact information for four different age groups (13–17, 18–22, 23–27 and 28–30) were again examined. Grouping of ages was on the basis that teenagers of age 13–17 are in secondary education, 18–22 is the maximum time required for the first university degree, 23–27 is the approximate age of a master's degree and 28–30 is the range where most young adults begin their professional life. Interestingly enough, results revealed that there is an association between (1) gender and revelation of e-mail address, (2) gender and revelation of IM screen names as well as (3) gender and revelation of home address among people aged 18–22 years old. In detail, the chi-square test comparing females and males aged 18–22 on whether they disclose their 'e-mail address' to others yielded a significant difference at the .05 level ($\chi^2 = 6.29$, $df = 1$, $p < .05$). This result suggests that females of this age (45.2%) are less likely to disclose their e-mail address on their profiles than males of this age (75.8%). Similarly, results suggested that males (19.4%) aged 18–22 are more likely to disclose their 'IM screen names' than females (3.3%) of the same age group ($\chi^2 = 3.85$, $df = 1$, $p < .05$). Finally, the chi-square test was found to be significant at the .05 level in the disclosure of 'home address' among females and males aged 18–22 ($\chi^2 = 4.87$, $df = 1$, $p < .05$). Again, this result suggests that males (27.3%) are more likely to disclose their home address on their profiles than females (6.5%) aged 18–22.

Important findings were also discovered in the examination of profile representations based on the four age groups: 96.6% of the participants aged 13–17 had their profile set as private, whereas among participants aged 18–22 only 64.1% had that. For the other two age groups, 84% of the participants aged 23 –27 had set their profile as private, whereas 76.9% of those aged 28–30 had done so. The chi-square test showed that there is a significant difference among age group and profile type ($\chi^2 = 11.249$, $df = 3$, $p < .05$). In all other types of disclosure, no significant differences were found among participants of the four age groups.

DISCUSSION AND CONCLUSIONS

The aim of the present study was to examine how young people deal with privacy issues in SNSs, when comparing members that have a public profile on Facebook to those that have a private one. The results showed that the vast majority have a private profile available to friends only. One possible explanation for this can come from the recent change in the default privacy settings that was enforced in mid-2008 by the Facebook company. Unfortunately, evidence that can reveal whether users set their profile as private or public themselves cannot be obtained. Past literature, however, reports that people are creating profiles without being aware of privacy settings (Acquisti and Gross 2006; Lampe et al. 2007; Stutzmann 2006a, b; Wildemuth 2008). So, if someone created a profile when the default privacy setting was set to public, s/he would not consciously realize that his/her personal and contact information was made available to all members of the site, irrespective of the friendship list. In the same way now, when people are creating a profile on Facebook, they do not realize that their profile is by default on 'privacy' and thus their information is

available only to friends. This may explain why most people seem to have a private profile rather than a public one.

It is worth noting that even though profiles are set to private, people tend to accept as their friends complete strangers (e.g. Lenhart and Madden 2007; Livingstone 2008). Thus, revealing personal and contact information on their profile only to friends can be equally threatening as having a public profile. In examining the type of information that young people disclose on Facebook profiles, results showed first that most people use a facial picture of themselves in their profiles through which gender and an age estimate can be identified. This can pose a risk to members as it removes their protection of anonymity and allows them to be identified in real life as well. Besmer and Lipford (2008) argue that the increased access to an individual's physical appearance through high-quality profile pictures has led to such images being used for purposes that were not intended by the owner. For instance, profile pictures are easily downloadable and can appear in any other website, pornographic websites included. Some employers perform Internet checks on job applicants in general and those on Facebook in particular (Palank 2006). Pictures in Facebook profiles have also been used by law enforcement officers in criminal investigations (Romano 2006).

Second, the results showed that the majority of the sample studied used their full names in their profiles instead of using only their first name or a nickname. Providing a full name can make users more easily traceable in their real life. For example, a thorough Internet search of a full name might result in a vast amount of real-life information about a particular person, such as former high school, workplace, profession, hobbies and other activities. Interestingly enough, it was also found that the whole sample used in this study disclosed their birth date in their profiles. Even though this kind of information alone cannot pose a threat for the privacy and security of members, in conjunction with other personal information disclosed in these profiles it can expose members' identities and threaten their privacy, and, taken to its extreme, their lives. Not without good reason, Acquisti and Gross (2006; Gross and Acquisti 2005) emphasize the existence of a potential ability to reconstruct users' social security numbers utilizing a combination of information often found in profiles, such as their full name, date of birth and hometown.

In examining the contact information disclosed by young people on their Facebook profiles, results showed that the majority of people reveal their e-mail address to others and their IM screen names. This in itself may not be considered serious, but it opens a whole new spectrum of risks: that of giving strangers the option to use instant messaging or e-mails, to either verbally harass or bully. Disclosures of mobile phone number, other phone numbers, home address and a link to a personal website were only reported by a small percentage of the sample under study. However, half of the sample was found to disclose their hometown in their profile. A holistic approach to the disclosure of information by young users shows that usually those who disclose important 'identifying' information also disclose important 'contact' information. Disclosing all types of personal and contact information not only eliminates the privacy of people, but also gives full access to strangers to find them both on the Internet and in their own homes, schools and workplaces. Several incidents have become known through the media, where strangers found potential victims from SNSs, tracked them down, followed them and sometimes abused or even killed them.

Moreover, the examination of gender differences in the disclosure of personal and contact information to Facebook profiles did not reveal much. The

only significant finding as between males and females is that males report more often their mobile phone number than females do, in line with the findings of Acquisti and Gross (2006). As there is a gap in the literature on gender differences and the disclosure of personal and contact information, one can only speculate about possible explanations of this finding. In general, males are considered to be more dynamic and powerful, also less concerned with possible harm. Thus, without thinking too much about it, they reveal their mobile phone number on the Internet.

However, when a second analysis was conducted on gender and the disclosure of personal and contact information while controlling for age, differences among females and males were found in the age group 18–22 as regards three types of information (revelation of e-mail address, revelation of IM screen names and revelation of home address). In all three instances the results showed that males between 18 and 22 are more likely to disclose that kind of information in their profiles than females. One possible explanation of this is that males of this age group are developmentally changing (moving from teens to adulthood) and want to present themselves as more independent, powerful and available to other people. Another explanation might be found in the different effects the Internet has on attitudes in men versus women. Broos (2005) found that males are more likely to have positive attitudes towards the Internet as well as greater experience in using it. Thus, male Facebook users might react more enthusiastically and therefore reveal more information about themselves.

Last, an examination of age differences in the disclosure of the type of profile revealed significant differences. A very small percentage of people aged thirteen to seventeen years had their profile type set to 'public' whereas all other age groups had a much higher percentage. Again, this can probably be explained by the change in the default setting of Facebook, in which most people who have registered before the change in the privacy setting are not only more likely to be the older ones, but are more likely not to have realized that their profile is being viewed by any member of Facebook without restrictions.

Youth are attracted by online SNSs as they offer appealing opportunities for various activities, communication, interaction and sharing of thoughts and digital assets. At the same time, SNSs raise privacy concerns among parents, politicians and young people themselves because many members of SNSs publicly reveal personal and often identifying information. In May 2008, for example, the European Youth Forum held its first pan-European youth meeting on Safer Internet in order to increase the dialogue between children and decision makers on Safer Internet issues as well as to raise awareness about the most effective ways to protect minors and young people online (Shitta et al. 2008). Among SNSs, Facebook stands out for its popularity and enormous number of members. Moreover, members openly share a variety of identifiable unique and personal information.

This study used the methodology of observing profiles, which, as the search of the past literature suggests, is an approach that has rarely been used in this field. The study quantified patterns of information revelation from the actual field data, that is, examining profiles, rather than conducting surveys. It examined the habits of young Facebook members with respect to publishing personal and contact information. Caution is required when interpreting the results of this study. Even though the results are consistent with the past literature, the sample under analysis was fairly small, which affects the generalizations one can make. In addition, people in this study were primarily selected

from Cyprus and circled around friendship lists that were mostly Cypriots. This is not to say that results reflect only Cypriot habits on Facebook, but rather that youth in other countries may need to be studied further to more generally validate the results found here.

In accordance with previous findings (Acquisti and Gross 2006; Stutzman 2006b), Facebook youth-members are willing to share personal information, that is, real full name, gender, hometown and full date of birth, which can potentially be used to identify details of the members' real life, such as their social security numbers. Hence, by publishing personal information in Facebook, young people make themselves easily identifiable to anybody in their friends' list: close friends, acquaintances and even strangers. This study confirmed that young people reveal crucial aspects of their personal and contact information that can enable their identification and potentially their victimization in more ways than one. In this context, and in order to fend off illegal activities online in general, the Cypriot Safer Internet Awareness Node 'CyberEthics' (http://www.cyberethics.info) was set up. One of its purposes is to educate not only young people, but also parents and teachers about possible risks when joining SNSs, as well as how to protect oneself without being afraid of using the Internet. In cooperation with the EU Kids Online project, CyberEthics is also in the process of conducting a quantitative survey in order to assess whether young people in Cyprus are aware of Internet risks and if they know how to deal with such risks (Aristodemou et al. 2008). Moreover, clarifying young people's knowledge and consciousness of privacy issues in SNSs with surveys or interviews is part of the continuing research agenda of this project.

It is crucial that future research assesses the level of 'conscious' awareness young people have about the possible dangers they put themselves into, when entering authentic private and contact information. In addition, future research should aim to investigate the type of information disclosure occurring in such other SNSs that do not ensure private profiles as their default privacy setting. Finally, a more detailed examination of gender and age differences in the revelation of personal and contact information is recommended.

ACKNOWLEDGEMENTS

This research was conducted by the New Media Lab of CNTI (Cyprus Neuroscience and Technology Institute) and supported by the EU Kids Online project (European research on cultural, contextual and risk issues in children's safe use of the Internet and new media). We would like to thank Artemis Hadjigeorgiou, Vaggelis Stamatiou and Theofania Chaaralambous as well as several students of the Faculty of Communication and Media Studies at the Eastern Mediterranean University for their support during the data collection phase, and two anonymous referees for their useful comments.

REFERENCES

Acquisti, A. and Gross, R. (2006), 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook', *Proceedings of the 6th Workshop on Privacy Enhancing Technologies*, Cambridge, UK.

Aristodemou, E., Taraszow, T. and Laouris, Y. (2008), 'Young Cypriot Internet Users: A Quantitative Survey in the Context of EU Kids Online', *Paper*

presented at the Conference Child and Youth Research in the 21st Century: A Critical Appraisal, Nicosia, Cyprus, May.

Barnes, S.B. (2006), 'A Privacy Paradox: Social Networking in the United States', *First Monday*, 11: 9, http://firstmonday.org/issues/issue11_9/barnes/index.html. Accessed 21 July 2008.

Besmer, A. and Lipford, H.R. (2008), 'Privacy Perceptions of Photo Sharing in Facebook', *Poster Presented at Symposium on Usable Privacy and Security (SOUPS)*, Pittsburgh, PA, 23–25 July.

boyd, d.m. and Ellison, N.B. (2007), 'Social Network Sites: Definition, History, and Scholarship', *Journal of Computer-Mediated Communication*, 13: 1, article 11, http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. Accessed 3 June 2008.

Broos, A. (2005), 'Gender and Information and Communication Technologies (ICT) Anxiety: Male Self-Assurance and Female Hesitation', *CyberPsychology and Behavior*, 8, pp. 21–31.

Cyprus Safer Internet Awareness Node (2008), 'CyberEthics', http://www.cyberethics.info.

CyStat (2008), 'Computer and communications usage survey in Cypriot households', *Ministry of Finance*.

Dwyer, C. (2007), 'Digital Relationships in the "MySpace" Generation: Results from a Qualitative Study', *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS)*, Hawaii.

Dwyer, C., Hiltz, S.R. and Passerini, K. (2007), 'Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace', *Proceedings of the Thirteenth Americas Conference on Information Systems*, Keystone, Colorado, USA, 9–12 August.

Dwyer, C., Hiltz, S.R. and Widmeyer, G. (2008), 'Understanding Development and Usage of Social Networking Sites: The Social Software Performance Model', *Proceedings of Hawaii International Conference on System Sciences (HICSS)*, http://csis.pace.edu/∼ dwyer/research/DwyerHICSS2008.pdf. Accessed 3 June 2008.

engtech (2007), 'How to use Facebook without losing your job over it', *Internet Duct Tape*, 8 March, http://internetducttape.com/2007/03/08/how-to-use-Facebook-without-losing-your-job-over-it/. Accessed 15 July 2008.

Gross, R. and Acquisti, A. (2005), 'Information Revelation and Privacy in Online Social Networks (The Facebook case)', *Proceedings of ACM Workshop on Privacy in the Electronic Society (WPES)*, Alexandria, VA, USA, 7 November 2005.

Introna, L.D. (1997), 'Privacy and the Computer: Why We Need Privacy in the Information Society', *Metaphilosophy*, 28, pp. 259–75.

Johnson, J.L. (1992), 'A Theory of the Nature and Value of Privacy', *Public Affairs Quarterly*, 6, pp. 271–88.

Lampe, C., Ellison, N. and Steinfield, C. (2007), 'A Face(book) in the Crowd: Social Searching versus Social Browsing', *Proceedings of the 20th Anniversary Conference on Computer Supported Cooperative Work*, Banff, AB, Canada, pp. 167–70.

Lenhart, A. and Madden, M. (2007), 'Teens, privacy and online social networks: How teens manage their online identities and personal information in the age of MySpace', http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf. Accessed 23 July 2008.

Lessing, L. (1998), 'The architecture of privacy', http://lessig.org/content/ articles/works/architecture_priv.pdf.Accessed 3 June 2008.

Livingstone, S. (2008), 'Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression', *New Media and Society*, 10, pp. 459–77.

Magnuson, M.J. and Dundes, L. (2008), 'Gender Differences in "Social Portraits" Reflected in MySpace Profiles', *CyberPsychology and Behavior*, 11, pp. 239–41.

Manago, A., Graham, M., Greenfield, P. and Salimkhan, G. (2008), 'Self-Presentation and Gender on MySpace', *Journal of Applied Developmental Psychology*, 29, pp. 446–58.

Palank, J. (2006), 'Face it: "Book" no secret to employers', *The Washington Times*, 17 July.

Romano, A. (2006), 'Walking a new beat: surfing MySpace.com helps cops crack case', *Newsweek*, 24 April.

Shitta, G., Taraszow, T. and Laouris, Y. (2008), 'Safer Internet forum: A Youth-Driven Initiative for Safer Cyberspace'. *Paper presented at the Conference Child and Youth Research in the 21st Century: A Critical Appraisal*, Nicosia, Cyprus, May.

Sophos (2007), 'Facebook members bare all on networks, Sophos warns of new privacy concerns: Facebook told to change its default privacy settings for geographic networks', 2 October, http://www.sophos.com/pressoffice/news/ articles/2007/10/facebook-network.html. Accessed 18 July 2008.

Stark, D. and Hodge, C. (2004), 'Consumer behaviors and attitudes about privacy: A TNS/TRUSTe study', *TNS/TRUSTe*, http://www.truste.org/pdf/Q4_2004_Consumer_Privacy_Study.pdf. Accessed 9 July 2008.

Stutzmann, F. (2005), 'The freshman Facebook Zeitgeist', http://chimprawk.blogspot.com/2005/10/freshman-facebook-zeitgeist.html. Accessed 5 June 2008.

——— (2006a), 'An evaluation of identity-sharing behavior in social network communities', http://ibiblio.org/fred/pubs/stutzman_pub4.pdf. Accessed 5 June 2008.

——— (2006b), 'Student life on the Facebook', http://www.ibiblio.org/fred/Facebook/stutzman_fbook.pdf. Accessed 3 June 2008.

Sundén, J. (2003), *Material Virtualities*, Peter Lang, New York.

Taraszow, T., Arsoy, A., Shitta, G. and Laouris, Y. (2008), 'How much personal and sensitive information do Cypriot teenagers reveal in Facebook?' *Proceedings of 7th European Conference on e-learning*, Agia Napa, Cyprus, 6–7 November, pp. 606–11.

Thelwall, M. (2008), 'Social Networks, Gender and Friending: An Analysis of MySpace Member Profiles', *Journal of the American Society for Information Science and Technology*, 59, pp. 1321–330.

Warren, S. and Brandeis, L. (1890), 'The Right to Privacy', *Harvard Law Review*, 4, pp. 193–220.

Westin, A. (1967), *Privacy and Freedom*, Atheneum, New York.

Wildemuth, B.M. (2008), 'The illusion of online privacy', University of North Carolina at Chapel Hill, http://sils.unc.edu/~wildem/Publications/CHI2006-Privacy.pdf. Accessed 5 June 2008.

APPENDIX 1. DETAILED DESCRIPTION OF MEASURES OF PERSONAL INFORMATION REVEALED BY FACEBOOK USERS:

- Type of profile
    - Public – open to all Facebook members or
    - Non-public – visible to friends only;
- Profile name
    - Real – name appears to be real,
    - Partial – only first name is given or name appears to be a nickname or an abbreviation, or
    - Fake – name is obviously fake;
- Profile picture
    - Portrait – facial image of the person enabling to recognize the person, gender and age included;
    - Other/non-portrait – non-facial image such as group picture or joke picture; or
    - None.
- Birth date
    - Full – date, month and year are provided;
    - Partial – date and month are provided; or
    - None.

APPENDIX 2. DETAILED DESCRIPTION OF MEASURES OF CONTACT INFORMATION REVEALED BY FACEBOOK USERS

- E-mail address
    - Yes – E-mail address revealed,
    - No – E-mail address not revealed;
- IM screen name
    - Yes – IM screen name revealed,
    - No – IM screen name address not revealed;
- Mobile phone number
    - Yes – Mobile phone number revealed,
    - No – Mobile phone number not revealed;
- Other phone number
    - Yes – Other phone number revealed,
    - No – Other phone number not revealed;
- Address
    - Yes – Address revealed,
    - No – Address not revealed;

- Hometown
    - Yes – Hometown revealed,
    - No – Hometown not revealed;
- Website
    - Yes – Website revealed,
    - No – Website not revealed.

Suggested Citation

Taraszow, T., Aristodemou, E., Shitta, G., Laouris, Y., & Arsoy, A. (2010), 'Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook™ profiles as an example', *International Journal of Media and Cultural Politics* 6: 1, pp. 81–102, doi: 10.1386/macp.6.1.81/1

CONTRIBUTOR DETAILS

Tatjana Taraszow has a Master's degree in psychology with the emphasis on media, educational and organizational psychology as well as political science as an elective subject. She is also a trained mediator. She is a Research Associate for CyberEthics, as well as for an ongoing collaboration between Prof. Peter Gerjets' team at KMRC (Knowledge Media Research Center) and Yiannis Laouris from the New Media in Learning Lab of CNTI. She is also working on the development of the scientific grounding and theory for the role that the 'categorization ability' plays in learning.

Contact: Tatjana Taraszow, Promitheos 5, 1065, Nicosia, Cyprus.
E-mail: tatjana@cnti.org.cy

Dr Yiannis Laouris is a Senior Scientist and President of CNTI and heads the 'New Media in Learning', and the Neuroscience Lab. Neuroscientist (MD, Ph.D.) and systems engineer (MS) he was trained in Germany and the United States. He publishes in the area of learning through computers, the web and mobile phones and about the potential role of IT to bridge the gaps (economic, gender, disabilities, and so on) in our society. He participates in Cost219: Accessibility for All, and Cost276: Knowledge Management. Laouris was a co-founder of a chain of computer learning centres for children (www.cyberkids.com). The curriculum (a new learning theory based on an educationally relevant and socially responsible approach) developed by members of the applicant organization under his supervision received seven international awards for innovation and social responsibility. He is the Executive Director of CyberEthics, the Safer Internet Awareness Node and Hotline for Cyprus.

Contact: 5. Yiannis Laouris, Promitheos 5, 1065, Nicosia, Cyprus.
E-mail: laouris@cnti.org.cy

Georgina Shitta has been with CNTI since February 2008 as an Assistant Coordinator of CyberEthics and as an Office Manager for the organization. She has a BA in Psychology from St. Francis College, Brooklyn, New York. She also has a degree in Secretarial Studies from Frederick Institute of Technology, in Cyprus. She began her career in various working environments as a personal

assistant while continuing her education in psychology. As the Assistant Coordinator of CyberEthics she is supporting the team by preparing material for the website, updating the website, contacting partners for various activities, writing reports, etc.

Contact: Georgina Shitta, Promitheos 5, 1065, Nicosia, Cyprus.
E-mail: georgina@cnti.org.cy

Dr (pend) Aysu Arsoy holds a double major BS degree in Computer Science and Educational Technologies and a Ph.D. (pending) in Visual Communication Arts from the Eastern Mediterranean University (EMU). She has a double appointment, at the EMU as instructor of new media studies and at the Olive Branch Foundation as coordinator of Safer Internet activities that take place in the northern part of the island; she is also a member of the New Media Lab research team.

Contact: Aysu Arsu, Promitheos 5, 1065, Nicosia, Cyprus.
E-mail: aysu@cnti.org.cy

Elena Aristodemou earned a BSc in Psychology from Monash University, Australia and an MSc in Psychological Research Methods (pending defence) from the Open University, United Kingdom. Employed as Research Scientist at the Cyprus Neuroscience & Technology Institute, her interests focus in the fields of learning disabilities, cognitive neuroscience and dangers of the Internet. She currently coordinates two research projects, which investigate the dangers and the perceptions about dangers in Web 3.0 environments such as Second Life. Elena is also the Coordinator of Cyprus's Hotline for Safer Internet and is working on research papers on various themes with the New Media Lab team.

Contact: Elena Aristodemou, Promitheos 5, 1065, Nicosia, Cyprus.
E-mail: elena@cnti.org.cy