Privacy in social networks: An analysis of Facebook

Özgür Külcü*, Türkay Henkoğlu

Department of Information Management, University of Hacettepe, Beytepe, Ankara, Turkey

ARTICLE INFO

ABSTRACT

The only way to be aware of the risks and threats of Facebook, the most commonly used social networking site in the world and Turkey, is to be a careful user changing the default settings or simply not to have a Facebook account. In Turkey, there is still no study in which personal information shared though social networking sites has been evaluated in terms of privacy. For this reason, the findings obtained of this study have a great importance in the general picture of the current situation and drawing attention to the risks of the issue in Turkey where there are no legal arrangements effectively protecting the users from such sites. This study aims to investigate the Facebook privacy of information professionals who are members of KUTUP-L, and to determine the sensitivity and level of awareness of information professionals in Turkey. Facebook user profiles of 400 information professionals, all KUTUP-L members, have been analyzed in a study examining 32 different privacy settings. A privacy score has been calculated for each user, and the relations between privacy results have been analyzed. The findings at the end of the study show that information professionals in Turkey do pay attention to privacy, and most of the users change the default settings in order to protect their personal information.

© 2014 Elsevier Ltd. All rights reserved.

1. Introduction

Social networks have an important place among the tools which are used both as digital information infrastructures in which personal or institutional ideas, messages and news are produced, shared and consumed, and as an interface to access new information. Being information access and communication tools, social networks are widely used, and they enable different cultures to interact one another. Among the most visited internet sites whose pages are the most displayed ones throughout the world and in Turkey, the popular social networking site Facebook comes the first (Alexa, 2013). The site has become one of the largest information sharing platforms and is used by more than one billion users actively per month. One can access important personal information or links through searching on Facebook. There are risks and responsibilities that may leave the users in difficult situations with regard to the protection of information on social networking sites and the privacy of personal data. The increase of security risks due to the proliferation of information sharing services on the internet, increasing amount of information, and the rapid development in information and communication technologies has caused

the protection of privacy to be one of the most controversial and worrisome issues (King & Raja, 2012). The largest amount of information in the internet comes from social networking sites (European Commission, 2011). The main reason for the need to be conscious about the use of social networking sites and attaching importance to privacy is the misuse of personal information by social networking sites or the misuse of the viewable content by other users. Awareness by the content owner concerning the administration of digital information has a crucial role in the protection of personal data. It is impossible to foresee and follow in where in the world the information shared in the internet would be used within a few minutes and how many copies of the information would be produced. Legal and technical precautions on the issue, on the other hand, are usually ineffective. Furthermore, many social networking sites improve their advertising policies using the personal data they have already obtained and they place ads on the site in accordance with the personal interests of the users. Use of personal data for such purposes is clearly indicated in the user agreement accepted by the user when signing up for the site. Moreover, the service provider can change the content of the agreement without having the confirmation of the user (Facebook, 2012a).

It is necessary to make the personal information secure through making the legal arrangements about the way social networking sites can use personal data, and the use or distribution of the information not allowed to be displayed by the user without his/her confirmation. Nevertheless, an important and essential

* Corresponding author. Tel.: +90 312 297 82 00; fax: +90 312 299 20 14.
E-mail addresses: kulcu@hacettepe.edu.tr, ozgurkulcu@gmail.com (Ö. Külcü),
henkoglu@hacettepe.edu.tr (T. Henkoğlu).

responsibility falls to the user in the protection of privacy since personal information is provided and shared on social networking sites by the user himself/herself. It is impossible to legally protect the information in the social network because the information, over which changes are made by the user, is provided by the users by their own will. The fact that there is not any legal arrangement about personal data in Turkey increases the importance of the issue and imposes more responsibilities on the users. For this reason, user awareness comes into the forefront in the secure use of social networking sites and studies emphasize the important position of users. In the literature, there is no study analyzing user profiles in Turkey which puts forward the sensitivity and awareness level of the users on the protection of personal data and privacy. In this study, unlike previous ones, the issue of protection of privacy has been analyzed considering legal approaches; Facebook user profiles have been analyzed directly for the first time in Turkey, and an evaluation of the current situation has been made on the basis of clear findings. This study reveals the deficiencies in the legal arrangements, and the users will benefit from the findings of the study in the sense of being able to act more consciously against the risks in the current situation. The research questions to be answered in this study are

- What is the awareness of the members of the Turkish Professional Librarians' Discussion List (KUTUP-L) using social networking sites in information services concerning the protection of personal information on Facebook?
- In what categories in the rate of sensitivity is higher?
- What is the attitude of group members concerning hiding sensitive information (religious beliefs, political views, etc.) that might lead to discrimination?
- What are the categories about which group members share information?
- What is the attitude of group members about the protection of personal data by gender?
- Is there any difference in the level of protection of privacy according to the year of signing up?
- Is there any difference in the number of friends and photos shared by the users according to privacy levels?

2. Security, privacy and personal data on Facebook

Information for which privacy needs to be protected can be classified into two categories: personal data of primary importance and sensitive data of secondary importance which might affect the attitude of the society toward the individual in case of sharing. Personal data is defined in the data protection directive 95/46/EC of the European Union (EU) as any information relating to an identified or (directly and/or indirectly) identifiable natural person (European Council, 1995). The same definition is adopted by the "Draft Law on Protection of Personal Data" which was prepared in accordance with the data protection directive of EU in Turkey in 2008. The draft law also includes the expression "legal person" along with "natural person" taking place in the EU directive. As clearly stated in the draft law, the personal data which might pose a risk to the privacy of private life and family life are composed of the information about individuals' race, political view, philosophical belief, religion, sect or other beliefs, foundation, association and union membership, health, private life and conviction (T.C. Premiership, 2008). Among the primary data concerning user privacy are telephone number, identity records, address information, e-mail address, photos, identity number, institutional or student number, education background, online user accounts, posts on social networking sites, banking information and health records (European Commission, MEMO/12/41, 2012a). IP address, genetic

information, biometric information, location information, online identity and cookies taken from the visited internet sites are other important data that reveal cultural and social identity.

The protection of the users' privacy on Facebook has been a matter of discussion since the first day the social platform began, which causes privacy policies to change each year. In the beginning, in 2005, visibility of personal information was restricted by Facebook; yet, in 2010, these data were opened to everyone and the users were offered the choice of restricting the visibility of their personal information (Opsahl, 2010). On one hand, this alteration in Facebook default settings enabled everyone to see the data in the user profile; on the other hand, the users were provided with the choice to change all settings in the profile to protect their privacy. However, the alterations based on the services agreement have sometimes become disconcerting for the users. The users who do not frequently visit their Facebook accounts, even though they are informed via their e-mail address, ignore their account information, which increases the possible risks. Another important issue is the complexity in accessing and applying the privacy settings which have to be offered to the users due to legal obligations, even though the settings contrast with the fundamental sharing principle of Facebook. The privacy settings of the time tunnel is one of the examples of the complexity of user's access (Vaknin, 2011).

Use of Facebook in a secure way requires users to be more and more conscious and professional each year, and particularly to be more aware of the protection of personal data. Users who are not well aware of the protection of personal data or who do not have enough information about the settings to protect their privacy on Facebook do not know which of their personal information is available. One can access all of an individual's personal data and characteristics based on the information acquired through Facebook (Kosinskia, Stillwella, & Graepe, 2013).

The information defined when signing up for Facebook can be displayed by any Facebook user unless the privacy settings are changed. For this reason, in order to measure the privacy of a Facebook profile, in other words the sensitivity of a user on privacy, one must consider the restrictions on the default settings which enable other users to display the Facebook profile. Through a Facebook profile of which privacy settings are not changed, one can access the personal data of primary importance and, in the case of sharing, sensitive data of secondary importance which might affect the attitude of the society toward the individual.

2.1. Legal approaches to data protection in social networks

Establishing a system in which data protection is efficiently provided and the freedom of transferring personal data is not restricted by social networking sites is only possible with improvements in the quality of laws on data protection. The report of a research study conducted by the European Commission in 2011 puts forth the users' concerns about data protection in social networking sites and also includes details about the reasons for the necessary reforms in the law on personal data protection titled 95/46/EC (European Commission, 2011). In fact, the new draft directive on data protection dated 25/01/2012 with reference number IP/12/46 was prepared in order to eliminate the concerns indicated in this report due to the ineffectiveness of the current directive 95/46/EC in practice the EU (European Commission, 2012b).

When the legal conditions in Turkey are analyzed, it can be seen that the current regulations are generally related to the ownership and removal of content. Although the issues about publishing and information sharing in the internet in Turkey are regulated by the law numbered 5651 (Law on Regulation of Publications on the

Internet and Suppression of Crimes Committed by Means of Such Publication), there are controversial practices that are not clearly determined by the law. The practices which are not clearly determined by the law are provided with legal grounds by means of the articles within the agreements made with users. This approach is adopted universally (APA, 2013). Having analyzed the user agreements of social networking sites that have become popular, it is astonishing to read that social media management do not have responsibility for controlling the content and it is only the user providing the content who is responsible for illegal content (Facebook, 2012b). In addition, the case of republishing or sharing the link of an illegal content belonging to another user should not be overlooked. In case it is convinced that "the content is adopted", as indicated in the paragraph 2 of the article 4 of the law numbered 5651, the responsibility of the content provider continues (Law no. 5651, 2007). Therefore, each sharing on social networking sites means an individual responsibility for the sharing user. It is not always possible to withdraw and control or lay a claim on the illegal content published via social networking sites. This is also referred in the user agreements of social networking sites, and it was laid down as a condition that posts of the third parties must be evaluated in terms of legal conditions (Facebook, 2012b). Within the framework of legal arrangements in Turkey, the strategies that can be applied with regard to content do not serve the purpose of the protection of users' privacy or regaining privacy. These strategies can only be used for preventing contents from being republished and displayed by more people.

In the article 135 and 136 of the Turkish Penal Code, recording, illegal delivery or acquisition of personal data is regarded as crime. However, it is unclear in which situations these acts are illegal. With a paragraph added to the Article 20 of the Constitution, everyone has been provided with the right to request the protection of his/her personal data, the right of being informed of, having access to, and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistently with envisaged objectives. It was also stated in the same paragraph that the principles and procedures regarding the protection of personal data shall be laid down in law (T.C. Constitution, 1982). Nevertheless, in Turkey, there is not yet any law on the protection of personal data which regulates the principles and procedures regarding the protection of personal data. Various proposals were prepared within the framework of the attempts to enact a law on the protection of personal data which began in 1989. However, the process could not be completed. Finally, the draft law prepared in 2008 was declared void due to the interruption by elections[1]. Studies to renew this draft law have been proceeding since 2011.

3. Literature review

Since one can access many characteristics of users by means of the information acquired from the social networking sites for various purposes, the issue of privacy and security draws great attention. Having the largest rate of use, Facebook has been the most popular subject matter for the studies in this field. There are many studies in the literature carried out using the methods such as survey, face-to-face interview, and analysis of user profiles. The common purpose of these studies is to measure the existing level of privacy and user awareness, and to draw attention to the risks and dangers of the issue. It is stated that survey and interview methods are preferred in studies concerning user behavior while

the most reliable method to evaluate the existing levels of privacy, security and awareness of users is collecting data from the user profiles. There are many studies in the literature in which, using this method, the existing situation is presented and the change in the level of awareness is measured after analyzing the same user profiles some time later.

In McKeon's study, in which the development of privacy on Facebook is shown in graphics, the increase in the rate of personal data obtained regularly from the profiles of Facebook users each year between 2005 and 2010 is analyzed. It was found out in the study that, in 2005, one could only access the information such as the name, photo(s), gender and profession/education of the users at a moderate level while in 2010 it was possible to access any information in the profiles of the same user group, except for contact information and birth date (McKeon, 2010). Stutzman, Grossy and Acquisti carried out a study using 5076 Facebook user profiles, users' sensitivity on privacy, and behavioral change in disclosing personal data between the years 2005 and 2011. It can be seen in the study that there is a decrease in the amount of personal data available to everyone while there is an increase in the amount of sharing with the users in the friend list. The study also draws attention to the fact that the alterations made in 2010 based on Facebook privacy policies led the personal data hidden by users to become available to everyone and the degree of privacy to decrease (Stutzman, Grossy, & Acquisti, 2012).

Within the framework of a study conducted by Kosinskia, Stillwella and Graepe, "likes" sections of more than 58,000 Facebook user profiles were analyzed in order to determine what kind of information can be accessed and how one can easily access the information. It was stated in the study that the analysis of digital records through which personal data that indicate user tendencies and affect the user behavior can be used in product promotion and can be one of the reliable methods to measure individuals' psychological characteristics (Kosinskia et al., 2013).

Protection of privacy in social networking sites is also a key item of the studies conducted within the scope of "EU Kids Online" project which aims to provide children with secure internet usage in the EU countries. It is considered important that such studies raise awareness about the issue among children, 59% of whom, use social networking sites. Findings from the EU Kids Online project show that profiles of 26% of the children in the EU are available to everyone. This rate is 46% in Turkey and occupies second place in this statistic after Hungary (EU Kids Online, 2012).

The study in which Nosko, Wood and Molema analyzed the information on Facebook user profiles group by group includes interesting findings about protection of privacy. The study which systematically analyze what information is more frequently shared by whom, puts forward that age and gender are important factors in hiding sensitive information. It is also noted in the study that sensitive data that might pose a risk to users can be accessed through Facebook, and these views are supported by the findings (Nosko, Wood, & Molema, 2010).

4. Method

4.1. Sample

Facebook profiles of 400 users whose user accounts are accessible were randomly selected out of 2458 information professionals who are members of the KUTUP-L group and were analyzed in the study. It aimed to reach unquestionable findings about users' attitudes to and awareness of privacy practices by investigating the user profiles through content analysis. The members of the KUTUP-L group are composed of information management graduates and professionals and academicians working in the related fields. Being

---

[1] Article 77 of the Rules of Procedure of The Grand National Assembly of Turkey: Government bills and private members' bills that are not concluded in a legislative term are deemed null and void. However, the Government and the members of the Grand National Assembly of Turkey may renew these bills.

the common and single platform by means of which most of the information professionals serving in various information centers in Turkey, follow professional developments, KUTUP-L plays an important role. The age of the users[2] which might affect the results of the study was taken into consideration while selecting the group whose profiles were to be analyzed.

Hiding personal data on Facebook is also related to the ability to manage the privacy settings. Information professionals have been widely using social networking sites in recent years not only as a personal communication tool but also for providing information services and as a professional tool for in-house communication in libraries. Furthermore, information centers have initiated new services on social networks because of the rapid increase in the rates of usage in all age groups. For this reason, it was decided, in order to assess the privacy situation in Turkey, to collect data from Facebook user profiles of KUTUP-L members most of whom were educated in departments of "Information Management" and who are assumed to have enough awareness about the rules of sharing on social networking sites.

4.2. Data collection and research method

E-mail addresses of 2458 information professionals who are KUTUP-L group members were acquired from their Facebook profiles. The e-mail addresses which are used by the information professionals in their Facebook accounts and open to everyone were put into order using a random listing method and every user in the list was assigned an identity number to be used in random selection. Although randomly selected, 975 members who do not have a Facebook account or whose on Facebook is different from the one they use as a member of KUTUP-L, and also the KUTUP-L member accounts created to represent the institution or organization were not included in the sample. However, so as not to change the possibility of selection, the process was repeated without excluding these e-mail addresses. Using this method, Facebook profiles of 400 KUTUP-L members accessed through Facebook user accounts were analyzed between March 20 and April 25, 2013. It was confirmed whether the Facebook accounts included in the analysis belonged to the KUTUP-L members in the sample by matching the e-mail addresses with names. Considering the possibility of multiple Facebook profiles belonging to a single user and analyzing the profiles using the e-mail addresses contributed to the reliability of the research. Facebook accounts without any friend list or group/network membership were used in the process of matching the users with their Facebook accounts in order to eliminate the possibility of affecting the result of the study.

Thirty-two user profile sections were determined (according to the setting of being accessible by "everyone") via a Facebook account created for determining the sections of Facebook profiles to be analyzed. These sections were classified into 10 main sections by considering the definition of personal data of primary importance and sensitive data of secondary importance within the legal framework, which has been described in Section 2, and the classifications of sections based on the features similar on Facebook. One point was given for each section accessible to everyone classified under the 10 main sections determined beforehand, and each user's total points were calculated in accordance with the data collection algorithm in Appendix. It was accepted that, in the evaluation (out of 10 points), the user profiles with higher scores would have lower

Table 1
Distribution of percentage and frequency of the protection of privacy.

Main sections	Subsections	N	%
Friends		214	53.5
Photos		119	29.8
Contact information	Website, e-mail, Networks	296	74.0
	Phones	399	99.8
	Address	396	99.0
Basic information	Religious views	391	97.8
	Languages	371	92.8
	Political views	398	99.5
	Birthday	383	95.8
Favorites	Music	288	72.0
	Books	320	80.0
	Movies	329	82.3
	TV Programs	312	78.0
Likes	Games	345	86.3
	Athletes	371	92.8
	Sports teams	351	87.8
	Sports	384	96.0
	Activities	364	91.0
	Other likes	182	45.5
	Interests	360	90.0
	Inspirational people	394	98.5
Living/Town		193	48.3
Work/Education		198	49.5
Relationships/Family		323	80.8
Sharings		233	58.3

privacy than the profiles with lower scores. In order to evaluate the relationships between privacy status and variables in the user profiles, data on the 22 subsections listed in Table 1, in addition to the 10 main sections in each user profile, analyzed.

Within the scope of the research questions related to the data acquired from user profiles of KUTUP-L members under 10 categories, the following investigations have been carried out:

- Privacy states of each element, being a part of personal data on Facebook set by the users were noted.
- Considering the users' dates of signing up for Facebook, privacy states of Facebook users signed up between the years 2007–2009 and of those signed up between the years 2010–2013 have been compared.
- It has been investigated how changes in Facebook settings affected the users.
- It has been detected which personal data have been given more importance by the users.
- It has been investigated what kind of private data can be reached through information shared by users (such as photos).
- The difference between the sharings (e.g. friend and photo sharings) of the users who do or do not pay attention to the protection of personal data has been investigated.
- The importance levels given by women and men to privacy have been compared.

In order to determine the rate of privacy according to the years of signing up for Facebook, 313 users whose signing-up dates are known for certain were divided into two groups according to the signing-up periods as 2007–2009 and 2010–2013, and privacy state was analyzed over 10 main sections. In another measurement, the privacy scores calculated over 10 points were divided into three groups namely high, moderate and low privacy levels, and the distribution over these groups was evaluated depending on gender. In addition, an independent sample t-test was applied in order to measure the difference in the privacy states based on signing-up dates and gender. Kruskal–Wallis (K–W) and Mann–Whitney (M–W) tests were applied to measure the difference in the number

---

[2] Although Facebook does not allow users under the age of 13 to create accounts, it applies a different configuration for minors within the framework of its privacy policies. Minors between the age of 13 and 18 can only share their contact information, photos, status updates and other sharings with "friends of friends". The choice of "everyone" referring to all users in the internet can only be chosen by adults.

Table 2
Privacy rates according to signing-up dates and gender.

	Users signed up in the period of 2007–2009		Users signed up in the period of 2010–2013		Female		Male	
	N	%	N	%	N	%	N	%
Photos	82	32.5	26	42.6	63	30.4	56	29.0
Likes	104	41.3	32	52.5	93	44.9	81	42.0
Living/Town	114	45.2	36	59.0	105	50.7	88	45.6
Work/Education	135	53.6	24	39.3	106	51.2	92	47.7
Friends	143	56.7	21	34.4	118	57.0	96	49.7
Favorites	153	60.7	51	83.6	134	64.7	120	62.2
Sharings	153	60.7	40	65.6	137	66.2	96	49.7
Contact information	173	68.7	56	91.8	151	72.9	139	72.0
Relationships/Family	208	82.5	50	82.0	168	81.2	155	80.3
Basic information	222	88.1	56	91.8	188	90.8	163	84.5

of friends and photos shared by the users depending on levels of privacy. Independent sample t-test, K–W test and M–W test were applied during the analysis of the data, and SPSS 20 was used to acquire frequency, percentage and mean values of the data.

As in previous studies (Stutzman et al., 2012) the content of users' profile sections were also examined in detail, yet no discrimination was made between the profiles with no data entry and the ones with data hidden from others (not to be seen by everyone). In other words, the information content in the sections which were blocked to others were also analyzed, and it was assumed that the privacy was protected unless there was information in the sections. One can realize whether the sections such as time tunnel were restricted by the user so as not to be seen by everyone. However, it is not possible to have certain information about the availability or restriction of the information about photos and friends. The fact that users make less information on Facebook publicly available due to their concern about whether their personal data would be collected by Facebook is regarded as one of the indications of awareness and that privacy is protected. For this reason, nonavailability and restriction of personal data on Facebook profile are regarded as the same in measuring the users' privacy and awareness levels.

The user profiles in the analysis are available to all Facebook users. Even so, as a matter of respect for privacy of the users, personal data acquired through Facebook profiles have been preserved in a database with a timestamp.

5. Findings

Each rate and number value for the main sections and subsections shown in Table 1 was calculated independently of others. If a user did not have privacy in any of the subsections (e.g. address, telephone or e-mail), then he/she was regarded as not having privacy in the main section (e.g. contact) related to the subsection either. As it is possible to access the information about gender of users through their names, users' restriction of information about their gender was not evaluated as a separate parameter. According to the distribution of percentage and frequency related to the protection of privacy shown in Table 1, more than 95% of Facebook users, who are KUTUP-L members, do not share personal information namely address, phones, political views, birthday, inspirational people, sports and religious views. The most shared information is photos, followed by other likes, living/hometown and work/education.

Privacy rates of Facebook users in relation to main sections depending on signing-up dates (of 313 people whose signing-up dates are known for certain) and gender (207 female and 193 male KUTUP-L members) are shown in Table 2.

Fig. 1 shows the data obtained from Table 1 and the privacy rates according to years of signing-up for Facebook. According to Fig. 1, there is not a significant difference between privacy rates of

61 users who signed up for Facebook in the period of 2010–2013 and 252 users who signed up in the period of 2007–2009. There is a decrease in the privacy rates of the data such as friends, family information and work/education information in the profiles of the users who signed up for Facebook in the years between 2010 and 2013.

Depending on the data obtained from Table 2, Fig. 2 shows the privacy rates according to gender. Female users are more sensitive than male users particularly in the privacy of sharings, friends, basic information and town/living information. There is not any category in the graphics in which male users are more sensitive than female users while it is an interesting fact that the section the privacy of which was given the least importance both by females and males is photos.

The distribution of percentage and frequency of 193 male and 207 female Facebook users can be seen in Table 3. The distributions were calculated according to the levels of privacy which were determined over the privacy scores of the users. Approximately the half of the female users (50.2%) take part in the high level of privacy while males have an equal distribution in the high and moderate level of privacy. Only 83 (20.8%) out of a total of 400 users composed by males and females take place in the low level of privacy.

Two independent sample t-tests were applied in order to understand whether the average privacy scores of the users differ depending on the dates of signing up (2007–2009 and 2010–2013) and gender (female–male). Before each test, Kolmogorov–Smirnov (K–S) test was applied to test the appropriateness to normal distribution, and, in case the normal distribution would be affected by the number of samples (Field, 2009), coefficient of skewness and coefficient of Kurtosis were calculated as well. As a result of the K–S test, average privacy values of the years 2007–2009, the years 2010–2013, males and females were statistically significant (respectively $D(252) = 0.134$, $p = 0.000$, $D(61) = 0.135$, $p = 0.007$, $D(193) = 0.109$, $p = 0.000$, $D(207) = 0.157$, $p = 0.000$). Nevertheless, according to the coefficient of skewness and coefficient of Kurtosis values, it was observed that measurements showed normal distribution.

According to the independent sample t-test results shown in Table 4, the difference between the averages of the years

Table 3
Distribution of male and female users based on the level of privacy.

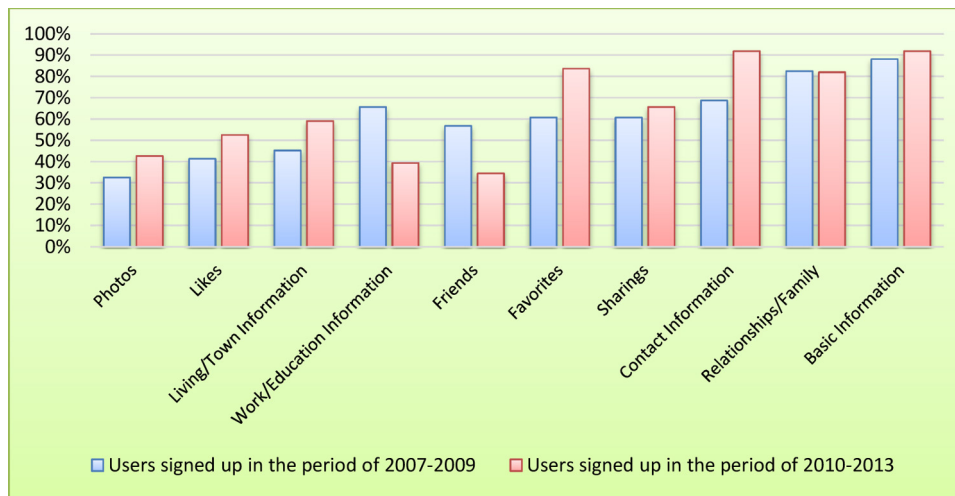|	Gender					
	Male		Female		Total	
	N	%	N	%	N	%
High level of privacy	74	38.3	104	50.2	178	44.5
Moderate level of privacy	74	38.3	65	31.4	139	34.8
Low level of privacy	45	23.3	38	18.4	83	20.8

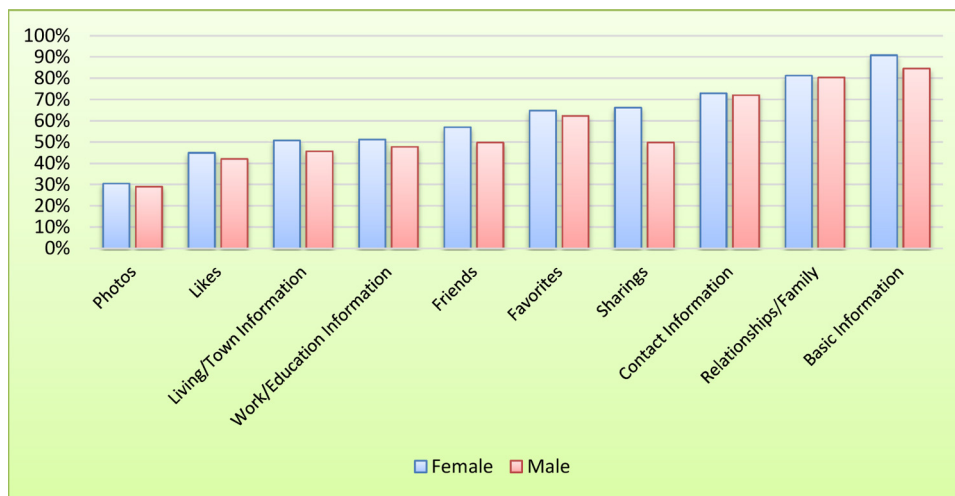Fig. 1. Privacy rates according to the years of signing-up for Facebook.

Fig. 2. Privacy rates according to gender.

"2007–2009" ($\bar{X} = 4.10$) and "2010–2013" ($\bar{X} = 3.57$) is statistically insignificant (t(311) = 1545, $p = 0.123$). The difference between the averages of privacy scores of males and females, on the other hand, is statistically significant (t(398) = 2003, $p = 0.046$). The average privacy score of males ($\bar{X} = 4.37$) is higher than that of females ($\bar{X} = 3.90$).

Of 400 KUTUP-L users whose Facebook profiles were analyzed, 216 (54%) users hide their friends while 119 (29.8%) users hide their photos. The average number of friends of the users who do not hide their friends is 293.8 while the average number of photos of the users who do not hide their photos is 79.4. The average number of friends and photos based on the privacy level of the users is shown in Table 5. Depending on the levels of privacy (low,

moderate, high), K–W and median tests were applied in order to measure the difference between the number of friends and photos which were permitted by the users to be available to everyone due to the fact that the result of K–S test applied to test the normal distribution of number of photos and friends was significantly significant ($p = 0.000$) and similarly the coefficient of skewness and coefficient of Kurtosis were not valued ±1 (there was not a normal distribution).

Depending on the privacy levels, there is a significant difference between the number of friends ($H = 75.972$, SD = 2, $p = 0.000$) and between the number of photos ($H = 62.573$, SD = 2, $p = 0.000$).

Table 5
Kruskal–Wallis test results of number of friends and photos.

	N	Rank mean	H	SD	p
Friend					
High level of privacy	178	154.83	75.972	2	0.000
Moderate level of privacy	139	214.72			
Low level of privacy	83	274.63			
Photo					
High level of privacy	178	154.75	62.573	2	0.000
Moderate level of privacy	139	217.60			
Low level of privacy	83	269.96			

Note: Bonferroni correction used to adopt the significance level 0.0167 for each effect.

Table 4
Privacy states according to dates of signing up for Facebook and gender.

Grouping strategy (Factor)	N	$\bar{X}$	SH	SD	t	p
Date of signing up for Facebook						
2007–2009	252	4.10	2.377	311	1.545	0.123
2010–2013	61	3.57	2.405			
Gender						
Female	193	4.37	2.474	398	2.003	0.046
Male	207	3.90	2.263			

This result is also confirmed by the median test. The numbers of photos and friends available to everyone in the three groups are not equal. As a result of K–W test, it can be seen that the users permitted more of their friends and photos to be seen by everyone through Facebook depending on the privacy level. As a result of M–W tests applied to find differing sections, it was found that there is a significant difference between the numbers of friends and photos of the subjects in all privacy levels ($p < 0.0167$). A statistical difference was found in terms of number of friends in the levels of high-moderate, high–low and moderate–low formed depending on privacy level (respectively $U = 8575$, $r = -0.300$, $U = 3053$, $r = -0.524$, $U = 3949.500$, $r = -0.271$). Similarly, a statistical difference was observed in terms of number of photos in the levels of high–moderate, high–low and moderate–low formed depending on privacy level (respectively $U = 8365.500$, $r = -0.284$, $U = 3249.500$, $r = -0.461$, $U = 4140.500$, $r = -0.236$). After analyzing r^2 values in the comparison of two groups, it was seen that rates of total varience in the numbers of friends and photos in between 5.76% ($r_{min} = -0.236$) and 27.04% ($r_{mak} = -0.524$) differ depending on privacy level.

6. Data analysis and evaluation

The distribution concerning KUTUP-L members' sensitivity to the protection of their personal data and their privacy on Facebook has been shown in Table 1 in detail. It can be seen that more than 95% of Facebook users hide important and sensitive personal data, namely address, phones, birthday, inspirational people, sports, political views and religious views. The sections having the lowest privacy rates are photos, town/living information and work/education information. As a result of the K–W and M–W tests carried out to measure the difference between the number of friends and photos, depending on the privacy level, it was found that as the level of privacy increases there is a decrease in the availability of friends and photos. This proves that the number of friends and photos shared on Facebook is related to the level of privacy and awareness. Nevertheless, although one can draw this conclusion from the statistical data, the difference value in the number of photos and friends is relatively low depending on the level of privacy, which means that further variants, not included in the study, might have a role in this difference. In the study carried out by Stutzman, Grossy and Acquisti, it was stated that more than 70% of the users shared their birthday, living/town, work/education and e-mail/networks information. It is observed in this study that only 32% of KUTUP-L members shared these data. From this point of view, it can be said that KUTUP-L members are sensitive in protecting personal and sensitive information. However, in some cases, it is possible to come across some profiles on which the user shares birthday party photos with date/location stamp although he/she does not share his/her birthday in the basic information section. Similarly, in some profiles, one can get information from the likes section about the user's political view, while the user does not share any information about his/her political view in the same section. As Kosinskia, Stillwella and Graepe stated in their study, one can access many data and characteristics of an individual through data mining on such information (Kosinskia et al., 2013). The findings of this study has shown that there is a difference in the attitudes of users concerning the conception of delicate data and information behavior expressed in the definitions in the Section 2.1. It is clear that all users make changes that could protect their privacy while customizing their privacy settings; however, they have inefficiencies in discriminating between the sensitive and unimportant information.

In the study in which Stutzman, Grossy and Acquisti investigated the changes in Facebook user profiles between the years 2005 and 2011, it was put forth that the privacy increased between the years 2005 and 2009; yet, due to the changes in the default settings and interface policies of Facebook in 2010, the amount of personal data available to everyone increased, which led to a decrease in the level of privacy (Stutzman et al., 2012). In 2010, there was a rapid increase in the amount of information available to everyone in the accounts of the users who are not sensitive about privacy or who are not aware of the change made by Facebook. It can be seen that similar results were obtained in McKeon's study (McKeon, 2010). In his study, depending on the results of the previous studies, the users' dates of signing up for Facebook were taken into consideration and the privacy states of Facebook users signed up between the years 2007–2009 and of those signed up between the years 2010–2013 were compared in order to measure the reaction of the users to the changes made by Facebook and their consciousness about the issue. It is know that, within the context of the changes that have been made in the Facebook interface since 2010, the data unavailable to everyone were not disclosed and there were not any changes that might affect the analysis in the last three years. Therefore, it is possible to determine what kind of behavior the users, who signed up for Facebook in the years between 2007 and 2009, exhibited upon the interface changes made in accordance with Facebook policies. According to the test results shown in Table 4, the changes made by Facebook in 2010 (Opsahl, 2010) did not cause a significant difference in the privacy level of the users who are KUTUP-L members. This fact reveals that, in the three-year period as of 2010, the old users were aware of the changes and customized their privacy settings in the same level with the new users. Also, the research findings put forward that the shortcomings upon which attention was drawn in previous studies (Stutzman et al., 2012) are not true for the awareness of KUTUP-L users. Another interesting figure shown in Table 4 is that the users signed up between the years 2010 and 2013 show an average of privacy over 60%. Configuration of the default privacy settings, on account of Facebook policies, in a way that are available to everyone did not make a negative effect on the privacy level of the users in the last three years. This fact indicates that KUTUP-L users have made changes in the default settings on Facebook in order to protect their personal data.

It can be seen in Table 2, which shows the levels of privacy in 10 main sections according to the year of registration, that privacy rates of the users, signed up between the years 2010 and 2013, concerning friends (34.4%) and work/education (39.3%) are lower than that of the users registered between 2007 and 2009 in the same categories: friends (56.7%) and work/education (53.6%). It can also be seen in the table that privacy rates of the users, who signed up in the period of 2010–2013, with regard to the data such as contacts, photos, living, basic information, favorites and likes, all of which might affect individual's status in society, are higher than that of those who registered in the period of 2007–2009. The "likes" section on Facebook is normally one of the empty sections of the site on which only the items, added by the users, can be displayed. In this respect, although about half of all the users hide the information in this section, the data not hidden by the remaining half of the users is of great importance.

According to the test results in Table 4, there is a significant difference between the averages of privacy score of male and female users. As in the previous studies in the literature, it can be seen in this study that women are more sensitive about privacy and they put more restriction on their profile than men via privacy settings. Many studies investigating tendencies and behaviors concerning privacy show that women are more cautious compared to men. It is obvious that women are generally more careful than men in sharing information, accepting friendships, joining a new group, and examining the privacy policies. This situation is associated with the fact that social pressure on women are much greater (Nosko et al., 2012). The similar result obtained at the end of this study

supports the views explaining the behavior based on gender. The figures in Table 3, which show the distribution of men and women according to the level of privacy, indicate that men are equally (38.3%) distributed in high and moderate privacy levels; however, it is interesting that half (50.2%) of the women take part in the high privacy level.

Contrary to the results of the studies concerning privacy of children in Turkey carried out within the scope of the "EU Kids Online" project conducted by the EU, it can be seen that adult information professionals pay attention to privacy on Facebook. In this respect, it can be said that, in Turkey, information professionals are more inclined to protect personal data, and they are more cautious depending on the age factor, which supports the results of the study carried out by Nosko, Wood and Molema. This conclusion is thought to result from the fact that information professionals are more experienced in using social networking sites than other users, and that age factor does not play an important role in the perception of risks and dangers stemming from the misuse of personal data.

In order to avoid the risks of Facebook, which has become one of the largest information platforms in which four billion pieces of content are shared everyday, there are three precautions a user can follow. These are as follows: choosing the "only friends" option which provides the privacy protections at a higher level; decreasing the shared information; or simply not having a Facebook account (Wilson, Gosling, & Graham, 2012). The protection of personal data has become one of the most crucial issues of our time. Personal data acquired in various ways may frequently be used in cyber crimes and for promotional purposes. They are also known to be causing dangers that might affect an individual's social status. It is a fact that in Turkey, where there is not yet any legal arrangement on protection of personal data, all the responsibility about this issue is taken by the users. For this reason, the users in Turkey, compared to other countries, need to be more conscious about the processes and sharings on Facebook. The legal connection between the user and Facebook, pertaining to the data collected or distributed for various reasons (advertising, etc.) by Facebook or many applications working on the site, is restricted to the user privacy agreement put forward by Facebook itself. Therefore, besides the information shared by users, the privacy level of personal data they have entered into the system is equal to the level of their trust in Facebook. That social networking sites do not take the necessary responsibility causes users to face many dangers due to the risks deriving from the indifference of users and the legal deficiencies.

7. Conclusion and suggestions

When legal conditions are investigated in Turkey, it can be clearly seen that legal arrangements are short of protecting personal rights and freedoms. Therefore, it is of utmost importance for users to be more conscious when sharing their personal data in social networks. It is clear that information professionals in Turkey

pay more attention to privacy and change their profile settings to protect their personal data compared to those users analyzed in previous studies in the literature. It was concluded that users particularly exhibit more sensitivity in the protection of basic and contacts information which is accepted as personal data of primary importance. Women are more sensitive in the protection of privacy than men, while there is not a significant difference between the level of privacy of those who signed up for Facebook in the last 3 years and those registered earlier. Facebook's decision to change its users' privacy settings in a way that made users' personal information available to the public without their consent, on the other hand, did not make any change in the level of privacy thanks to information professionals' conscious attitude. It was also seen that a few users did not pay attention to the category of bits of information they shared (e.g. photos, etc.) and overlooked the fact that one can access private information through such sharings. This deficiency can be overcome by organizing educational programs on secure internet usage for all ages of users and by carrying out studies to raise awareness on misuse of personal data.

If Facebook users become more conscious about privacy and they exhibit the required sensitivity on the issue, they can be avoid of risks by protecting their personal data from other users. Moreover, making the legal arrangements that would prevent the limitless use of personal data by service providers is of great importance. Looking through the EU lens, it has been seen that precautions taken by means of legal arrangements and conventions are reflected in user service agreements, and there has been an effort to protect user rights via new legal arrangements (Facebook, 2013). In Turkey, on the other hand, since there is not any legal arrangement concerning the protection of personal data, more responsibilities fall to users in the protection of privacy. A law on protection of personal data should be passed in Turkey. The law should clearly include the articles concerning social networking sites' obligation to inform the users themselves about the attempt to process, store and access the users' personal data, and collection of personal data at the lowest level. Also, the law should include arrangements such as configuration of default settings in a way that would protect users' privacy, receiving the confirmation of the user for the use of personal data, granting the user the right to ask the social networking site to permanently delete his/her personal data, and providing the freedom to transfer personal data.

The findings obtained from 400 KUTUP-L members' Facebook profiles, which were analyzed within the framework of the risks of information acquired through Facebook user profiles and existing legal arrangements, allowed the measurements of the information professionals' level of sensitivity and privacy related to the protection of personal data on social networking sites. Dealing also with the shortcomings of the existing legal arrangements, this study contributes to the protection of personal data on social networks and to the awareness on sharing sensitive information which might lead to discrimination within society.
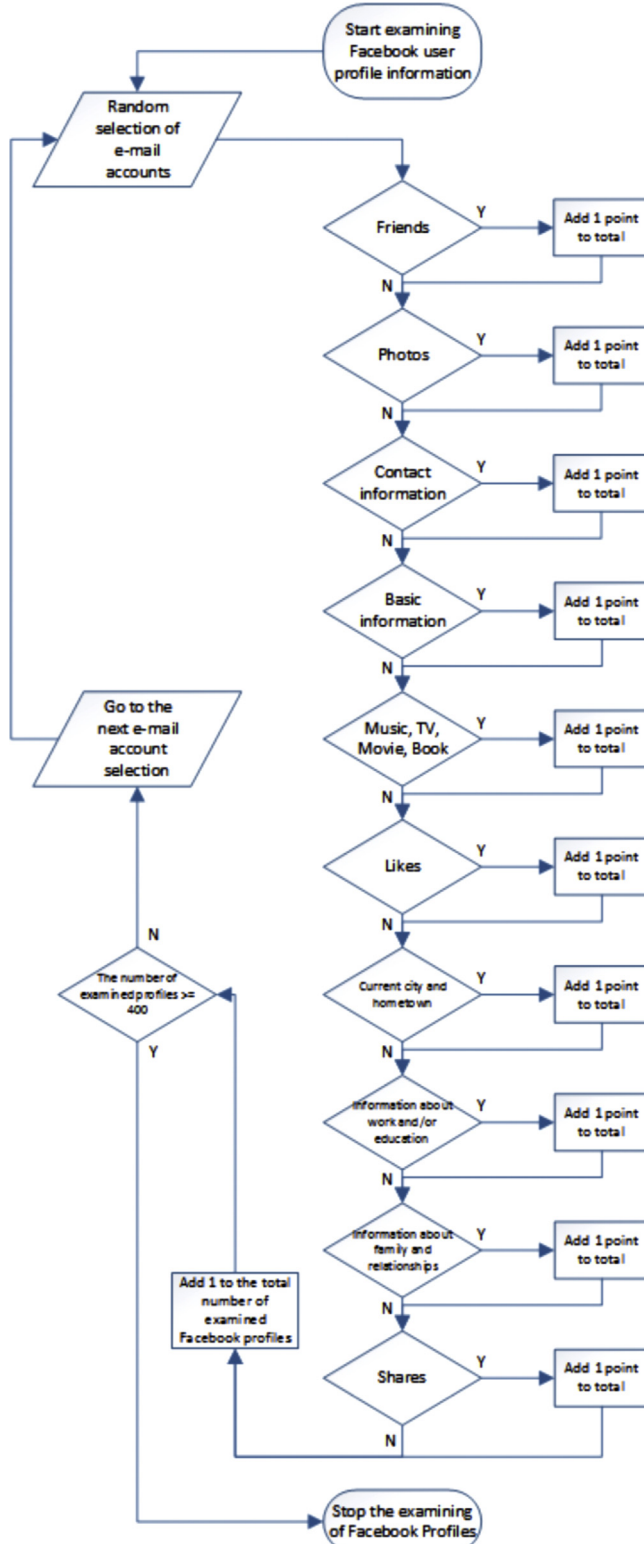
Appendix A. Appendix

Fig. A1. Data collection algorithm.

References

5651 Sayılı Kanun. (2007). *İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (online).* Available from: http://www.tbmm.gov.tr/kanunlar/k5651.html Accessed 1.03.2013

Alexa. (2013). *Top sites in Turkey (online).* Available from: http://www.alexa.com/topsites/countries/TR Accessed 29.04.2013

APA. (2013). *APA social media/forum policy (online).* Available from: http://www.apa.org/about/social-media-policy.aspx Accessed 1.03.2013.

EU Kids Online. (2012). *Avrupa çevrimiçi çocuklar projesi özet bulguları (online).* Available from: http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsExecSummary/TurkeyExecSum.pdf Accessed 4.05.2013

European Commission. (2011). *Attitudes on data protection and electronic identity in the European Union.* Brussels: European Commission.

European Commission. (2012a). *MEMO/12/41 (online).* Available from: http://europa.eu/rapid/press-release_MEMO-12-41_en.pdf Accessed 12.05.2013

European Commission. (2012b). *Regulation of the European Parliament and of the Council (online).* Available from: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf Accessed 27.02.2013

European Council. (1995). *Directive 95/46/EC Of The European Parliament and of the Council (online).* Available from: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf Accessed 11.05.2013

Facebook. (2012a). *Sizin hakkınızda aldığımız bilgiler (online).* Available from: http://www.facebook.com/about/privacy/your-info Accessed 27.02.2013

Facebook. (2012b). *Veri kullanımı ilkesi (online).* Available from: https://www.facebook.com/full_data_use_policy Accessed 1.03.2013

Facebook. (2013). *Veri kullanım ilkesi (online).* Available from: http://www.facebook.com/about/privacy/other Accessed 26.02.2013

Field, A. (2009). *Discovering statistics using SPSS* (3rd ed.). London: SAGE Publications.

King, N. J., & Raja, V. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law and Security Review*, 308–319.

Kosinskia, M., Stillwella, D., & Graepe, T. (2013). Private traits and attributes are predictable from digital records of human behavior (online). *Proceedings of the National Academy of Sciences*, 1–4. Available from: http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf Accessed 3.05.2013

McKeon, M. (2010). *The evolution of privacy on Facebook: Changes in default profile settings over time (online).* Available from: http://mattmckeon.com/facebook-privacy/ Accessed 16.03.2013

Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of Facebook. *Computers in Human Behavior*, 406–418.

Nosko, A., Wood, E., Kenney, M., Archer, K., De Pasquale, D., Molema, S., & Zivcakova, L. (2012). Examining priming and gender as a means to reduce risk in a social networking context: Can stories change disclosure and privacy setting use when personal profiles are constructed? (online). *Computers in Human Behavior*, 28(6), 2067–2074. Available from: http://www.sciencedirect.com/science/article/pii/S0747563212001604 Accessed 5.05.2013

Opsahl, K. (2010). *Facebook's eroding privacy policy: A timeline (online).* Available from: https://www.eff.org/deeplinks/2010/04/facebook-timeline Accessed 16.03.2013

Stutzman, F., Grossy, R., & Acquisti, A. (2012). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Condentiality*, 4(2), 7–41.

T.C. Constitution. (1982). *Türkiye Cumhuriyeti Anayasası (online).* Available from: http://www.tbmm.gov.tr/anayasa.htm Accessed 4.05.2013

T.C. Premiership. (2008). *Kişisel Verilerin Korunması Kanun Tasarısı (online).* Available from: http://www2.tbmm.gov.tr/d23/1/1-0576.pdf Accessed 11.05.2013

Vaknin, S. (2011). *How to protect your Facebook Timeline privacy (online).* Available from: http://howto.cnet.com/8301-11310_39-20112978-285/how-to-protect-your-facebook-timeline-privacy/ Accessed 2.04.2013

Wilson, R., Gosling, S., & Graham, L. (2012). A review of Facebook research in the social sciences. *Perspectives on Psychological Science*, 203–220.

Dr. Özgür Külcü is an associate professor in the Department of Information Management, Faculty of Letters, Hacettepe University, Ankara, Turkey. Previously he worked as a records manager in various public organizations. He is now Director of Team Turkey of InterPARES 3 Project which is International project on the authenticity, reliability and long term protection of electronic records. He wrote his doctorial thesis, Records Management in the Term of Quality Management and Quality System Documentation in Turkish Public Universities, in 2005. He is a lecturer on institutional information and records management at Hacettepe University since 2001. His main research interests are records management, quality management, and quality system documentation, particularly the analysis of institutional administrative systems. His work has been presented at national and international conferences and has been published in several journals.

Türkay Henkoğlu is a PhD student in the Department of Information Management, Faculty of Letters, Hacettepe University, Ankara, Turkey. He has worked in public organizations as a system administrator and been responsible for information security for 16 years. During his professional life, he has attended many training programs on information and computer security, computer systems and network management, and cryptography. His main research interests are information security policies, information access platform, legal and ethical responsibilities and freedom of internet access. He has wrote several books on informatics and information technology law. In addition, his work has been presented at national and international conferences and has been published in some respected journals.