Contents lists available at ScienceDirect

Heliyon

journal homepage: www.heliyon.com

Privacy perception and information technology utilization of high school students

Aytac Gogus[a,*], Yücel Saygın[b]

[a] Istanbul Okan Univesity, Faculty of Education, Istanbul, Turkey
[b] Sabancı University, Faculty of Engineering and National Sciences, Istanbul, Turkey

ARTICLE INFO

Keywords:
Information science
Education

ABSTRACT

Mobile technologies are commonly used and are important by high school students, since teens ages 14 to 17 use these open platforms to share information, communication and construction of their desired cyber identity. Accompanying technology for related data privacy within implementing educational applications is yet to be developed. This research was designed to investigate the perceptions of data privacy and the protection of personal data of high school students who are surrounded by the Internet, social media and technology. The perception of high school students' personal data privacy survey was developed and conducted with 1065 high school students (9th grades). The study presents five main themes: (1) ownership and utilization of different technologies and password sharing, (2) Internet utilization and perception of privacy, (3) social media utilization and perception of personal privacy on social media, (4) knowledge level and perception of personal data conservation, (5) Information technology utilization. High school students have a personal data privacy algorithm but persons or institutions outside this algorithm are perceived as a threat to their personal data and are rejected. This research suggests developing practices and techniques to overcome students' concerns about privacy risks that result from the collection and sharing personal data.

1. Introduction

Social networking websites like Facebook, YouTube, Instagram and Snapchat are commonly used and are important by high school students, teen's ages 14 to 17 since teens use these open platforms to share information, communication and construction of their desired cyber identity (Christofides et al., 2009). According to Pew Research Center (2018), 95% of teens have a smartphone or access to one, and also 45% of teens use the Internet 'almost constantly' for online activities. Teens reveal generous amounts of information on social media sites and Internet by connecting with friends, relatives, and others and these activities are important for them to construct or show of their identity, but revealing generous amounts of information may lead to privacy risks (Christofides et al., 2009; Patchin, 2012). For instance, Facebook offers some privacy settings for users to control their information, but still some users are not aware of social media privacy settings and privacy implications (Madejski et al., 2012; Oz, 2014). On the other hand, Facebook users care about their privacy, but they exchange their privacy for a small reward like popularity and identity construction (Rauhofer, 2008). Especially preteen and teens engage in risky activities online and do not take adequate care to protect themselves. Ignorance of privacy settings and privacy implications can cause privacy problems (Patchin, 2012), therefore understanding privacy concerns and privacy awareness is important because those attitudes can affect the evolution of social media (Boyd, 2013; Oz, 2014). The research study on Internet habits and safe Internet use of children in Turkey and Europe (Kasikci et al., 2014) states that the majority of children's Internet skills are not adequate and they are exposed to many online risks, therefore, families, school, policy makers and the Internet service providers should save their children from the Internet risks. According to this study (Kasikci et al., 2014), 24.9% of children in Turkey get in habit which is perceived as the Internet addiction whereas this ratio is 32.1% for Europe, there are some risks of being bullied and being bothered with images both in Europe and Turkey.

The widespread use of information systems and the Internet in schools, and the fact that many processes have been performed on these systems, have increased the importance of data security and students' data protection perception. In the context and culture of this study, The Turkish Ministry of Education has initiated the FATIH project (Movement of Enhancing Opportunities and Improving Technology) with the aim of

[*] Corresponding author.
E-mail address: aytacgogus@gmail.com (A. Gogus).

https://doi.org/10.1016/j.heliyon.2019.e01614
Received 21 September 2018; Received in revised form 5 February 2019; Accepted 26 April 2019

providing equal opportunities in education and improving technology in schools for efficient usage of ICT tools in the learning-teaching processes (FATIH, 2012) in Kpre-12, between years of 2010–2015. Within the scope of the FATİH project (FATIH, 2012), it is aimed to use information technologies more effectively in the learning and teaching process and to improve the technology in the schools. In line with this aim, LCD panels and Internet network infrastructure were provided to the classrooms in the schools and additionally tablet computers were given to teachers and students. Within the FATİH project (FATIH, 2012), accompanying technology for related data privacy within implementing educational applications is yet to be developed. Therefore, this research project aimed to identify the privacy risks that result from the collection, sharing and analysis of the data collected about students, parents, instructors, and school managers, and to develop techniques to overcome those risks. This research was designed to investigate the perceptions of data privacy and the protection of personal data of high school students who are surrounded by the Internet, social media and technology.

Philosophers and legal scholars have worked to conceptualize privacy and fundamentally described as a social construct that reflects the values and norms of everyday people, but how people conceptualize privacy and locate it in their life varies wildly (Baruh et al., 2017; Boyd and Marwick, 2011; Nissenbaum, 2010). Following the widespread adoption of Internet and social network sites (SNSs), scholarly attention has increasingly focused on informational privacy that is individuals' right to have control over the flow of information about them (Baruh et al., 2017; Nissenbaum, 2010) and privacy concerns that refers to individuals' beliefs about the risks and potential negative consequences associated with sharing information (Cho et al., 2010; Zhou and Li, 2014 cited in Baruh et al., 2017). According to the communication privacy management (CPM) theory (Petronio, 2002) that focuses on individuals' (and groups') decision-making processes regarding privacy argues, privacy should not be considered as establishing a maximum boundary for keeping others out, but rather as a negotiation between accessibility and retreat (Baruh et al., 2017; see also, Taddicken, 2014; Trepte et al., 2015). A meta-analysis of Baruh et al. (2017) presents the studies to understand the responsibility of privacy protection to users (Baruh and Popescu, 2015), the influence of individuals' concerns about privacy on use of online services, information sharing, and engaging in privacy protective behavior (e.g., Baruh et al., 2017; Joinson et al., 2010; Walrave et al., 2012), and the relationship between privacy concerns and these behaviors have provided inconclusive results (e.g., Acquisti and Gross, 2006; Debatin et al., 2009; Taddei and Contena, 2013; Tüfekci, 2008). In addition to these privacy literatures, some studies focus on how teens understand privacy and what strategies they take in their efforts to achieve social privacy, and emphasize the implications of teens' practices, revealing the importance of social norms as a regulatory force (Boyd and Marwick, 2011). Informed by the communication privacy management (CPM) theory (Petronio, 2002), this study investigates perceptions of data privacy and the protection of personal data of high school students.

2. Theory

2.1. Communications Privacy Management theory

Communications Privacy Management (CPM) Theory (Mullen and Hamilton, 2016; Petronio, 2002, 2010), is an evidence-based theory centered on understanding the tension between disclosing and protecting private information to control one's personal information and develop privacy rules to help impose this control. As Mullen and Hamilton (2016) state that once information is disclosed, collective ownership of the shared information appears. There are many medium to share the information and need to control data privacy or personal privacy. In school data systems, once the data is shared with teachers, administrators, parents, or ministry of education staff, the personal data moves to a collective privacy boundary. In social media settings, once a person share an information, status, or photos, social media friends become co-owners of the posted information and disclosure of the personal data can occur on a global stage. Therefore, CPM theory investigates both the personal self-disclosure practices and the management of obtaining a collective privacy boundary (Mullen and Hamilton, 2016). CPM theory has been used some studies investigates the privacy dilemmas of students with friends and parents (e.g., Child and Agyeman-Budu, 2010; Child and Westermann, 2013; Mullen and Hamilton, 2016). However, there appears to be a lack of data on students' attitudes towards personal data protection, how adolescents regulate online disclosure and how adolescents impose collective privacy boundary rules. Therefore, this study investigates users' awareness of privacy issues and perceived benefits and risks of utilizing information technologies and social media by focusing on high school students' attitudes and practices.

2.2. Teen attitudes toward teen privacy and data privacy

It is well-known that teenagers and younger children engage in risky activities online and these groups often do not take adequate care to protect themselves online (Clemons and Wilson, 2015; De Souzaa and Dick, 2009; Pew Research Center, 2013; Shear, 2013). Facebook and other social network sites pose severe risks to their users' privacy and users continually negotiate and manage the tension between perceived privacy risks and expected benefits (Debatin et al., 2009; Kaya and Bicen, 2016; Tüfekci, 2008). In addition, educational applications that collect users' information present the opportunity for students' data to be mined; that is, data-mining privileges that are now being granted to some providers of educational applications and services create new risks to preteen and teen privacy (Clemons and Wilson, 2015). High school students' attitudes toward data mining of educational applications, data privacy, and privacy while using mobile technologies, Internet, and SNSs have been examined with different focus in the literature of the different contexts and cultures.

To measure high school students' Internet attitudes, Taiwanese researchers (Chou et al., 2013; Tsai et al., 2001) developed a 6-T -model of Internet attitudes that represent that teens perceived Internet as a Tool for information acquisition, a Toy for pleasure and gaming, a Telephone for communication, a Territory for self-expression, a Treasure of Information and a Trade for selling and buying online. Ozcan and Buzlu (2007) used the Online Cognitive Scale to measure problematic Internet use; the scale includes four dimensions: loneliness/depression, diminished impulse control, distraction and social comfort. Ozcan and Buzlu (2007) observed that the students who scored higher on the scale were less engaged in online activities related to learning and more engaged in online activities related to entertainment. The researchers (e.g. Chou et al., 2016; Masrek et al., 2012; Tsai et al., 2001) state the positive correlation between the Internet attitude and Internet addiction. In addition, researchers (e.g. Chou et al., 2016; Porter and Donthu, 2006; Tsai et al., 2001) state that experienced Internet users are more sensitive to the concept of Internet risks since researchers conclude that less trusting attitudes toward the Internet are more informed attitudes. Therefore, this study includes examining teen attitudes toward teen privacy and data privacy of high-school-aged students in Turkey.

3. Method

3.1. Participants and data collection

This survey study was conducted in 9 high schools at one of the district of Istanbul, Turkey. The research study obtained ethical approval from Sabancı University Research Ethics Committee, also obtained permission from the District Ministry of Education and informed consent was obtained from all voluntary participants. The study was based upon a survey distributed to 9th grade students of these 9 high schools. Self-completion of 45 questions by using paper and pencil method in the classrooms with volunteer student groups is used in this quantitative research study. 1069 students in total completed to fill in the survey but the validated results are reported by using 1065 of these students.

3.2. *Data collection instrument and data analysis*

The perception of high school students' personal data privacy survey was developed in this study. Cross data check method was applied on the answers in completed surveys and surveys with inconsistent answers are excluded from the analysis. Descriptive statistics are used for data analysis by the use of Excel and the Statistical Package for the Social Sciences (SPSS). Also, inferential statistic with an one way analysis of variance (ANOVA) and the Scheffé post hoc tests are conducted for comparisions of means according to school types. The survey included 45 questions (see the Questionnaire) but only 41 questions are included to data analysis by excluding 4 demographic information related students' family background. 41 questions include 2 demographic information and 39 questions related to five themes: five main themes: (1) ownership and utilization of different technologies and password sharing, (2) Internet utilization and perception of privacy, (3) social media utilization and perception of personal privacy on social media, (4) knowledge level and perception of personal data conservation, (5) Information technology utilization.

3.3. *Research questions*

The study has five main questions:

1. What kinds of mobile technologies do the students use and consider the users' privacy?
2. How much do the students attach importance to data privacy and do they take any precaution on conservation of their data privacy?
3. With whom sharing their personal data is okay for the students?
4. Do the students know that protection of personal information is a basic human right and guaranteed by the constitution?
5. How frequently and for which purpose do the students use information technologies?

4. Results

4.1. *Demographic information*

Table 1 presents demographic information of participant high school students who are 15.4 years old in average (N = 1065), of which 60% are female (N = 634) and 40% are male students (N = 423). Participants are from three types of high schools. 42% of the students are from Anatolian High School, 44% of the students are from Vocational High School, and 14% of the students are from Imam Hatip High School (Religion School).

The results of the study are presented with five following sub-titles:

1. Ownership and utilization of different technologies and password sharing
2. Internet utilization and perception of privacy
3. Social media utilization and perception of personal privacy on social media
4. Knowledge level and perception of personal data conservation
5. Information technology utilization

Table 1
Demographic information.

Demographics	Mean and Standard Deviation	Percentage
Age (9th grades)	15.4 (SD = 1.3)	
Gender		
Female		634 (60%)
Male		423 (40%)
Type of School		
Anatolian High School		447 (42%)
Vocational High School		469 (44%)
Imam Hatip High School (Religion School)		149 (14%)

4.2. *Ownership and utilization of different technologies and password sharing*

Table 2 presents the percentages of utilization and ownership of different technologies like computer, laptop, tablet, and smart phone. Among ownership of different technologies, 87.5% of high school students have smart phones while nearly half of the students have computer, laptop and tablet. Only 2% of the students who involved in this project do not own any technological devices and only 1% of them do not use any technological devices. 77.4% of the students (N = 824) share the devices they use with their family member. Only 22.6% of them state that they do not share their devices with anybody.

Fig. 1 presents rates of ownership of different technologies in three types of high school. Rate of the students who owns a technological device is higher in Anatolian high schools than the other high schools.

When comparing data according to school type, an one way analysis of variance (ANOVA) is conducted for ownership of technologies (computer, laptop, tablet, smart phone, or none of them). ANOVA shows that the effect of school type is significant at $p < .001$ level for ownership of laptop F (2,1060) = 15.419, p = .000, tablet F (2,1060) = 10.768, p = .000, smart phone F (2,1060) = 8.959, p = .000, or none of them F (2,1060) = 8.436, p = .000. Post hoc analyses using the Scheffé post hoc criterion for significance indicates that the average number of errors is significantly higher in the Anatolian High School than in the other two schools Vocational High School (Mean Difference = 0.1 for laptop, tablet, and smart phones) and Imam Hatip (Mean Difference = 0.1 for laptop and smart phones), and also the average number of errors is significantly higher in the Vocational High School than İmam Hatip (Mean Difference = 0.08 for only smartphones). By considering students who do not have any of these technologies, the Scheffé post hoc criterion for significance indicates that the average number of errors is significantly lower in the Imam Hatip School (M = 0.06, SD = 0.2) than in the other two schools Vocational High School (M = 0.01, SD = 0.1, Mean Difference = -0.04) and Anatolian High School (M = 0.01, SD = 0.1, Mean Difference = -0.05)."

Sharing password habits are asked as "With whom do you share the password of devices such as your mobile phone/computer/tablet?" Fig. 2 presents the percentages of students who do not share password. Most of the high school students (Fig. 2) are not willing to share the password of their devices with the teachers, the government and other acquaintance, on the other hand, only 35.5% of students do not share password of devices with close friends and only 42.6% of students do not share password of devices with family members.

4.3. *Internet utilization and perception of privacy*

Frequency of Internet utilization, time spent on Internet, perception of privacy related security, accessibility and pursuit of personal information, and privacy habits in daily life and sharing personal information are analyzed.

4.3.1. *Frequency of Internet utilization and daily time spent on internet*

As presented in Table 3, according to the frequency of Internet

Table 2
Utilization and ownership of different technologies & sharing the technology at home.

	Computer	Laptop	Tablet	Smart Phone
Utilization	35.5%	47.2%	39.3%	86.5%
Ownership	44.8%	53.7%	50.9%	87.5%

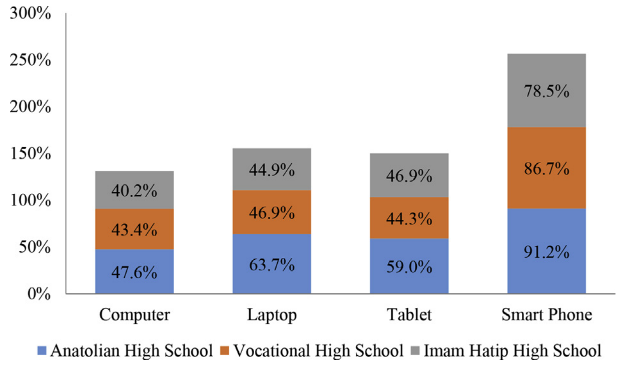

Fig. 1. Ownership of different technologies in three types of high school.

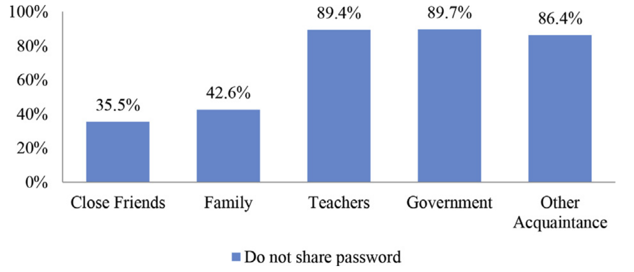

Fig. 2. The percentages of students who do not share password of devices with others.

utilization and time spent on Internet, 3 out of every 4 students have the habit of daily Internet utilization. According to time spent on Internet per day, 28.4% of the students spend less than 1 hour, 22.9% of the students spend 2 hours, 17.8% of the students spend 3 hours, 11% of the students spend 4 hours, 19.8% of the students spend more than 4 hours per day on Internet.

4.3.2. *Perception of privacy*

Perception of privacy are asked with five items as choose the option that suits you best for each of the statements for asked in Table 4. While 54% of students are uncomfortable about tracking which applications and when they use them on a computer or tablet (in item 1), more than half of the students look a bit more positive if new application is developed in the light of usage tracking (in item 2) (see Table 4). Only 17.3% of students approve of the general usage data such as search and web history in computers and tablets without the identification information (in item 3) while 47.7% of the students strongly disagree with the statement that general usage data like the search and web history can be made visible, even after the identification information has been removed. Within the scope of the FATIH Project, the tablet computers have properties of using camera and microphone recording and Internet access in exams and lectures, but 48.3% of the students do not accept that these properties are useful while 31% of the students partly agree about usefulness of these properties, and only 20.7% of the students believe that video and sound recording during examinations and lessons is necessary for their safety (in item 4). In addition, 13.5% of the students find it is okay to have the Internet access on our tablets remotely blocked when needed while 51.8% of the students do not accept being blocked the Internet access remotely (in item 5) (see Table 4).

Furthermore, students are asked to label the first three best appropriate answers for the question “In your opinion, who can decide best whether a web page is safe or not?” Table 5 shows scores of the chosen answers. The formula for the weighted average is $(N_1{*}50 + N_2{*}33 + N_3{*}17)/(N_1{+}N_2{+}N_3)$, where N_j denotes the number of students who answered the question in the jth label, $j = 1,2,3$. The weight of the first choose, N_1, is 50; the weight of the second choose, N_2, is 33; and the weight of the third choose, N_3, is 16. The total of these three weights is 100. After all scores are calculated, the scores are ranged from the highest score to the lowest score. As seen in Table 5, my family, myself, and my close friends have been chosen as first three ranks. On the other hand, students do not want their teachers and the government to decide the safety of a web page for them.

Table 3
Frequency of Internet utilization and time spent on Internet daily.

Frequency of Internet utilization	Percentage	Time spent on Internet daily	Percentage
Everyday	74.7%	Less than 30 minutes	10.8%
5–6 days per week	6.8%	30 minutes-1 hour	17.6%
3–4 days per week	7.1%	1–2 hours	22.9%
1–2 days per week	7.7%	2–3 hours	17.8%
A few times in a month	1.8%	3–4 hours	11.0%
Only one time or less in a month	1.9%	4 hours or more	19.8%

4.3.3. *Privacy in daily life and personal information*

Privacy in daily life and personal information are asked with three items: “Do you think it is okay for following people to know when you are outside of the school and where?” “Do you think it is okay for the following people to have your web history be seen?” “Do you think it is okay for the following people to have your e-school grade information be seen?” Participants answer to the questions by choosing three choose (Yes, Maybe, No) for the following six groups of people: Close Friends, Family, Teachers, Government, Other Acquaintance, and Other Strangers. Table 6 presents means and standard deviation for each group for three questions.

Furthermore, Table 7 presents the percentages of the choose “No” for three items: “It is not okay to know when you are outside of the school and where?”, “It is not okay to have your web history be seen?”, and “It is not okay to have your e-school grade information be seen?” (see Table 7). Only students' close friends and families have consent to know when, where they are outside the school, also to know what Web sites they visit. Close friends and family members are the most moderate looking people to know about students' privacy information like their physical location outside the school and their web site they visit, while teachers, government, other acquaintances or strangers are more objectionable to know these data. On the other hand, being e-school grade information visible by their teachers and the government is as acceptable as being visible by the close friends and families.

4.4. *Social media utilization and perception of personal privacy on social media*

Social media account, awareness of social media settings, perception of relationship management on social media, perception of sharing personal information on social media, social media and perception of security in social media settings have been analyzed in this section.

4.4.1. *Social media account*

Fig. 3 presents the percentages of having social media user account. Percentage of the students who do not have any social media user account is 8.2% and the most popular social media is Facebook and then Instagram.

4.4.2. *Awareness of social media settings*

About awareness of social media settings, 75.2% of the students indicate that they know about the audience settings that regulate who can see the shares in social networks and changed. Only 10.7% of the students do not know these settings and 14% of them know these setting but do not apply any change (see Fig. 4).

Table 4
Perception of privacy.

Items	Strongly agree	Partly agree	Strongly disagree	Mean (Std. Deviation)
Item 1. It makes me uncomfortable to have my application usage statistics (which programs, when and how long) in computers/tablets tracked.	54.5%	34%	12%	2.4 (SD = 0.6)
Item 2. Development of new content according to my application usage statistics in computers/tablets is important for me.	32.4%	50.9%	16.7%	2.1 (SD = 0.6)
Item 3. General usage data such as my search and web history in computers/ tablets can be made visible without my personal information.	17.3%	35%	47.7%	1.6 (SD = 0.7)
Item 4. Video and sound recording during examinations and lessons is necessary for our safety.	20.7%	31%	48.3%	1.7 (SD = 0.7)
Item 5. It is okay to have the Internet access on our tablets remotely blocked when needed.	13.5%	34.7%	51.8%	1.6 (SD = 0.7)

Table 5
Scores of “who can decide best whether a web page is safe or not?”

Who can decide	N_1	N_2	N_3	Scores
Family	416	376	111	35
Myself	432	157	126	30
Close Friends	34	161	316	24
Teachers	21	148	204	7.3
Government	67	77	91	6.8
No one	34	58	78	4.3

Table 6
Means of three questions about privacy in daily life like their physical locations, Web site visit history and e-school grade.

For which of the following people/three items	Do you think it is okay for following people to know when you are outside of the school and where?	Do you think it is okay for the following people to have your web history be seen?	Do you think it is okay for the following people to have your e-school grade information be seen?
Close Friends	0.3 (SD = 0.6)	0.5 (SD = 0.7)	0.5 (SD = 0.7)
Family	0.4 (SD = 0.7)	0.6 (SD = 0.8)	0.4 (SD = 0.7)
Teachers	0.6 (SD = 0.8)	0.9 (SD = 0.9)	0.4 (SD = 0.7)
Government	0.7 (SD = 0.8)	0.9 (SD = 0.9)	0.6 (SD = 0.8)
Other Acquaintance	0.7 (SD = 0.8)	1.0 (SD = 0.9)	0.9 (SD = 0.9)
Other Strangers	1.1 (SD = 0.9)	1.3 (SD = 0.8)	1.2 (SD = 0.9)

4.4.3. *Privacy perception of personal data sharing on social media*

Privacy perceptions of personal data sharing on social media is asked with the questions, *“Do you think it is okay for following people to see your personal data like photos, shared content, friend list, profile information, and contact information on social media?*” (see Table 8). Participants answer to the questions by choosing three choose (Yes, Maybe, No) for each of the following six groups of people: close friends, family, teachers, government, other acquaintance, and other strangers. Yes refers that she/he minds to be seen her/his data by the chosen people. No refers she/he does not mind to be seen her/his data by the chosen people. Table 8 presents means and standard deviation for each group for five different personal data, photos, shared content, friend list, profile information, and contact information on social media. In Table 8, bigger means represents the concerns of being seen the personal data on social media. In addition, Table 9 presents the percentages for the answer, “*it is okay for following people to see your personal data*”. According to means of the concerns of being seen the personal data on social media (see Table 9), the high school students do not care about the audience settings of their photograph and shared contents. Although the close friends and the family are perceived as the least objectionable audience, it is not a problem for nearly half of the students to have their shared content visible by the teachers, the government or the other acquaintances. 1 out of each 3 students is not cautious about having their shared content on social media visible. Those students do not perceive this against their personal data privacy even if the contents are visible by anyone, or they do not evaluate this in the scope of personal data privacy. Similarly, the high school students do not evaluate the friend list and personal information in the scope of personal data privacy. It is not a problem for the students to have these data accessible by their close friends, family, teachers, other acquaintances and the government. However, different from the virtual environment, the students concern about their personal data privacy when it comes to the contact information that is directly related to being accessible outside the virtual life. Still, the percentage of the students who consider that strangers can have their contact information is 17.3% (see Table 9).

4.4.4. *Perception of security on the use of technology and social media*

Perception of security on social media is presented in Table 10 with items 6–10. 28.3% of students state “strongly disagree” for the item 6, “*while installing a new application on my smart phone, I cancel the installation*

Table 7
Privacy in daily life and personal information like web history and e-school grade.

For which of the following people/items	It is not okay to know when you are outside of the school and where?	It is not okay to have your web history be seen?	It is not okay to have your e-school grade information be seen?
Close Friends	70.9%	65.2%	64.1%
Family	75%	61.2%	72%
Teachers	56.4%	46.3%	73%
Government	55.8%	43.9%	62.1%
Other Acquaintance	52.6%	40.2%	42.9%
Other Strangers	38.7%	28.5%	31%

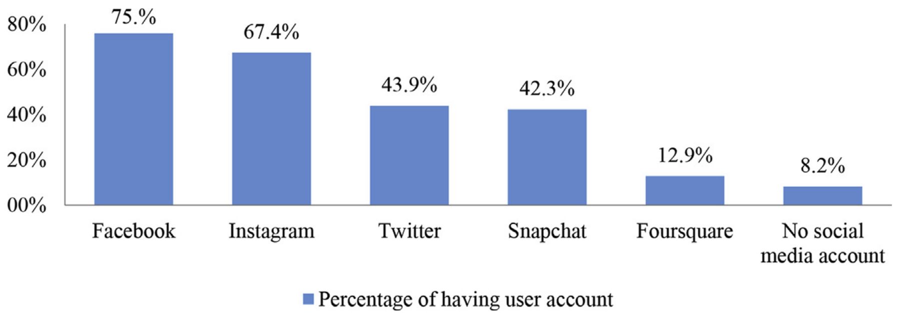

Fig. 3. Percentages of having social media user account.

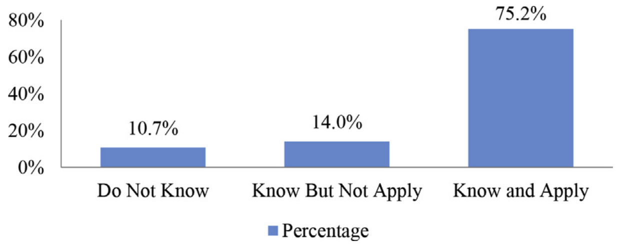

Fig. 4. The audience settings for the shared content on social media accounts.

if it asks for permission to access contacts, location information etc.". In addition, 52% of the high school students are indecisive about their actions when an application asks for permission to access contacts and location information for the installation. 59.7% of students state "strongly disagree" for item 7, *"it is not safe to install the application that my close friends use."* It can be assumed that in such a situation, students are influenced by the experiences of their close friends and families about the application. 46.9% of students state "strongly agree" for item 8, *"it is not safe to be friends with strangers on social media."* On the contrary, the other half of the students are open-minded on this. In addition, 23% students state "strongly disagree" for item 9, "It is not safe to be friends with

Table 8
Means and Standard Deviations for groups about personal data like photos, shared content, friend list, profile information, and contact information on social media be seen.

People/Type of data	Photos	Shared content	Friend List	Profile Information	Contact Information
Close Friends	0.1 (SD = 0.5)	0.1 (SD = 0.4)	0.2 (SD = 0.5)	0.2 (SD = 0.5)	0.3 (SD = 0.7)
Family	0.2 (SD = 0.6)	0.2 (SD = 0.5)	0.3 (SD = 0.6)	0.1 (SD = 0.5)	0.2 (SD = 0.6)
Teachers	0.5 (SD = 0.7)	0.5 (SD = 0.7)	0.4 (SD = 0.7)	0.3 (SD = 0.6)	0.7 (SD = 0.8)
Government	0.7 (SD = 0.8)	0.7 (SD = 0.8)	0.6 (SD = 0.8)	0.5 (SD = 0.8)	0.9 (SD = 0.9)
Other Acquaintance	0.6 (SD = 0.8)	0.6 (SD = 0.8)	0.5 (SD = 0.8)	0.5 (SD = 0.8)	1.0 (SD = 0.8)
Other Strangers	1.1 (SD = 0.9)	1.0 (SD = 0.9)	1.0 (SD = 0.9)	1.1 (SD = 0.9)	1.5 (SD = 0.7)

Table 9
For which of the following people do you think it is okay to have your personal data on social media be seen.

People/Type of data	Photos	Shared content	Friend List	Profile Information	Contact Information
Close Friends	87.1%	89.8%	85.2%	86.9%	73.4%
Family	80.1%	78.9%	78.7%	89.2%	85%
Teachers	60.5%	60.5%	67.4%	75.9%	53.3%
Government	54.8%	57%	61.6%	60.9%	45.4%
Other Acquaintance	57.2%	59.4%	63.1%	59.3%	38.7%
Other Strangers	36.3%	40.4%	43.7%	36.3%	17.3%

Table 10
Perception of security on social media.

Items	Strongly agree	Partly agree	Strongly disagree	Mean (Std. Deviation)
Item 6. "While installing a new application on my smart phone, I cancel the installation if it asks for permission to access contacts, location information etc."	19.4%	52.3%	28.3%	1.9 (SD = 0.6)
Item 7. "It is not safe to install the application that my close friends use."	6.9%	33.4%	59.7%	1.4 (SD = 0.6)
Item 8. "It is not safe to be friends with strangers on social media."	46.9%	37.1%	16.0%	2.3 (SD = 0.7)
Item 9. "It is not safe to be friends with people that are friends of my friends but that I do not know personally."	28.8%	48.2%	23.0%	2.0 (SD = 0.7)
Item 10. "Government should impose restrictions on social media in case of need."	36.7%	33.3%	30.0%	2.0 (SD = 0.8)

Table 11
Knowledge and utilization of information technologies.

Knowledge and utilization of information technologies	Percentage
Taking a course in which information technology devices such as a smart board, projector, computer or tablet is used.	63.1%
Using information technology devices in any of the courses this semester.	73.3%
Using information technology devices comfortably.	88.4%

Table 12
Percentages of using information technologies.

How often	Outside of the school	Outside of the school for homework & project	At school
Never	9.6%	8.7%	20.9%
A few times a month	10.2%	24.8%	16.2%
Several times a week	27.0%	38.7%	33.8%

people that are friends of my friends but that I do not know personally." More than half of the high school students find it unsafe to become friends with people that are friends of their friends but that they do not know personally. 30% students state "strongly disagree" for item 10, *"government should impose restrictions on social media in case of need."* while high school students have different opinions about imposing restrictions on social media by the government in case of need.

When comparing data according to school type, an one way analysis of variance (ANOVA) is conducted for the item "Government should impose restrictions on social media in case of need". ANOVA shows that the effect of school type is significant at $p < 0.05$ level, F (2,1047) = 11.992, p = .000. Post hoc analyses using the Scheffé post hoc criterion for significance indicates that the average number of errors is significantly lower in the Anatolian High School (M = 1.9, SD = 0.8) than in the other two schools Vocational High School (M = 2.1, SD = 0.7, Mean Difference = -0.1) and Imam Hatip (M = 2.8, SD = 0.7, Mean Difference = -0.3).

4.5. Knowledge level and perception of personal data conservation

86.5% of the students think that the protection of personal information is a basic human right. 8.2% of the students are unsure about this statement and 5.2% of the students do not think that the protection of personal information is a basic human right. In addition 54.7% of the students think that the protection of personal information is guaranteed by the constitution. 32.1% of the students are unsure about this statement and 13.2% of the students do not think that the protection of personal information is guaranteed by the constitution. It is known that the protection of personal information is a basic human right but awareness of hat the protection of personal information is guaranteed by the constitution is much less.

4.6. Information technology utilization

88.4% of the students are able to use information technology devices comfortably. 63% of the students have taken a course in which information technology devices such as a smart board, projector, computer or tablet is used. 73.7% of the students have used information technology devices in any of their courses this semester (see Table 11).

Information technologies help with homework and provide online access to the course materials to the young students who show a tendency to use technology for their needs. Fig. 5 presents the benefits of using information technology devices for the courses.

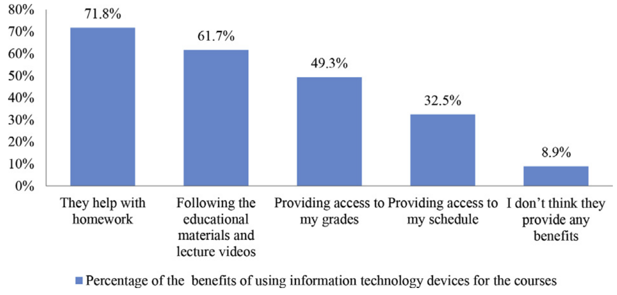

Fig. 5. The benefits of using information technology devices for the courses.

4.7. Frequency of utilization of information technologies

Table 12 shows percentages of using information technologies. More than half of the students use information technology devices in their out of school time. However, only 29% of these students use information technology devices daily for their homework and project. The rest of the students use these devices for out of school activities such as playing games, spending time on social media, watching movie/episode. In general, the frequency of the technology utilization for the courses at school or out of school is a few times in a week. 1 out of 5 students indicates that they do not use any information technology devices for education.

5. Conclusions

This research was designed to measure the perceptions of data privacy and the protection of personal data of high school students who are surrounded by the Internet, social media and mobile technologies. High school students have the habit of daily Internet utilization and nearly 20% of the students spend more than 4 hours per day on Internet. Among ownership of different technologies, smart phones are the most common device between the students. Ownership of a technological device is higher in Anatolian high schools than the other high schools. It can be concluded that different types of school can be represented with different social economic conditions. While computers and laptops are more likely to be shared by family members, smart phones are usually used personally. In addition, students are not much willing to share the password of their devices. High school students are very conscious about the password protection as one of the key parts of the data privacy conservation.

High school students perceive their habit of tablet and computer utilization inside the scope of the personal privacy according results of perception of privacy related security, accessibility and pursuit of personal information. More than half of the students are uncomfortable about tracking which applications and when they use them on a computer or tablet and also they look a bit more positive if new application is developed in the light of usage tracking. In addition, the clear majority do not approve of the statement that general usage data like the search and web history can be made visible, even after the identification information has been removed. The tablet computers that are provided to the students within the scope of the FATIH project allow students to use camera and microphone recording and Internet access in exams and lectures. However, these properties are not preferable, acceptable for the high school students. Majority of the students do not accept being blocked the Internet access remotely when it is needed.

According to results about using social media, the most popular social media is Facebook and then Instagram. About awareness of social media settings, only 75% of students are aware of using social media settings to protect their personal data. The high school students who are active on social media as a user do not care about the audience settings of their photograph and shared contents. In addition, high school students do not perceive personal data such as photos, written shares, friend list, general personal information they share on social media as personal data; also, they do not have a high level of concern that their shares in these areas are visible. Personal data concerns arise only when it comes to contact information that allows physical access outside the virtual world, however, stills 17.3% of the students do not have concern about known their contact information by strangers, which is very interesting and unexpected result for their safety and privacy issues. This result can be concluded that revealing generous amounts of information may lead to privacy risks as stated in the literature (Christofides et al., 2009; Patchin, 2012).

Friends' behaviors on the use of technology and social media affect students' perception of security on the use of technology and social media. According to results of students' perception of security on the use of technology and social media, it is common between the students to use the applications that are used by their close friends. For the high school students, the main goal of social media utilization is not only to share and follow the shared content of their friends and keep in touch but also to make new friends. As stated in the literature, following peer's attitudes on the use of social media are important for them to construct or show of their virtual identity, but sharing generous amounts of personal data may lead to privacy risks (Christofides et al., 2009; Patchin, 2012). High school students' perception include that sharing of personal data of any kind is acceptable to the individual family and close friends, but having access to the personal data by state, acquaintance, people who are not familiar and even their teachers, cause distress among students. On the other hand, being e-school grade information visible by their teachers and the government is as acceptable as being visible by the close friends and families, therefore, students do not perceive the e-school grade information as “private data/information”. In addition, it is known that the protection of personal information is a basic human right but awareness of that the protection of personal information is guaranteed by the constitution is much less.

This study intended to understand students' perceptions related data privacy besides understanding their daily behaviors of technology utilization. Overall results indicate that high school students have a personal data protection and data privacy algorithm defined for them in terms of personal data they currently share in social media or other platforms. On the other hand, persons, institutions or practices outside this algorithm are regarded as a threat to their personal data and are rejected. In addition, the results related to how high students benefit from information technology in education indicate that information technology supports both homework and is enjoyed by young people who are inclined to apply technology for all their needs, providing online access to educational materials. By using Communications Privacy Management (CPM) Theory (Mullen and Hamilton, 2016; Petronio, 2002, 2010) as an evidence-based theory centered on understanding the personal self-disclosure practices and the management of obtaining a collective privacy boundary, this study results presented under five main themes: (1) ownership and utilization of different technologies and password sharing, (2) Internet utilization and perception of privacy, (3) social media utilization and perception of personal privacy on social media, (4) knowledge level and perception of personal data conservation, (5) Information technology utilization. The collective data from these themes present that more than half of the students are aware that once the data is shared with teachers, administrators, parents, or ministry of education staff, the personal data moves to a collective privacy boundary as it is explained by CPM Theory (Mullen and Hamilton, 2016; Petronio, 2002, 2010). In the literature, the privacy dilemmas of students with friends and parents (e.g., Child and Agyeman-Budu, 2010; Child and Westermann, 2013; Mullen and Hamilton, 2016) are stated but, in this study the privacy dilemmas of students not with friend and parent, but there are bigger the privacy dilemmas of students with teachers, government, other acquaintance.

The study results support that social media, as the significant part of the daily lives, has accepted as the socialization tool for the young individuals and has become an indispensable habit of young people including high school students; communication and sharing have been moved to these platforms (Christofides et al., 2009). Besides, as the information technologies become part of education, importance of data security and data protection also increases in the same direction. In this study context, within the FATIH project (FATIH, 2012), even though tablets are provided and e-school systems are used by the schools, parents, and the Ministry of Education, accompanying technology for related data privacy within implementing educational applications and e-school systems does not exist. Therefore, developing data protection application that can be embedded into e-school system, educational applications, and mobile devices are required to overcome privacy risks. However, the idea that the tablets provided to the students within the framework of the FATİH Project can provide access to camera, voice recording and Internet in exams and class sessions is not particularly welcomed with the high school students in the district. Likewise, *personal data sharing* requirement as the idea of designing a personal application by accessing personal data on tablets or computers is accepted by only half of the students. In addition, when comparing data according to school type, the Anatolian High School students have more negative viewpoints than students in other two schools on the state intervention for restrictions on social media in case of need. This result describes high school students' perceptions of data privacy and suggests the protection of personal data of high school students who are surrounded by the Internet, social media and technology since teens are not aware of the privacy risks during using mobile technologies and allowing access to personal data by friends, parents, teachers, administrators and others. The similar studies in other cultures about privacy risks also point that teens are not fully aware of privacy setting of social media and privacy implications of sharing their personal data (Christofides et al., 2009; Madejski et al., 2012; Oz, 2014; Patchin, 2012). The study results confirm the research study on Internet habits and safe Internet use of children in Turkey and Europe (Kasikci et al., 2014) that states that the majority of children's Internet skills are not adequate and they are exposed to many online risks. However, protecting teens' personal data and give adequate skills to use the technology safety and effectively are still important issues for families, schools, policy makers and technology providers.

This research study describes high school students' perceptions of data privacy and suggests the protection of personal data of high school students who are surrounded by the Internet, social media and technology in one district of a metropolitan city. Further research is needed to investigate the influence of socioeconomic conditions of the school environment with regard to their effects on students' attitudes and behaviors about data privacy and using technology safety. This study could be repeated using a larger population in many high schools selected from among those with different socioeconomic conditions than those in this study.

Declarations

Author contribution statement

Aytac Gogus, Yücel Saygın: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Funding statement

This study is a part of the grant project supported by TUBITAK (The Scientific and Technological Research Councilof Turkey) with the grant number 114E261, title "Privacy Preserving Data Analysis and Publishing in Education", one of the funded projects of TUBITAK 1003, the BT0102 FATIH Project Security and Privacy call, 2014–2016. The authors wish to thank TUBITAK, the project team, and the participating schools, students, and teachers.

Competing interest statement

The authors declare no conflict of interest.

Additional information

Supplementary content related to this article has been published online at https://doi.org/10.1016/j.heliyon.2019.e01614.

References

Acquisti, A., Gross, R., 2006. Imagined communities: awareness, information sharing, and privacy on the Facebook. In: Danezis, G., Golle, P. (Eds.), Privacy Enhancing Technologies. Springer Berlin Heidelberg, Berlin, pp. 36–58.

Baruh, L., Popescu, M., 2015. Big Data Analytics and the Limits of Privacy Self-Management. New Media & Society. Advance online publication.

Baruh, L., Secinti, E., Cemalcilar, Z., 2017. Online privacy concerns and privacy management: a meta-analytical review. J. Commun. 67, 26–53.

Boyd, D., 2013. Networked norms: how tech startups and teen practices challenge organizational boundaries. In: Paper Presented at the ASTD Tech Knowledge Conference,San Jose, CA.

Boyd, D., Marwick, A., 2011, September. Social privacy in networked publics: teens' attitudes, practices, and strategies. In: Paper Presented at the Oxford Internet Institute's. A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society.

Child, J.T., Agyeman-Budu, E.A., 2010. Blogging privacy management rule development: the impact of self-monitoring skills, concern for appropriateness, and blogging frequency. Comput. Hum. Behav. 26 (5), 957–963.

Child, J.T., Westermann, D.A., 2013. Let's be Facebook friends: exploring parental Facebook requests from a communications privacy management (CPM) perspective. J. Fam. Commun. 13, 46–59.

Cho, H., Lee, J., Chung, S., 2010. Optimistic bias about online privacy risks: testing the moderating effects of perceived controllability and prior experience. Comput. Hum. Behav. 26 (5), 987–995.

Chou, H.L., Chou, C., Chen, C.H., 2016. The moderating effects of parenting styles on the relation between the Internet attitudes and Internet behaviors of high-school students in Taiwan. Comput. Educ. 94, 204–214.

Chou, C., Wu, H.C., Chen, C.H., 2013. Tool, toy, telephone, territory, trade, or treasure of information: a cross-sectional study of Taiwanese students' attitudes toward the Internet. Chin. J. Commun. 6 (2), 202–220.

Christofides, E., Muise, A., Desmarais, S., 2009. Information disclosure and control and Facebook: are they two sides of the same coin or two different processes? Cyberpsychol. Behav. 12 (30), 341–345.

Clemons, E.K., Wilson, J.S., 2015. Family preferences concerning online privacy, data mining, and targeted ads: regulatory implications. J. Manag. Inf. Syst. 32 (2), 40–70.

Debatin, B., Lovejoy, J.P., Horn, A., Hughes, B.N., 2009. Facebook and online privacy: attitudes, behaviors, and unintended consequences. J. Computer-Mediated Commun. 15, 83–108.

De Souzaa, Z., Dick, G., 2009. Disclosure of information by children in social networking-not just a case of "you show me yours and I'll show you mine". Int. J. Inf. Manag. 29 (4), 255–261.

FATIH, 2012. FATIH Project, Movement of Enhancing Opportunities and Improving Technology. Ministry of Education. Retrieved from. http://fatihprojesi.meb.gov.tr/tr/english.php.

Joinson, A.N., Reips, U.-D., Buchanan, T., Schofield, C.B.P., 2010. Privacy, trust, and self-disclosure online. Hum. Comput. Interact. 25, 1–24.

Kasikci, D.N., Cagiltay, K., Karakus, T., Kursun, E., Ogan, C., 2014. Findings of european online kids project (EU kids online): Internet habits and safer Internet use among children from Turkey and Europe. Educ. Sci. 39 (171), 230–243.

Kaya, T., Bicen, H., 2016. The effects of social media on students' behaviors; Facebook as a case study. Comput. Hum. Behav. 59, 374–379.

Madejski, M., Johnson, M., Belovin, M., 2012, March. A study of privacy setting errors in an online social network. In: Paper Presented at the 4th IEEE International Workshop on Security and Social Networking, Lugano, Switzerland.

Masrek, M.N., Aziz, N.S.A., Johare, R., 2012. The relationship between Internet attitude and Internet addiction. Asian J. Inf. Technol. 11 (4), 125–130.

Mullen, C., Hamilton, N.F., 2016. Adolescents' response to parental Facebook friend requests: the comparative influence of privacy management, parent-child relational quality, attitude and peer influence. Comput. Hum. Behav. 60, 165–172.

Nissenbaum, H., 2010. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, Palo Alto, CA.

Oz, M., 2014. Changes in use and perception of privacy: exploring Facebook users' privacy concerns and awareness of privacy implications. J. Yasar Univ. 9 (35), 6245–6254.

Ozcan, N.K., Buzlu, S., 2007. Internet use and its relation with the psychosocial situation for a sample of university students. Cyberpsychol. Behav. 10 (6), 767–772.

Patchin, J.W., 2012. Cyber Bullying Prevention and Response: Expert Perspectives. Routledge, New York.

Pew Research Center, 2013, August. Teens and mobile App Privacy. Washington, DC: Mary Madden, Amanda Lenhart, Sandra Cortesi, Urs Gasser. Received from. http://www.pewInternet.org/Reports/2013/Teens-and-Mobile-Apps-Privacy.aspx.

Pew Research Center, 2018, May. Teens, Social media & Technology 2018. Monica Anderson & Jingjing Jiang, Washington, DC. Received from. http://www.pewInternet.org/2018/05/31/teens-social-media-technology-2018/.

Petronio, S., 2002. Boundaries of Privacy: Dialectics of Disclosure. Suny Press, New York.

Petronio, S., 2010. Communication privacy management theory: what do we know about family privacy regulation? J. Fam. Theory Rev. 2 (3), 175–196.

Porter, C.E., Donthu, N., 2006. Using the technology acceptance model to explain how attitudes determine Internet usage: the role of perceived access barriers and demographics. J. Bus. Res. 59 (9), 999–1007.

Rauhofer, J., 2008. Privacy is dead, get over it! Information privacy and the dream of a risk-free society. Inf. Commun. Technol. Law 17 (3), 185–197.

Shear, B., 2013, 8 August. New Federal Legislation Aims to Stop the Digital Exploitation of Children. Received from. http://safegov.org/2013/8/9/new-federal-legislation-aims-tostop-the-digital-exploitation-of-children.

Taddei, S., Contena, B., 2013. Privacy, trust and control: which relationships with online self-disclosure? Comput. Hum. Behav. 29, 821–826.

Taddicken, M., 2014. 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. J. Computer-Mediated Commun. 19, 248–273.

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". In: Gutwirth, S., Leenes, R., de Hert, P. d. (Eds.), Reforming European Data protection Law. Springer, Heidelberg, pp. 333–365.

Tsai, C.C., Lin, S.S., Tsai, M.J., 2001. Developing an Internet attitude scale for high school students. Comput. Educ. 37 (1), 41–51.

Tüfekci, Z., 2008. Can you see me now? Audience and disclosure regulation in online social network sites. Bull. Sci. Technol. Soc. 28, 20–36.

Walrave, M., Vanwesenbeeck, I., Heirman, W., 2012. Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. Cyberpsychology 6 (1) article 1.

Zhou, T., Li, H., 2014. Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. Comput. Hum. Behav. 37, 283–289.