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