Id: 989597

Participatory Educational Research (PER)
Vol.9(3), pp. 22-45, May 2022
Available online at http://www.perjournal.com
ISSN: 2148-6123
http://dx.doi.org/10.17275/per.22.52.9.3

Examining University Students' Online Privacy Literacy Levels on Social Networking Sites

Sinan KAYA*
Faculty of Communication, Department of Journalism, Ondokuz Mayıs University, Samsun, Turkey
ORCID: 0000-0003-3829-2646

Deniz YAMAN
Institute of Social Sciences, Department of Communication Sciences, Süleyman Demirel University, CoHE 100/2000 PhD Scholarship Student, Isparta, Turkey
ORCID ID: 0000-0002-3916-8244

Article history

Received:
01.07.2021

Received in revised form:
01.10.2021

Accepted:
09.10.2021

Key words:
Online privacy literacy,
Use of social networking,
Online privacy behavior,
Usage purpose of social networking sites

This research aims to examine the privacy behaviors of university students on social networking sites. For this purpose, first of all, students' online privacy literacy (OPL) levels on social networking sites were determined. Then it was examined whether these levels differ according to students' gender, frequency of using social networking sites, and the frequency of changing their privacy settings. Also, the relationship between university students' OPL levels on social networking sites and their purposes of using social networking sites and the relationship between university students' OPL levels on social networking sites and social network privacy behaviors were examined. Correlational research and causal-comparative research models were used in the study. The research study group consists of 314 undergraduate students studying in different faculties of a state university. The data of the research were obtained online in the spring semester of 2019-2020. Personal information form, Privacy Settings Experience Questionnaire, Online Privacy Literacy Scale, and Social Privacy Behaviors Questionnaire were used as data collection tools in the research. Descriptive statistics, Mann-Whitney U test, Kruskal-Wallis H test, and Spearman's Rank-Order Correlation were used to analyze the data obtained in the study. The results showed that university students have a high level of OPL. Besides, female students have higher OPL levels than male students, and their OPL levels are similar according to the social networking sites used and the frequency of changing the privacy settings on these sites. In addition, it was determined that there was a low level of positive correlation between students' use of social networking sites to follow the agenda and news, like posts or comment on posts, and their privacy behaviors on Facebook and OPL levels on social networking sites.

* Correspondency: sinan.kaya@omu.edu.tr

Introduction

Developments in communication technologies have brought about changes in the way the individual presents himself. Especially with the mobile phone and social media being a part of human life, private life has been moved to the virtual environment; individuals have produced, changed, and revealed themselves through technology (Ager, 2011). The revolutionary changes brought about by mobile technologies and the internet, which provides the functionality of these technologies in the social lives of individuals and the relatively new habits these changes bring to them, cause current debates about the phenomenon of privacy and the emergence of discourses on the necessity of reshaping the boundaries of personal privacy in the context of technology. Social networking sites (SNSs) allow individuals to create public or "semi-public" profiles in virtual space and interact with other users with whom they share their interests.

In virtual worlds, individuals are in constant interaction with each other both socially and professionally. Considering the large number of active users of SNSs, the level of concerns regarding the protection and privacy of personal information of users also arises. Publishing relatively sensitive and private information in these areas opens the user to public scrutiny. It may lead to permanent records that may adversely affect the user's life in the future. Information published on these sites can lead to security risks such as identity theft, online stalking, cyberbullying, and social engineering (Williams et al., 2009). In particular, as a requirement of the online interaction feature of SNSs, individuals' sharing their information, feelings, and thoughts on these platforms, whether they are aware or not, facilitates the emergence of privacy problems. For example, factors such as which information will be shared with whom and within what limitations affect users' perceptions of privacy and security in the online environment. With these situations in mind, users' attitudes and underlying risk perceptions also become essential to protect against privacy and security threats (van Schaik, Jansen, Onibokun, Camp & Kusev, 2018).

The internet has become a part of social life and has also created a challenging environment to protect personal privacy. The fact that documents, photos, and personal information shared in virtual space through social networking applications can be accessed, and some changes can be made on them has caused some privacy problems for internet users. Violations of privacy in the online environment can also cause individuals to suffer great social, financial, and psychological harm (Saeri, Ogilvie, La Macchia, Smith & Louis, 2014).

The fact that concerns about privacy change according to person, time and culture makes it difficult to define the concept of privacy and determine its boundaries. Despite this, the measures that can be taken to protect the information of people who participate in the online environment for collecting data, expressing opinions, and having fun in this process constitute the framework of online privacy (Aslanyürek, 2016; Strauss & Rogerson, 2002; Wu, Lau, Atkin & Lin, 2011). This framework includes the privacy and security level of personal information shared on the internet, consciously or unconsciously, and concerns about privacy and security (Aslanyürek, 2016). One of the main reasons individuals face privacy issues online is their desire to see and be seen. This desire to see and be seen starts from the birth of the individual. So much so that they have tried to make their voices heard, starting from their infancy. The desire to see and be seen contains an element of observation and control (Barbarosoğlu, 2013). The basis of the surveillance element is to stay abreast of (someone or something), ripple through something, and have something hung up and salted. In the past, those who tried to keep people under such control were not welcome, and these people were branded as voyeurs (who spied on the person without the person's permission or

unannounced). However, by dint of the developing communication technologies and social networks, the "those who show" have become the people themselves (Çelikoğlu, 2008). From this point of view, the protection of privacy in online social networks can be seen as a paradox or contradiction (Dienlin, Masur & Trepte, 2021). Because the primary purpose of participating in social networks is to maintain and expand one's social relations by sharing the individual's feelings, thoughts, and information, mostly personal. The informal nature of social networks, the possibility to communicate in a few words using status updates or other types of content such as photos and videos, the prevalence, and user-friendliness motivate users to post frequently. This motivation enables users to disclose significant amounts of personal information voluntarily (Debatin, 2011). In this respect, social networks, which work with the principle of circulating more information among more users, have a structure that does not prioritize privacy. Because the individual who is accessible through the social network and trying to take attention of other users also pushes the limits of online privacy and even removes these limits with voluntary disclosure (Bostancı, 2019).

It is seen that individuals' concerns about privacy in online environments are increasing compared to the past. Individuals stated that this increase in anxiety was due to the rise in their social privacy awareness, that they would suffer a lot in their private lives when their privacy was violated, and that they had some experiences that changed their perspective on the concept of privacy (Hoofnagle, King, Li & Turow, 2010). Johnson, Egelman and Bellovin (2012), in a study investigating the privacy concerns of Facebook users, found that users are most concerned about cyber hackers and sexual abusers who hijack their accounts and share inappropriate content on their profiles. Dienlin and Trepte (2015) categorized privacy types related to privacy in online social networks as informational, social, and psychological privacy and examined each of these privacy types within the framework of the Facebook sample. As a result of the study carried out in the context of the theory of planned behavior, it was revealed that individuals' online privacy concerns, attitudes, and intentions are indirect indicators of privacy behavior.

Although online privacy and personal information security have been widely researched in the literature, online privacy literacy (OPL) is a relatively new topic in research (Bartsch & Dienlin, 2016; Debatin, Lovejoy, Horn & Hughes, 2009; Weinberger, Zhitomirsky-Geffet & Bouhnik, 2017a). Online privacy literacy, which encompasses a conscious concern for maintaining privacy in online environments and practical strategies to protect privacy, is seen as a combination of declarative knowledge expressed based on online privacy-related facts and procedural understanding namely the know-how; the knowledge of the *modus operandi* (Debatin, 2011; Trepte et al., 2015). In terms of declarative information, OPL includes users' knowledge of the technical aspects of protecting data online, laws and regulations, and corporate practices. In terms of procedural information, it refers to the ability of users to implement strategies developed for privacy regulations and data protection (Trepte et al., 2015). Park (2013) stated that high awareness of online surveillance and technical information, including online digital literacy skills, impacts online privacy control behavior. The study differentiated between technical OPL skills (e.g., using data and various tools for privacy control) and social OPL skills (e.g., avoiding disclosing personal information and presenting false personal details).

Protecting personal privacy in daily life is necessary for emotional relaxation, self-assessment, and secure communication. In order to ensure privacy in daily life, there are some privacy behaviors such as locking the doors in the environment, closing the curtains, and speaking in a low voice. These usual behaviors are used to protect and hide privacy. However,

in online environments, individuals never fully can implement privacy behaviors such as locking doors or speaking in a low voice (Trepte & Reinecke, 2011). Attitudes towards the privacy of individuals in online environments are generally limited to some preferences, such as hiding the profile offered to individuals by social networking applications, restricting access by foreigners (Bartsch & Dienlin, 2016). In addition, although SNSs provide privacy settings for users, these settings are not attracted by users due to a lack of technical knowledge and insufficient knowledge of risks. For example, the default sharing feature on Facebook is that the posts can only be seen by that person's entire friend list. A Facebook user who does not configure the privacy settings correctly can be seen, shared, and circulated on SNSs by all of his close and distant friends (Bostancı, 2019; Tüfekçi, 2008). Also, the increase in the thoughts that online services collect personal data about individuals, use this data for secondary purposes, and share it with third parties without permission for purposes that are not expressly stated, raises concerns about online privacy (Bergström, 2015; Hong & Thong, 2013; Hsu & Lin, 2016). While individuals' online privacy concerns and awareness levels increase, it is also seen that this concern and awareness is not reflected in the behavior of revealing their personal information more (Thon & Jucks, 2014; Tüfekçi, 2008).

The technical difficulties that individuals experience in hiding their data may cause them not to think about this issue, experience a feeling of boredom about online privacy, and have problem protecting their online identities (Choi, Park & Jung, 2018). The line of literature on Facebook users, unearth that most of the users are unaware of the surveillance and violation of their privacy, but they have doubts about online privacy (Choi, Park & Jung, 2018; Kalaman, 2017). Research conducted by Rainie and Madden (2015) on users' attitudes towards online privacy and anonymity revealed that most users do not consider or are unaware of the available tools that can improve their online privacy, thus indicating a low level of their attitudes. It is stated that opposing the assumption that young people do not protect their personal information on SNSs, they use their own strategies such as using pseudonyms and giving false information, not giving contact information, using privacy settings, limiting friend requests, deleting tags and photos; thus, it is emphasized that they take specific measures to protect their online privacy (boyd & Hargittai, 2010; Miltgen & Peyrat-Guillard, 2014; Young & Quan-Haase, 2013).

Every behavior such as sharing and commenting on SNSs, to like or dislike other users' posts, and reporting location turns into an essential source of information. When the users' movements on social networks who exhibit these behaviors with their own identity are examined, many ideas about the user can be easily reached. SNSs act as a hidden resume. All kinds of data made visible through the created online profiles are considered within the scope of information privacy. In this respect, information privacy is directly related to online privacy (Bostancı, 2019). Saridakis, Benson, Ezingeard and Tennakoon (2016), in their study conducted to determine the relationship between personal information security, user behavior, and cyber victimization in online environments, found that those who have a high level of control over personal information in social networks and individuals who use social networks to meet their multi-purpose needs are less likely to be victims of cybercrime; on the other hand, it has been determined that users who use social networks only for information sharing and have low privacy awareness are more likely to be victims of cybercrime.

Research on online privacy on SNSs reveal that university students share their personal information on social networks without any concerns or reservations and rarely use privacy preferences in applications (Barth & De Jong, 2017; Gross & Acquisti, 2005), most of the users tend not to read privacy policies and the processing of personal data because they are

long and cumbersome (Custers, Van der Hof & Schermer, 2014; Jones & Soltren, 2005; Meier, Schäwel & Krämer, 2020), nearly half of the university students in the study group did not refer to the concept of privacy when using social networks (Yıldız & Kruegel 2012), if individuals tend to reveal themselves in their social lives, the action of the individual to reveal themselves continues in social networks (Taddicken, 2013), and social network users, although they are aware of all privacy violations, it is seen that their tendency to abandon internet use is low (Aslanyürek, 2016). When the relevant literature is searched, it is seen that university students' online privacy behaviors and awareness have been examined in the context of OPL (Sindermann, Schmitt, Kargl, Herbert & Montag, 2021), transactional information for privacy, privacy policies and terms of service of SNSs (Obar & Oeldorf-Hirsch, 2020), emotional intelligence (Yabancı, Akça & Ulutaş, 2018), use of the tools designated for controlling and enhancing online privacy (Weinberger, Zhitomirsky-Geffet & Bouhnik, 2017a), gender (Weinberger, Zhitomirsky-Geffet & Bouhnik, 2017b), age (Kezer, Sevi, Cemalcilar & Baruh, 2016; Steijn, Schouten & Vedder, 2016), digital literacy, interpersonal trust in the virtual environment, internet and mobile device usage years and daily average usage time of social networking (Karadaş & Kara, 2021; Korkmaz, Korucu & Gürkez, 2019; Vergili & Töngel, 2019), and privacy paradox (Adorjan & Ricciardelli, 2019; Dienlin & Trepte, 2015; Masur, 2021).

The concept of privacy is one of the most critical issues that need to be emphasized and discussed in the 21st-century technology age, where digitalization continues at an incredible pace, and virtual space has become an indispensable part of the individuals. The widespread use of the Internet causes the concept of privacy to differ from its traditional meaning and the debates on the necessity of redrawing its borders. Situations such as cyberbullying and the disclosure of personal data brought by digitalization that individuals are exposed to on online platforms get the concept of privacy back to the agenda. In addition, concern for violations of online privacy and self-protective behaviors are determined by many different factors (Yıldırım, 2016). There are limited studies within the bulk of literature that reported the correlations between OPL and intention to use SNSs, use of online services to protect privacy, intentions to share information, and use of SNSs (Baruh, Secinti & Cemalcilar, 2017). Also, the culture that individuals are situated in, and specifically the meanings that a culture attributes to privacy play an important role in the privacy decision-making (Petronio, 2002). From this point of view, although OPL and related variables were examined in terms of university students from different cultures, no study examining university students in Turkey was found in the literature. The scarcity of studies in the literature examining OPL, which is the focus variable of the research, has been reported. However, it is thought that understanding the variables considered together with OPL in the research within the framework of OPL may be helpful in providing an understanding of the privacy paradox in SNSs. Therefore, it is essential to investigate the privacy behaviors of university students who use SNSs extensively in terms of their OPL levels, purposes, and duration.

This research aims to examine the privacy behaviors of university students on SNSs. For this purpose, first of all, students' OPL levels on SNSs were determined, and then it was examined whether these levels differ according to students' gender, frequency of using SNSs, and changing their privacy settings. In addition, the relationship between university students' OPL levels on SNSs and their purposes of using SNSs and the relationship between university students' online privacy literacy levels on SNSs and social network privacy behaviors were examined. The answers to the following questions were sought for the purpose of the study:

(1) What is the OPL level of students on SNSs?

(2) Do students' OPL levels on SNSs differ according to their gender?
(3) Do students' OPL levels on SNSs differ according to whether they use SNSs or not?
(4) Do students' OPL levels on SNSs differ according to the frequency of their use of SNSs?
(5) Do students' OPL levels on SNSs differ according to the frequency of changing their privacy settings on SNSs?
(6) Is there a significant relationship between students' OPL levels on SNSs and their purpose of using SNSs?
(7) Is there a significant relationship between students' OPL levels on SNSs and their privacy behaviors on Facebook?

Method

Research Design

In this study, correlational and causal-comparative design models from quantitative research methods were used. The correlational research model is a research model that aims to determine the existence or degree of covariance between two or more variables. Although the correlational model does not give a real cause-effect relationship, it allows the estimation of the other variable if the situation is known. In causal-comparative design, the causes of a naturally occurring or existing condition and the variables affecting these causes or the results of an effect are determined (Büyüköztürk, Kılıç Çakmak, Akgün, Karadeniz & Demirel, 2016). The research model used in the study within the framework of the research questions is described with the diagram in Figure 1.

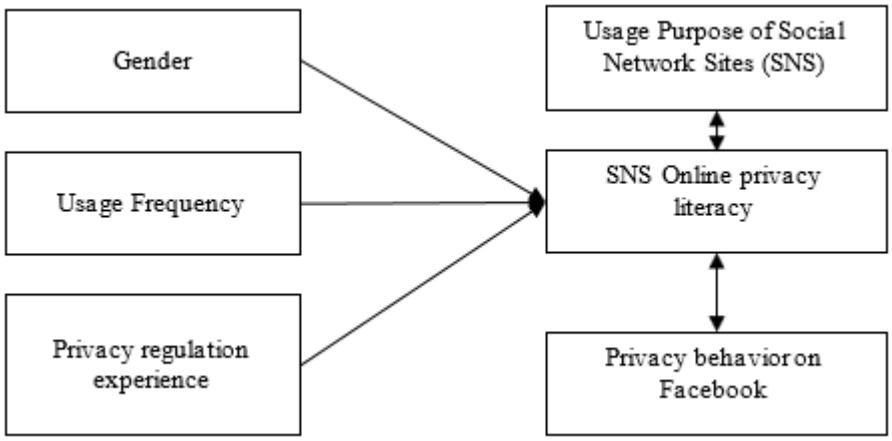

Figure 1. Research Model

Study Group

The study group of this research consists of 335 undergraduate students studying at different faculties of a state university in Turkey. The research data was obtained through an online questionnaire in the spring semester of 2019-2020. 21 out of 335 students who answered all the questions in the survey were not analyzed because they did not have an account in any of the social media networks such as Facebook, Instagram and Twitter. The data obtained of 314 students were analyzed in this study. The ages of the students in the study group vary between 18 and 26 and the average age is 21.4. Demographic characteristics of the students are shown in Table 1, and the average daily usage time of SNSs is shown in Table 2.

Table 1. Demographic characteristics of the study group

Variable	Groups	Number (n)	Percent (%)
Gender	Female	219	67.9
	Male	95	30.3
Grade	1st Grade	68	21.7
	2nd Grade	113	36.0
	3rd Grade	95	30.3
	4th Grade	38	12.0
Total		314	100.0

When Table 1 is examined, it is observed that 67.9% of the students in the study group are female and 30.3% are male students. In addition, 21.7% of the students are first grade, 36.0% are second grade, 30.3% are third grade and 12.0% are fourth grade.

Table 2. Average daily use of SNSs

	Facebook		**Instagram**		**Twitter**	
	n	**%**	**n**	**%**	**n**	**%**
Not have an account	188	59.9	26	8.3	114	36.3
Less than 1 hour	109	34.7	51	16.2	97	30.9
Between 1 and 2 hours	8	2.5	100	31.8	51	16.2
Between 2 and 4 hours	4	1.3	93	29.6	36	11.5
More than 4 hours	5	1.6	44	14.0	16	5.1
Total of who has an account	126	40.1	288	91.7	200	63.7

When Table 2 is examined, it is seen that 40.1% of the students in the study group use Facebook, 91.7% Instagram, and 63.7% Twitter. This shows that university students use Instagram more than Facebook and Twitter, and less use Facebook than Twitter and Instagram.

Most studies have confirmed that interpersonal interaction, time spent, and frequency of interaction on SNSs are positively associated with bridging and incorporating social capital (Kim & Kim, 2017; Lin, 2015; Sánchez-Arrieta, González, Cañabate & Sabate, 2021). Therefore, knowing with whom and how often the users of the SNSs examined in this study communicate is considered important in terms of understanding the results of the research. Seven item questionnaire was used to determine how often the students in the study group communicate with individuals or groups using the SNSs as Facebook, Instagram, and Twitter. Responses to the questionnaire were coded as 1=never, 2=rarely, 3=sometimes, 4=often, and 5=always. The descriptive statistics of the people or groups that the students communicate with using SNSs are presented in Table 3. The act of communicating using SNSs refers to the state of being a friend or following, depending on the characteristics of the SNS.

Table 3. Persons or groups with whom students communicate using SNSs

Person or groups	M	SD	Skewness	Kurtosis
Group of close friends	4.16	1.047	-1.290	1.032
School or classmates	3.53	1.102	-.377	-.644
Family members	3.32	1.264	-.257	-.988
Relatives interviewed face to face	2.79	1.174	.325	-.683
Far away friends that are not seen often	2.57	1.025	.409	-.189
Far away relatives that are not seen often	2.18	1.149	.822	-.111
Lecturers	2.11	.978	.663	.105

When Table 3 is examined, it is seen that the students communicate primarily with their close friend's group using SNSs, and they communicate with the lecturers the least. It can be said that students often become friends or follow them by using SNSs with close friends, class or school friends, and family members with whom they can communicate face-to-face. Table 4 shows the descriptive statistics on how often the students in the study group change their privacy settings on social networking sites in a year.

Table 4. Descriptive statistics on students' privacy regulation experience on SNSs

	n	**%**
I do not know	60	19.1
Never changed	86	27.4
1-3 times	129	41.1
4-6 times	22	7.0
7-9 times	11	3.5
10-12 times	3	1.0
13 times and more	3	1.0
Total	314	100.0

According to Table 4, 19.1% of the students stated that they did not have information about changing privacy settings on SNSs. In addition, 27.4% of the students did not make any adjustments to their privacy settings while using SNSs in a year, 41.1% made privacy adjustments 1-3 times in a year, and 12.5% adjusted 4 or more privacy settings in a year.

Data Collection

The data of the research was obtained by the online questionnaire prepared by the researchers with Google Forms. During the data collection process, on the first page of the questionnaire, firstly, the students were informed about the purpose of the research, the data collection tool, and the data will be kept confidential, then it was stated that participation in the study was on a voluntary basis and the students who wanted to participate in the research were asked to answer the scale. The link of the online questionnaire used in the study was shared in the Google Classroom lesson groups where the students conducted their online lesson activities and in the WhatsApp groups of the students. The data collection tools used in the study were presented in the Appendix, Table A1.

Privacy regulation experience

Privacy regulation experience was determined using how often participants changed their privacy settings on social networks in a year (Bartsch & Dienlin, 2016). For this purpose, a single item ordinal scale was used which includes the following options; *1= Never Changed, 2= 1-3 times, 3= 4-6 times, 4= 7-9 times, 5= 10-12 times,* and *6= 13 times and more.* 19.1% of the students (n=60) stated that they did not know the privacy setting. When the data obtained from the students who knew how to edit their privacy settings were analyzed, it was calculated as M=1.92 and SD=0.94 (n=254). It would be fair to state that the average score of the students' experience of regulation of their privacy settings is low. Accordingly, students do not or rarely regulations their privacy settings.

Online Privacy Literacy

In this study, the "Online Privacy Literacy Scale" developed by Bartsch and Dienlin (2016) was used to determine the ability of students to edit their privacy settings in social networks. In the study conducted by Bartsch and Dienlin (2016), on six items, respondents indicated their agreement on a scale ranging from *1 = I absolutely do not know how to do this*

to *5 = I completely know how to do this*. it was determined that the scale is a valid (χ^2 = 0.75, df = 2, p .69, CFI = 1, TLI = 1, RMSEA < 0.01, %90 CI [<0.01, 0.06]) and reliable (Cronbach alfa α = 0.84) scale. Bartsch and Dienlin (2016) used the Online Privacy Literacy Scale for Facebook, but report that it can also be used for other SNSs in their study. Because the hypotheses established in the research were created by generalization of social networking sites. When the items that are included in the scale are examined, it is seen that the items can provide information about privacy literacy on Twitter and Instagram social networking sites. Expert opinions on this issue also report that the scale can be used for Facebook, Twitter and Instagram.

The original language of the scale is English. The scale was translated to Turkish by the researchers. After translation, the scale was prepared as a structure including original item, translated item and proposed form, and given to experts for their opinion. The final version of the scale was created based on expert opinions.

The rating options of the six items 3-point Likert-type scale is *1= I absolutely do not know how to do this, 2= I am undecided, 3= I totally know how to do this completely,* and the scale has a one-factor structure. According to the results of the exploratory factor analysis made with the data obtained from this research, in which six items scale was used, it was seen that the factor loadings of the items in the factor varied between 0.52 and 0.81, and the one-factor explained 44.2% of the total variance. Confirmatory factor analysis showed that construct validity was only moderate ($\chi^2_{(N=314)}$ = 23.108, df = 9, p = .006, χ^2 /df = 2.568, GFI = 0.976, CFI = 0.962, RMSEA = 0.071, IFI = 0.963). According to these values, it could be said that the observed fit values show an acceptable goodness (Kline, 2015). The Cronbach alpha internal consistency coefficient was 0.74. It is considered sufficient for the variance explained in a one-factor scales to be 30% or more (Büyüköztürk, 2018). It could be said that statistically Online Privacy Literacy Scale is a valid and reliable scale that could be used in the identification of the OPL levels of students. For each student, the smallest score that can be obtained from the scale is 1 and the highest score is 3, since the average score of the items is obtained depending on the answers to the scale items. The low score obtained from the scale shows that the level of OPL of the student is low. When the obtained data were analyzed, it was calculated as M=2.70 and SD=0.43.

Social Privacy Behavior

Social Privacy Behavior Scale developed by Bartsch and Dienlin (2016) was used to determine the accessibility of the participants' Facebook profiles. In this scale, participants answered 15 items on an ordinal scale ranging from *1=Only me, 2=Some of my friends/Friends I have designated, 3=All my friends, 4=my friends and their friends,* and *5=Everyone (open to everyone).* Also, the option *I do not know* was provided and coded as missing value. Responses to the items were reverse coded, with higher values indicating stricter privacy behaviors.

The original language of the scale is English. The scale was translated to Turkish by the researchers. After translation, the scale was prepared as a structure including original item, translated item and proposed form, and given to experts for their opinion. The final version of the scale was created based on expert opinions. The item of sexual orientation on the scale was removed from the scale based on expert opinions and the final version of the scale was used with 14 items.

According to the results of the exploratory factor analysis made with the data obtained from

this research, it was seen that the factor loadings of the items in the factor varied between 0.60 and 0.79, and the single factor explained 43.3% of the total variance. The Cronbach alpha internal consistency coefficient was 0.89. It is considered sufficient for the variance explained in a one-factor scales to be 30% or more (Büyüköztürk, 2018). It could be said that statistically Social Privacy Behavior Scale is a valid and reliable scale that could be used in the identification of the privacy behaviors levels of students for Facebook. For each student, the smallest score that can be obtained from the scale is 1 and the highest score is 5, since the average score of the items is obtained depending on the answers to the scale items. When the obtained data were analyzed, it was calculated as M=3.61 and SD=0.73.

Purpose of using social networking sites

A 12-item questionnaire prepared by the researchers was used to determine the participants' purposes for using SNSs. The rating options of the 5-point Likert-type questionnaire are as follows: *1=Never, 2=Rarely, 3=Sometimes, 4=Often,* and *5=Always.* In the analysis of the data obtained, an average score was not obtained in the questionnaire, and each item was evaluated separately. Descriptive statistics of the survey items are presented in Table 5.

Table 5. Descriptive statistics for students' purposes of using SNSs

	M	**Median**	**Mod**	**SD**	**Skewness**	**Kurtosis**
Following the agenda and news	3.93	4	4	0.949	-0.657	-0.129
Sending private messages to my friends	3.93	4	5	1.074	-0.74	-0.234
Like or comment on posts	3.46	4	3	1.178	-0.321	-0.765
Sharing pictures	2.88	3	3	1.212	0.24	-0.738
Sharing an instant message (status)	2.85	3	3	1.203	0.174	-0.829
Sharing academic knowledge	2.71	3	3	1.181	0.243	-0.729
Sending group messages to my friends	2.68	3	3	1.338	0.332	-1.004
Sending messages to my friends' profile page	2.34	2	2	1.176	0.606	-0.495
Sharing videos	2.26	2	2	1.138	0.791	-0.033
Making new friends	2.16	2	1	1.091	0.802	0.148
Sharing location	2.09	2	1	1.11	0.91	0.174
Playing games	2.00	2	1	1.212	1.083	0.162

When Table 5 is examined, it is seen that university students frequently use the SNSs (Facebook, Instagram, and Twitter) examined within the scope of the research to follow the agenda/news and send private messages to their friends. However, it is seen that they frequently use SNSs for the purpose of like or commenting on the posts. It has been determined that students use SNSs less (rarely) for playing games, sharing locations and making new friends compared to other purposes.

Data Analysis

Before the analysis, it was tested whether the data showed normal distribution or not, by looking at the central distribution, skewness, and kurtosis values on the distribution of the average scores obtained from the scale and based on the Kolmogorov-Smirnov (n>30) and Shapiro-Wilk (n<=30) test result (Büyüköztürk, 2018; Morgan, Leech, Gloeckner & Barrett, 2004). Since the ratios of the kurtosis and skewness statistics to the standard error values are

outside the limits of +1.96 and -1.96, the mean scores are not normally distributed for the examined groups (Can, 2014). In Table 6, Shapiro-Wilk statistics are given when the number of observations is less than 30 (n<30), and Kolmogorov-Smirnov statistics are given when the number of observations is 30 or more (n=>30).

Table 6. Kolmogorov-Smirnov and Shapiro-Wilk statistics for the groups

Variable		n	Statistic	p
OPL - Gender	Female	219	0.294	.000
	Male	95	0.251	.000
OPL - Facebook	Non-user	188	0.288	.000
	User	126	0.265	.000
OPL - Instagram	Non-user	26	0.325	.000
	User	288	0.289	.000
OPL - Twitter	Non-user	114	0.278	.000
	User	200	0.289	.000
OPL - Facebook - Usage frequency	A- Less than 1 hour	109	0.269	.000
	B- Between 1 and 2 hours	8	0.292	.043
	C- Between 2 and 4 hours	4	0.441	.000
	D- More than 4 hours	5	0.473	.001
OPL - Instagram - Usage frequency	Less than 1 hour	51	0.297	.000
	Between 1 and 2 hours	100	0.305	.000
	Between 2 and 4 hours	93	0.251	.000
	More than 4 hours	44	0.368	.000
OPL - Twitter- Usage frequency	Less than 1 hour	97	0.261	.000
	Between 1 and 2 hours	51	0.318	.000
	Between 2 and 4 hours	36	0.319	.000
	More than 4 hours	16	0.355	.000
OPL - Frequency of Changing Privacy Settings	Never changed	86	0.283	.000
	1–3 times	129	0.279	.000
	4–6 times	22	0.402	.000
	7–9 times	11	0.377	.000
	10–12 times	3	0.385	.000
	13 times or more	3	0.376	.000
Privacy behavior on Facebook		314	0.123	.000
OPL		314	0.279	.000

After testing the normality of the results is shown in Table 6, whether the OPL levels of the students on SNSs differ according to their genders were analyzed with the Mann-Whitney U test. The Kruskal-Wallis H test was used to determine whether students' OPL levels on SNSs differ according to their use of SNSs and the frequency of changing privacy settings on SNSs. The relationship between students' OPL levels on SNSs and their purposes of using SNSs, and the relationship between OPL levels on SNSs and social network privacy behaviors were analyzed by Spearman's Rank-Order Correlation. Statistical significance level was taken as .05 in the analysis using SPSS software.

Findings

The findings obtained from the research are presented below, taking into account the order of the research questions. Descriptive statistics about the OPL levels of university students on SNSs are shown in Table 7.

Table 7. Descriptive statistics about OPL levels on SNSs

	N	M	SD	Median	Mod	Min	Max	Skewness	Kurtosis
OPL	314	2.702	0.43	3	3	1	3	-1.601	2.332

According to Table 7, it can be said that university students' OPL levels (M=2.7) on SNSs are high. The Mann-Whitney U test was used to reveal whether the OPL levels of university students on SNSs differ according to gender. Analysis results are presented in Table 8.

Table 8. Mann-Whitney U test of OPL levels on SNSs by gender

	Gender	n	Mean Rank	Sum of Ranks	U	p
OPL	Female	219	164.82	36095	8800	.019
	Male	95	140.63	13360		

As seen in Table 8, it was determined that there was a significant difference between male and female students in terms of OPL levels on SNSs [U=8800, p<.05, η^2=0.13]. According to this finding, it can be said that female students have higher OPL levels on SNSs than male students.

The Mann-Whitney U test was used to determine whether the OPL levels of university students on SNSs differ according to the use of Facebook, Instagram and Twitter, which were examined within the context of the research. According to the results of the analysis, it was determined that there was no significant difference in terms of OPL levels in SNSs between those who used Facebook, Instagram and Twitter and those who did not. The results of the analysis results are presented in Table 9.

Table 9. Mann-Whitney U test results according to Facebook, Instagram and Twitter usage status of OPL levels on SNSs

	Using Status	n	Mean Rank	Sum of Ranks	U	p
OPL - Facebook	Non-user	188	158.74	29843.5	11610.5	.75
	User	126	155.65	19611.5		
OPL - Instagram	Non-user	26	151.02	3926.5	3575.5	.68
	User	288	158.09	45528.5		
OPL - Twitter	Non-user	114	157.05	17903.5	11348.5	.94
	User	200	157.76	31551.5		

The Kruskal-Wallis H test was used to determine whether university students' OPL levels on SNSs differ according to the frequency of their use of SNSs, and the analysis results are presented in Table 10.

Table 10. Kruskal-Wallis H test results on the usage frequency of SNSs by students' OPL levels on SNSs

	Usage frequency	n	Mean Rank	sd	χ^2	p
OPL – Facebook	A- Less than 1 hour	109	64.58	3	12.40	.006
	B- Between 1 and 2 hours	8	26.88			A-B
	C- Between 2 and 4 hours	4	83.75			B-C
	D- More than 4 hours	5	82.30			B-D
OPL – Instagram	Less than 1 hour	51	141.10	3	3.62	.31
	Between 1 and 2 hours	100	147.93			
	Between 2 and 4 hours	93	135.11			
	More than 4 hours	44	160.50			
OPL – Twitter	Less than 1 hour	97	96.73	3	3.19	.36

	Between 1 and 2 hours	51	97.09
	Between 2 and 4 hours	36	107.31
	More than 4 hours	16	118.91

When Table 10 is examined, it is seen that the OPL levels on SNSs differ according to the frequency of Facebook usage of the students [χ^2(sd=3, n=126)=12.40, p<.05, η^2=0.10]. The results of Mann-Whitney U tests to determine which groups the difference originated from showed that it was between those who used Facebook for 1 to 2 hours and others. There was no significant difference between the OPL levels of SNSs according to usage frequency of Instagram [χ^2(sd=3, n=288)=3.62, p>.05] and Twitter [χ^2(sd=3, n=200)=3.19, p>.05] by the students. It is possible to said that the OPL levels of the students on SNSs are similar according to the frequency of their use of Twitter and Instagram.

The Kruskal-Wallis H Test was used to determine whether university students' OPL levels on SNSs differ according to the frequency of changing privacy settings on SNSs. Results of the analysis are presented in Table 11.

Table 11. Kruskal-Wallis H test results about the relationship between students' OPL levels and frequency of changing privacy settings on SNSs

Frequency of Changing Privacy Settings	**n**	**Mean Rank**	**sd**	**χ^2**	**p**
Never changed	86	124.45	5	5.25	.386
1–3 times	129	123.94			
4–6 times	22	149.20			
7–9 times	11	133.64			
10–12 times	3	127.00			
13 times or more	3	187.00			

According to Table 11, the results of the analysis showed that there was no significant difference between OPL levels and frequency of students changing their privacy settings on SNSs [χ^2(sd=5, n=254) = 5.25, p>.05]. In addition, the results of the Mann-Whitney U test conducted to determine whether there is a difference in terms of OPL levels on SNSs between students who know (n=254, Mean Rank=159.81) how to change privacy settings on SNSs and those who do not (n=60, Mean Rank=147.70), showed that there was no significant difference between the two groups [U=7032, p>.05]. In the context of these findings, it can be said that OPL levels of students do not change according to their frequency of changing privacy settings on SNSs.

Spearman's Rank-Order Correlation test was applied to determine whether there is a significant relationship between students' OPL levels on SNSs and their purposes of using SNSs and between OPL levels and privacy behaviors on Facebook. Analysis results are shown in Table 12.

Table 12. The relationship between students' OPL levels on SNSs and their use of SNSs, and between OPL levels and privacy behaviors on Facebook

	OPL level on SNSs r
Following the agenda and news	.16**
Sending private messages to my friends	.09
Like or comment on posts	.12*

Sharing pictures	.02
Sharing an instant message (status)	.05
Playing games	-.09
Sharing academic knowledge	.10
Making new friends	-.07
Sharing location	.00
Sharing videos	.06
Sending messages to my friends' profile page	.07
Sending group messages to my friends	.04
Privacy behavior on Facebook	.13*

* p<.05, ** p<.01

When Table 12 is examined, it is seen that there is a low level of positive correlation between the students' use of SNSs to follow the agenda and news (r=.16, p<.01), to like or comment on posts (r=.12, p<.05), and their OPL levels in SNSs. It was determined that there was no relationship between using SNSs for other purposes and students' OPL levels in SNSs. In addition, it was observed that there was a low level of positive correlation between students' OPL levels and their privacy behaviors on Facebook (r=.13, p<.05). According to this finding, as OPL increases, privacy behaviors on Facebook also increase too.

Conclusion and Discussion

The increase of using SNS causes privacy problems in sharing in virtual environments. The disregard for privacy in social networks causes users to share in these environments without developing a critical perspective. The results of a meta-analytic review of individuals' online privacy concerns and privacy management behaviors confirm online privacy literacy's role in promoting the use of privacy safeguards (Baruh, Secinti & Cemalcilar, 2017).

In this study, which examines university students' OPL levels on SNSs, according to gender, frequency of using SNSs, and frequency of editing privacy settings, it has been found that students have a high level of OPL. Türkten (2018) emphasizes that graduate students are conscious about online privacy, they are careful about sharing their personal information while sharing, but they are concerned about their privacy despite taking every precaution. The results of this study showed that female students' OPL levels were higher than male students. This result may be due to the fact that women have higher privacy concerns than men. Because the literature shows that women have more privacy concerns and privacy tendencies than men (Kalaman, 2017; Livberber Göçmen, 2018; Saeri et al., 2014; Türkten, 2018; Weinberger et al., 2017b). In a study conducted by Fogel and Nehmad (2009) on university students, it was observed that women have more privacy concerns than men. In addition, it was stated that men were more likely to share their personal data such as home addresses and phone numbers on SNSs. Another remarkable point regarding the research findings is that individuals who are members of online sharing sites have a higher tendency to take risks than those who do not use the relevant applications. İvren (2019) found that women's online privacy concerns were higher than men's in a study that examined individuals' privacy concerns and surveillance awareness in social networks and collected data from 1848 participants for this purpose.

In the research, it was determined that the OPL levels of the students were similar according to the social networking site they use. Also, while the OPL did not change according to the frequency of using SNSs by the students using Instagram and Twitter, it was seen that there was a difference in terms of OPL levels according to the frequency of use of the students using Facebook. When the groups that caused this difference were examined, it was determined that those who used Facebook between 1 and 2 hours had a lower OPL level than the others. The findings of the study showed that the OPL levels of the students on SNSs were similar according to the frequency of changing their privacy settings on SNSs. The literature indicates that the duration of use of SNSs has an effect on showing less privacy behaviors in these environments. Because individuals who use SNSs less frequently, generally act more carefully in the online environment and therefore may have more online privacy behavior (Acılar & Mersin, 2015; Bartsch & Dienlin, 2016). For this reason, it can be said that the privacy awareness of users increases as the duration of use of social networking applications increases (Öz, 2014). It has also been observed that as the time spent by the users in the Facebook application increases, they tend to limit the shares they make so that only their friends can access them. Topbaş and Gazi (2016), in their study that aimed to measure privacy concerns in social networks, determined that there was a significant difference between the duration of social network use and privacy concerns of the participants. According to the findings of the related research, it was determined that the current difference was between individuals who use SNSs every day and those who rarely use them; moreover, as the duration of social media use of individuals increases, they pay less attention to their privacy settings. Besides, as the number of followers of individuals using SNSs increases, the value they attach to social network privacy decreases. In this context, it is possible to say that the duration of using SNSs is an essential variable in terms of social network privacy and online privacy behavior.

It was determined that there was a low level of positive correlation between the students' use of SNSs to follow the agenda and news, to like or comment on posts and their OPL levels on SNSs. Furthermore, it was detected that there was a low level of positive correlation between students' OPL levels and their privacy behaviors on Facebook. Sindermann et al. (2021) also reported that there is a low level of positive and significant relationship between OPL and privacy behavior. In the study of Govani and Pashley (2005), in which they examined the users of the social networking site Facebook, it was found that although 84% of the participants were aware of the existing risks related to privacy and the alternative to changing their privacy settings, 48% of the participants were insufficient in making any adjustments. Stutzman, Capra and Thompson (2011) determined that the participants who read the privacy statement shared less content on online social networks. Researchers draw attention to the fact that reading the confidentiality agreement increases the privacy concerns of the participants; however, they underline that this level of anxiety can be minimized by simplifying the privacy settings and the contract text. When the studies in the literature are examined, it can be concluded that the development of online security and privacy awareness takes time (Agosto & Abbas, 2017). This situation can be interpreted as changing privacy settings on SNSs is more affected by the privacy experiences of users on SNSs. Öztürk (2015) reached an important finding that can be evaluated within the context of OPL in his study, which deals with the effect of new media tools on the transformation in the perception of privacy within the framework of undergraduate students. According to the research findings, 65.9% of the 396 participants stated that they did not read the confidentiality agreement when creating a user profile on social media, but 88.9% of the participants stated that they were in control of the personal information they shared on social media. Likewise, similar findings were reached in Budak's (2016) research in which he discussed the concept of privacy and conducted with

the participation of 736 people. Accordingly, 259 out of 736 participants stated that they did not read the terms of use and confidentiality agreement while subscribing to social networks, while 337 participants stated that they read only part of the relevant texts. Therefore, only 140 participants indicated that they had read all the statements in the contract. Töngel (2020) observed that there is a positive relationship between students' digital literacy and privacy awareness in her study, which deals with university students' online privacy awareness. Cengiz (2020), who reached similar findings in his research in which he measured users' perceptions of privacy and privacy, determined a significant relationship between privacy awareness and security awareness. As a result of the study, it has been observed that as the security awareness of social network users increases, privacy awareness also increases. OPL needs to be evaluated within a broad framework of knowledge and skills, such as privacy knowledge, web usage skills, privacy awareness, digital awareness, information about online safety tools, online advertising and web cookies, internet literacy, technical familiarity, awareness of social media applications, social media experience, understanding of online politics, internet and e-commerce experience, awareness of online security measures, knowledge of privacy settings, and social privacy literacy (Baruh, Secinti & Cemalcilar, 2017). Such a comprehensive assessment may be necessary to more effectively examine the variables associated with OPL.

The contributions of the research to the literature can be expressed as follows in terms of the research results. This study has shown that university students have a high level of OPL. However, OPL, which is high, is not reflected in the students' privacy regulation experience. Because the findings of the study showed that students rarely change their privacy settings, and the level of the OPL is similar in terms of changing their privacy settings on SNSs. In general, privacy literacy and attitudes about privacy are two factors that have received a lot of attention as predictors of privacy management behavior. A widely shared argument is that people with higher privacy literacy who have declarative and procedural information are better at protecting their privacy. In the context of the use of social networks, research shows that having technical skills and familiarity with privacy settings are positively related to changing privacy settings (Kezer, Sevi, Cemalcilar & Baruh, 2016). In addition, there is no difference between the students who use the SNSs examined in the study and the students who do not use it, and the OPL levels of the students. The literature shows that social networking platforms differ significantly in terms of the possibilities they create for the selective management of knowledge sharing activities (Bazarova & Choi, 2014). However, there is no difference between those who use Facebook, Twitter and Instagram and those who do not, in terms of their OPL levels.

The results presented in the literature on the level of OPL in terms of gender and the results obtained from the current research show that the level of female students is higher than that of male. These results show that female students who are advantaged in terms of OPL are more likely than male to take action to protect their privacy. However, the way to understand this may be a multidimensional investigation of online privacy behavior in terms of gender with data obtained from large samples.

The low positive relation between OPL and privacy behavior on Facebook is indicating that knowing more about online privacy issues does not necessarily go along with corresponding online privacy protection behaviors. These results suggest that not only OPL, but also more variables may play a role in explaining online privacy behavior. OPL is important not only to feel safe, but also to be safe. Because, as the literature emphasizes, OPL is related to privacy behavior. As a result, when SNS users want to improve their online privacy and want to feel

more secure in SNSs, they should aim to increase their OPL.

Privacy studies emphasize that surveys may not be the most appropriate option to measure individuals' attitudes towards privacy. Because it makes it highly likely that online surveys will exclude individuals with higher privacy concerns. This possibility is seen as a limitation of this study (Baruh, Secinti & Cemalcilar, 2017; Evans & Mathur, 2005).

In the 21st-century technology age, it is indisputable that SNSs are indispensable for individuals' daily and social lives. The concept of privacy still has a role and place in human life despite all the changing conditions over the centuries; although the notion has altered mostly due to the development of technology, it has continued to be a phenomenon that individuals and societies value. Therefore, the issue of privacy in online environments needs to be re-evaluated with different samples in terms of changing environment and individual characteristics. Although OPL seems to be an important factor in online privacy behavior, it remains unclear which psychological characteristics of a person are associated with OPL and behavior. Therefore, in future studies, individual differences in OPL along with online privacy literacy can be investigated. In addition, in a study to be conducted with a large sample, students with high and low OPL can be examined for the purposes of using SNSs, privacy behaviors, privacy regulation experiences, and the SNSs they use.

Appendix

Table A1. Items used in the study.

Variable	**Item**
Frequency of use SNSs	How much time do you spend on average on SNSs in one day? Facebook – Instagram – Twitter (Sosyal ağ sitelerinde bir günde ortalama ne kadar süre geçirirsiniz? Facebook – Instagram – Twitter)
Privacy regulation experience	How often have you already changed your privacy settings on SNSs in a year? (Sosyal ağ sitelerinde gizlilik ayarlarını bir yılda hangi sıklıkla değiştirirsiniz?)
Frequency of communication with people or groups	How often do you communicate with the following people or groups using SNSs? (Aşağıdaki kişi ya da gruplarla sosyal ağ sitelerini kullanarak hangi sıklıkta iletişim kurarsınız?)
Usage Purpose of Social Network Sites (SNS) How often do you use social networking sites for the following purposes? (Sosyal ağ sitelerini aşağıda belirtilen amaçlarla hangi sıklıkta kullanırsınız?)	
UP1	Following the agenda and news (Gündemi ve haberleri takip etmek)
UP2	Sending private messages to my friends (Arkadaşlarıma özel mesaj göndermek)
UP3	Like or comment on posts (Gönderileri beğenmek ya da gönderilere yorum yapmak)
UP4	Sharing pictures (Resim paylaşmak)
UP5	Sharing an instant message (status) (Anlık ileti (durum) paylaşmak)

UP6	Sharing academic knowledge (Akademik bilgi paylaşmak)
UP7	Sending group messages to my friends (Arkadaşlarıma grup mesajları göndermek)
UP8	Sending messages to my friends' profile page (Arkadaşlarımın profil sayfasına mesaj göndermek)
UP9	Sharing videos (Video paylaşmak)
UP10	Making new friends (Yeni arkadaşlar edinmek)
UP11	Sharing location (Konum paylaşmak/Yer bildirimi yapmak)
UP12	Playing games (Oyun oynamak)
Online Privacy Literacy Using the privacy settings and tools of SNSs … (Sosyal ağ sitelerinin gizlilik ayarlarını ve araçlarını kullanarak …)	
OPL1	I know how to delete or deactivate my account (Hesabımı pasif yapabilirim ya da silebilirim.)
OPL2	I know how to restrict access to profile information such as hobbies, interests (İlgilerim, hobilerim gibi profil bilgilerime erişimi sınırlandırabilirim.)
OPL3	I know how to make my profile not accessible via Google (Google arama motoru üzerinden hesabıma erişilmesini ya da profilime bağlantı verilmesini engelleyebilirim.)
OPL4	I know how to control if others tag my name on pictures (Başkaları tarafından paylaşılan fotoğraflarda adımın etiketlenip etiketlenmediğini kontrol edebilirim.)
OPL5	I know how to restrict access to my postings (Paylaştığım iletilere diğer hesapların erişimini kısıtlayabilirim.)
OPL6	I know how to restrict access to my contact information (e.g. name, address) (İletişim bilgilerime (adım, adresim vb.) diğer hesapların erişimini kısıtlayabilirim.)
Social privacy behavior	
SPB1	Contact information such as e-mail or phone (E-posta ya da telefon numarası gibi iletişim bilgilerim)
SPB2	Date of birth (Doğum tarihim)
SPB3	Relationship status (İlişki durumum)
SPB4	Religion (Dini inancım)
SPB5	Current school/university/employment (Mevcut okul ya da eğitim bilgilerim)
SPB6	Residential address (Ev adresim)

SPB7	Who can see what others post on your profile? (Başkalarının profilimde paylaştığı gönderiler)
SPB8	Interests (music, sports, hobbies) (İlgi alanlarıma ait bilgiler (beğendiklerim, hobilerim vb.))
SPB9	Status updates/activity feeds (Durum güncellemelerim)
SPB10	List of friends (Arkadaşlarımın listesi)
SPB11	Photos (Fotoğraflarım)
SPB12	Videos (Videolarım)
SPB13	Political orientation (Siyasi görüşüm)
SPB14	Current location (Konum bilgilerim)

References

Acılar, A., & Mersin, S. (2015). The relationship between Facebook usage and privacy concern among university students. *Electronic Journal of Social Sciences, 14*(54), 103-114. https://doi.org/10.17755/esosder.71918

Adorjan, M. & Ricciardelli, R. (2019). A new privacy paradox? Youth agentic practices of privacy management despite "nothing to hide" online. *Canadian Review of Sociology, 56*(1), 8-29.

Ager, B. (2011). *Sanal benlik [The Virtual self]*. (V. Hacıoğlu, Trans.) İstanbul: Babil Publishing.

Agosto, D. E., & Abbas, J. (2017). "Don't be dumb-that's the rule I try to live by": A closer look at older teens' online privacy and safety attitudes. *New Media & Society, 19*(3), 347-365. https://doi.org/10.1177/1461444815606121

Aslanyürek, M. (2016). Internet and Social Network Users' Opinions and Awareness Regarding Internet Security and Online Privacy. *Maltepe University Communication Faculty Journal, 3*(1), 80-106.

Barbarosoğlu, F. (2013). *Şov ve Mahrem [Show and Private].* İstanbul: Profil Publishing.

Barth, S., & De Jong, M. D. (2017). The privacy paradox - Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review. *Telematics and informatics*, 34(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56*, 147-154. https://doi.org/10.1016/j.chb.2015.11.022

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26-53. https://doi.org/10.1111/jcom.12276

Bazarova, N. N., & Choi, Y. H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication, 64*, 635-657. http://dx.doi.org/10.1111/jcom.12106

Bergström, A. (2015). Online privacy concerns: A Broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavio*r, 53, 419-426. https://doi.org/10.1016/j.chb.2015.07.025

Bostancı, M. (2019). Digital Parents' Perception of Privacy in social media. *AJIT-e: Online Academic Journal of Information Technology*, *10*(38), 115-128. https://doi.org/10.5824/1309-1581.2019.3.005.x

boyd, danah, & Hargittai, E. (2010). Facebook privacy settings: Who cares?. *First Monday, 15*(8). https://doi.org/10.5210/fm.v15i8.3086

Budak, H. (2016). *New age new media and new borders of privacy*. (Unpublished doctoral dissertation). Selçuk University, Konya.

Büyüköztürk, Ş. (2018). *Sosyal Bilimler İçin Veri Analizi El Kitabı [Manual of data analysis for social sciences]*, (24th edition). Ankara: Pegem Publishing.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö.E., Karadeniz, Ş. ve Demirel F. (2016). *Bilimsel Araştırma Yöntemleri [Scientific Research Methods]*. Ankara: Pegem Akademi Publishing.

Can, A. (2014). *SPSS ile Bilimsel Araştırma Sürecinde Nicel Veri Analizi [Quantitative Data Analysis in Scientific Research Process with SPSS]*. Ankara: Pegem Publishing.

Çelikoğlu, N. (2008). *Mahremiyet: Kişiye Ait Özel Alanlar Tartışması [Privacy: Discussing Personal Private Spaces]*. İstanbul: İskenderiye Publishing.

Cengiz, A. B. (2020). *User behavior in online social networks: Social network site users' privacy perceptions*. (Unpublished master's thesis). Bahçeşehir University, İstanbul.

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42-51. https://doi.org/10.1016/j.chb.2017.12.001

Custers, B., Van der Hof, S., & Schermer, B. (2014). Privacy expectations of social media users: The role of informed consent in privacy policies. *Policy & Internet, 6*(3), 268-295. https://doi.org/10.1002/1944-2866.POI366

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 47-60). Springer, Berlin, Heidelberg.

Debatin, B., Lovejoy, J.P., Horn, A.K. & Hughes, B.N. (2009). Facebook and online privacy: attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83-108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297. https://doi.org/10.1002/ejsp.2049

Dienlin, T., Masur, P. K., & Trepte, S. (2021). A longitudinal analysis of the privacy paradox. *New Media & Society*. https://doi.org/10.1177/14614448211016316

Evans, J. R., & Mathur, A. (2005). The value of online surveys. *Internet Research, 15*, 195-219.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153-160. https://doi.org/10.1016/j.chb.2008.08.006

Govani, T., & Pashley, H. (2005). Student Awareness of the Privacy Implications When Using Facebook. Unpublished paper presented at the *Privacy poster fair" at the Carnegie Mellon university school of library and information science*, 9, 1-17. Retrieved from http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf

Gross, R., & Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks (The Facebook Case). In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (pp. 71-80).Virginia.

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, *37*(1), 275-298.

Hoofnagle, C., King, J., Li, S., & Turow, J. (2010). *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* (April 14, 2010). Available at SSRN: https://ssrn.com/abstract=1589864 or http://dx.doi.org/10.2139/ssrn.1589864

Hsu, C. L., & Lin, J. C. C. (2016). An empirical examination of consumer adoption of internet of things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior*, *62*, 516-527. https://doi.org/10.1016/j.chb.2016.04.023

İvren, B. (2019). *Social media surveillance: A research on the privacy concerns and surveillance awareness of users on facebook data policy*. (Unpublished master's thesis). Ege University, İzmir.

Johnson, M., Egelman, S., & Bellovin, S.M. (2012). Facebook and privacy: it's complicated. *Proceedings of the Eighth Symposium on Usable Privacy and Security*. SOUPS'12, Washington, DC USA, July, 11-13.

Jones, H., & Soltren, J. H. (2005). Facebook: Threats to privacy. Project MAC: MIT Project on Mathematics and Computing, 1, 1-76.

Kalaman, S. (2017). New media and transformation of privacy: Facebook cases in Turkey. *International Peer-Reviewed Journal of Communication and Humanities Research, 14*(1), 1-19.

Karadaş, E., & Mehmet, K. (2021). Investigation of university students' online privacy awareness in terms of certain factors. *The Journal of Turkish Social Research, 25*(1), 147-162.

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(1), Article 2. https://doi.org/10.5817/CP2016-1-2

Kim, B., & Kim, Y. (2017). College students' social media use and communication network heterogeneity: Implications for social capital and subjective well-being. *Computers in Human Behavior, 73*, 620-628. https://doi.org/10.1016/j.chb.2017.03.033

Kline, R. B. (2015). *Principles and practice of structural equation modelling* (4th ed.). New York: The Guilford Press.

Korkmaz, Ö., Vergili, M., & Töngel, E. (2019). Üniversite öğrencilerinin çevrimiçi mahremiyet farkındalık düzeylerinin incelenmesi [Examining University Students' Online Privacy Awareness Levels]. *100th Year Symposium of Educational Sciences*, Ondokuz Mayıs University, Samsun.

Korucu, A. T., & Gürkez, Ş. (2019). An analysis of online privacy concerns of teacher candidates. *Participatory Educational Research, 6*(2), 15-25. https://doi.org/10.17275/per.19.9.6.2

Lin, J. H. (2015). The role of attachment style in Facebook use and social capital: Evidence from university students and a national sample. *Cyberpsychology, Behavior, and Social Networking, 18*(3), 173-180. https://doi.org/10.1089/cyber.2014.0341

Livberber Göçmen, T. (2018). *Individuals' privacy orientation in social life: A field survey on social network users*. (Unpublished doctoral dissertation). Selçuk University, Konya.

Masur, P. K. (2021). Understanding the effects of conceptual and analytical choices on 'finding' the privacy paradox: A specification curve analysis of large-scale survey data, Information, Communication & Society, 1-19. https://doi.org/10.1080/1369118X.2021.1963460

Meier, Y., Schäwel, J., & Krämer, N. (2020). The Shorter the Better? Effects of Privacy Policy Length on Online Privacy Decision-Making. *Media and Communication, 8*(2), 291-301. doi:https://doi.org/10.17645/mac.v8i2.2846

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems, 23*(2), 103-125. https://doi.org/10.1057/ejis.2013.17

Morgan, G. A., Leech, N. L., Gloeckner, G. W., & Barret, K. C. (2004). *SPSS for Introductory Statistics: Use and Interpretation*. Second Edition. London: Lawrance Erlbaum Associates.

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128-147. https://doi.org/10.1080/1369118X.2018.1486870

Öz, M. (2014). Changes in use and perception of privacy: Exploring Facebook users' privacy concerns and awareness of privacy implications. *Journal of Yaşar University, 35*(9), 6245-6254.

Öztürk, A. (2015). *The impact of new media tools on the transformation of intimacy perception*. (Unpublished master's thesis). Sakarya University, Sakarya.

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research, 40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Petronio, S. (2002). *Boundaries of privacy*. New York: State University of New York Press.

Rainie, L., & Madden, M. (2015). *American's privacy strategies post-Snowden*. Pew Research Center. https://www.pewresearch.org/internet/2015/03/16/americans-privacy-strategies-post-snowden/

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior. *The Journal of Social Psychology, 154*(4), 352-369. https://doi.org/10.1080/00224545.2014.914881

Sánchez-Arrieta, N., González, R. A., Cañabate, A., & Sabate, F. (2021). Social Capital on Social Networking Sites: A Social Network Perspective. *Sustainability, 13*(9), 5147. https://doi.org/10.3390/su13095147

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change, 102*, 320-330. https://doi.org/10.1016/j.techfore.2015.08.012

Sindermann, C., Schmitt, H. S., Kargl, F., Herbert, C., & Montag, C. (2021). Online Privacy Literacy and Online Privacy Behavior–The Role of Crystallized Intelligence and Personality. *International Journal of Human–Computer Interaction, 37*(15), 1455-1466. https://doi.org/10.1080/10447318.2021.1894799

Steijn, W., Schouten, A., & Vedder, A. (2016). Why concern regarding privacy differs: The influence of age and (non-) participation on Facebook. *Cyberpsychology-Journal of Psychosocial Research on Cyberspace, 10*(1), article 3. http://dx.doi.org/10.5817/CP2016-1-3

Strauss, J., & Rogerson, K. S. (2002). Policies for online privacy in the United States and the European Union. *Telematics and Informatics, 19*(2), 173-192. https://doi.org/10.1016/S0736-5853(01)00012-0

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior, 27*(1), 590-598. https://doi.org/10.1016/j.chb.2010.10.017

Taddicken, M. (2013). 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*, 248-273. https://doi.org/10.1111/jcc4.12052

Thon, M., & Jucks, R. (2014). Regulating privacy in interpersonal online communication: The role of self-disclosure. *Studies in Communication Sciences, 14*, 3-11. https://doi.org/10.1016/j.scoms.2014.03.012

Töngel, E. (2020). *Investigation of the university students' online privacy awareness in terms of certain variables*. (Unpublished master's thesis). Amasya University, Amasya.

Topbaş, H., & Gazi, M. A. (2016). Privacy concern measurement on social networks: A search on the students of the University of İnonu. *İnönü University International Journal of Social Sciences, 5*(1), 143-160.

Trepte, S., & Reinecke, L. (2011). The Social Web as a Shelter for Privacy and Authentic Living. Trepte S., Reinecke L. (Eds.) *Privacy Online* (pp.61-73). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-21521-6_6

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale"(OPLIS). *Reforming European data protection* law (pp. 333-365). Springer, Dordrecht. DOI: 10.1007/978-94-017-9385-8_14

Tüfekçi, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science Technology Society*, *28*(1), 20-36. https://doi.org/10.1177/0270467607311484

Türkten, E. (2018). Perception of Masters students' Social Media Privacy: Gümüşhane University Faculty of Communication Example. *The Journal of Akdeniz University's Faculty of Communication, 30*, 143-161. https://doi.org/10.31123/akil.460160

van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior, 78*, 283-297. https://doi.org/10.1016/j.chb.2017.10.007

Weinberger, M., Zhitomirsky-Geffet, M. & Bouhnik, D. (2017a). Factors affecting users' online privacy literacy among students in Israel. *Online Information Review, 41*(5), 655-671. https://doi.org/10.1108/OIR-05-2016-0127

Weinberger, M., Zhitomirsky-Geffet, M., & Bouhnik, D. (2017b). Sex differences in attitudes towards online privacy and anonymity among Israeli students with different technical backgrounds. *Information Research: An International Electronic Journal*, *22*(4), n4.

Williams, K., Boyd, A., Densten, S., Chin, R., Diamond, D., & Morgenthaler, C. (2009). *Social networking privacy behaviors and risks*. Seidenberg School of CSIS, Pace University, USA.

Wu, Y., Lau, T., Atkin, D. J., & Lin, C. A. (2011). A comparative study of online privacy regulations in the US and China. *Telecommunications Policy, 35*(7), 603-616. https://doi.org/10.1016/j.telpol.2011.05.002

Yabancı, C., Akça, F., & Ulutaş, E. (2018). Investigating the Relationship between Anxiety and Emotional Intelligence with Regard to Online Privacy. *Connectist: Istanbul University Journal of Communication Sciences, 54*, 191-218. https://doi.org/10.26650/CONNECTIST406310

Yıldırım, F. E. (2016). Privacy after internet and an investigation upon studies about this topic. *The Journal of Academic Social Science, 4*(33), 568-582.

Yıldız, H., & Kruegel, C. (2012). Detecting social cliques for automated privacy control in online social networks. *2012 IEEE International Conference on Pervasive Computing and Communications Workshops* (pp. 353-359). IEEE.

Young, A. L. & Quan-Haase, A. (2013). Privacy Protection Strategies on Facebook. *Information, Communication & Society*, *16*(4), 479-500. https://doi.org/10.1080/1369118X.2013.777757