Synthesis
International Scientific Conference of IT and Business-Related Research

PRIVACY PROTECTION ON FACEBOOK, TWITTER AND LINKEDIN

ZAŠTITA PRIVATNOSTI NA DRUŠTVENIM MREŽAMA FACEBOOK, TWITTER I LINKEDIN

Vida Vilić[1], Ivan Radenković[2]
[1]Clinic of Stomatology in Niš, Assistant Director of Legal Matters, Niš, and PhD student at the Faculty of Law, University of Niš, Serbia
[2]Lawyer, Law Office „Stanković", Obrenovićeva 36/4, Niš, Serbia

Abstract:
The social networks and companies providing sites for social networking build up their wealth and popularity on the grounds of close observations of social behavior and relations, as well as on targeted advertising of various things, mainly relying on the data collected on social network users and logs on their regular activities on social networks.
Some of the most frequent reasons for voluntary disclosure of personal data recognized by several authors include desire for attention, disinterest or lax attitude toward one's own or other people's privacy, incomplete placement of information, confidence in security of the data on social networks, as well as trust in their social media friends. Violation of the right to privacy most often occurs within the social networks with the highest number of registered users such as Facebook, Twitter and LinkedIn. The issue of whether or not social network users are still the owners of all information and whether permanent removal of a user account and deleting of the data once posted is possible at all.

Key words:
right to privacy, social networking, data security, voluntary disclosure of personal data.

Apstrakt:
Društvene mreže i kompanije koje nude sajtove za društveno umrežavanje grade svoje bogatstvo i popularnost na osnovu pomnog posmatranja društvenog ponašanja i odnosa, kao i na ciljanog oglašavanja različitih stvari, uglavnom oslanjajući se na podatke prikupljene o korisnicima društvenih mreža i izveštajima o njihovim svakodnevnim aktivnostima na tim mrežama.
Prema mišljenju nekoliko autora, najčešći razlozi koji navode pojedinca da otkriva lične podatke na društvenim mrežama su sledeći: potreba za pažnjom, nezainteresovanost ili nedovoljno čvrst stav prema sopstvenoj privatnosti ili privatnosti drugih, nepotpune informacije, poverenje u bezbednost podataka na društvenim mrežama, kao i poverenje u svoje prijatelje na društvenim medijima.
Do kršenja prava na privatnost najčešće dolazi na društvenim mrežama na kojima je registrovan najveći broj korsinika kao što su Facebook, Twitter i Linkedin. Pitanja koja se nameću su da li korisnici društvenih mreža i dalje imaju kontrolu nad tim informacijama, kao i da li je moguće trajno izbrisati korisnički nalog ili podatke koji su već postavljeni na tim mrežama.

Ključne reči:
pravo na privatnost, društveno umrežavanje, bezbednost podataka, dobrovoljno objavljivanje ličnih podataka.

INTRODUCTION

The social networks and companies providing sites for social networking build up their wealth and popularity on the grounds of close observations of social behavior and relations, as well as on targeted advertising of various things, largely relying on the data collected on social network users and logs on their regular activities on social networks.

Social networks often share users' personal data with various companies, most often with those involved in marketing and advertising, to whom they release users' personal data together with users' interests (Catanese *et al.*, 2011).

MAIN TEXT

Some of the reasons for voluntary disclosure of personal data recognized by several authors include desire for attention, disinterest or lax attitude toward one's own or other people's privacy, incomplete placement of information, confidence in security of the data on social networks, as well as trust in their social media friends (Gross & Acquisti, 2005).

The growing popularity of social networking sites led to more intense considerations of the issue of privacy protection. Spokeo is not a classical social network, but represents a social search engine intended to link people using data collected by aggregation. Namely, the site contains information on issues such as the age, type of relationship, property/wealth status, information on close family members, as well as the addresses of registered users. The mentioned information is collected from the data already available on the Internet, posted by social network users, but the site does not guarantee their accuracy (About Spokeo).

Violation of the right to privacy most often occurs within the social networks with the highest number of registered users such as Facebook, Twitter and LinkedIn. The issues that impose themselves are whether or not the social network users are still the owners of all information on them and whether permanent removal of a user account and deleting of the data once posted is possible at all.

E-mail: vila979@gmail.com
DOI: 10.15308/Synthesis-2015-735-738

TWITTER

When a Twitter account is created or restored, one must leave certain personal data including the username, password and e-address. Twitter servers automatically record all the data (in the so-called Log Data) created by the user (Twitter - Privacy policy). The log data can contain information such as user's IP address, browser type, pages visited, location, mobile carrier, search terms, and information on user's interactions with Twitter site, applications and ads. Twitter collects some personal data from its users, their private and public messages, public tweets or number of users' clicks on a certain link, and all the data collected in this way can be shared with third persons (Rushe, 2011).

An interesting example of violation of the right to privacy happened in January 2011 when the Government of the United States of America obtained a court order seeking to compel Twitter to reveal account information associated with several of its users associated with Wikileaks. Another interesting case is the one connected with Birgitta Jonsdottir, a member of the Icelandic Parliament and Wikileaks volunteer, who is in the center of a legal case with the US judicial system because of their attempt to use her private messages sent or received on Twitter starting from November 1, 2009. Jonsdottir made a statement that she was aware that a real issue was not only that the argued information was her own, but that it was actually a warning to all the people cooperating with Wikileaks. As an MP, she is protected by parliamentary immunity from public disclosure and publishing of private messages, but what might happen to ordinary people who, for one reason or another, find themselves in a similar situation? (American Civil Liberty Union, 2011). Twitter reacted by moving to unseal the court order, advocating that the Internet users should receive notice, and an opportunity to go to court to defend their constitutional rights, before their rights are compromised.

As for the „trade" with the data collected from its users, Twitter reserves the right to sell them all if the network owner changes. When a Twitter account gets deactivated, it is not deleted for 30 days; after that period a procedure of account deleting starts, which can last up to seven days (Twitter- Privacy policy).

FACEBOOK (FB)

Upon closer examination of this social network, one gets the impression that the main tendency is actually to make as much users' personal data as possible available for viewing by the entire public surfing through the virtual space of the Internet, because at user's registration all the data are at the minimum privacy protection level until such time when the user himself/herself sets certain limits. The users of this social network can set their own privacy options and thus ensure several different degrees of their own privacy protection.

A user who wants to create an account on Facebook must state his/her name, e-mail address, date of birth and gender (Facebook - Privacy policy). The mentioned data, including profile picture, username and password become available to everybody on the Internet. Each time when a user signs up to get to his/her own Facebook page, or views other people's profiles, searches for a certain page or a friend, clicks on an ad on the page, or uses any application, Facebook gets, collects and stores such data, and if the user posts a picture or a video, Facebook records the time, date and place when the given picture or video appeared. Data are collected and stored regardless of the way or source from which they were sent to the profile (whether from the computer, mobile phone or any other device allowing access to Facebook).

There are several types of personal data collected via Facebook (McCown & Nelson, 2009):

1. List of Friends – containing a list of all the users that a specific user accepted and labeled as "friends"; depending on the safety level set for each individual account, and this information can be seen only by the user's friends or it can be public and available to everybody on the Internet.
2. Personal information – a part including all information that the user chose to disclose about himself/herself, such as the first name and surname, profession, age, political and religious affiliation, things that the user likes, personal interests, membership in various groups on the social network, *etc.*
3. Wall posts –public messages received from other users or applications used on the social network, as well as various kinds of notifications; such data most often reflect the way the user feels, the things (s)he does, his/her attitudes and who (s)he is with at a certain point in time.
4. Massages – a body of private messages received from other users of this social network, similar to e-mail messages.
5. Photos – that the user is not obliged to post, *i.e.* which are posted at the user's sole discretion on which (s)he can tag all the persons appearing on them; depending on the safety level, social network users can make comments about them.
6. Notes – user's writings similar to blogs which may contain texts and photographs, allowing other users to comment and share.

The listed information collected by Facebook becomes available to a wide circle of people: user's friends, all Facebook users, and unless this option is deactivated, it will also be available to Facebook's marketing partners, publishers buying advertising space, as well as to the authors of video games and Facebook applications. The founders of Facebook immediately explained the purpose of using their users' personal data, mentioning issues such as safety of Facebook products and services, protection of intellectual property rights of Facebook and its users, sharing of local events and services with other users, measuring and better understanding the effects of advertising space on users, giving recommendations for tracking down possible friends or sharing mutual pictures, solving technical problems, and improvement of services.

In order to keep Facebook a free service for everyone, the founders of this social network "must" share their users' personal data with various marketing companies in order to give them an opportunity to send them advertising material through the Internet. The very rules of Facebook are such as to stimulate their users to disclose as much of their personal data as possible, thus undermining their own privacy.

In the policy on using Facebook services it is stated that each user is still the owner of all information, that (s)he can ban usage of his/her personal information and data or request that his/her name is not mentioned in order to prevent identification. It is interesting that most users do not even know anything about such options or rights, because the greatest number of users rarely use the option of setting their account and make no personal requirements for the implementation of the mentioned options.

If a user wants to deactivate his/her account, the policy of Facebook is not to allow immediate deactivation. In such cases, the account first acquires a "waiting status" during which period

DOI: 10.15308/Synthesis-2015-735-738

it is not visible to other social network users. The information posted during account deactivation is not deleted, even after deactivation. Account deactivation takes approximately a month, while certain information may remain in fallback copies and records up to 90 days.

It is interesting to know that this social network, relying on their users' ignorance, used to make their personal data available even without their consent. Back in 2007, Facebook started using the so-called Beacon program which had a task to notify various interested parties and advertising agencies of social network users' Internet activities, which made millions of Facebook users very angry. In such a way, each purchase made by any Facebook user would be placed in the "News Feed" and made available to all of his/her Internet friends. The user was not even aware that in a second all of his/her Internet friends would be informed of such activity, not to mention the fact that the settings regarding privacy issues did not at all allow the user to cancel this option permanently or at least block it temporarily. It was only in 2009 that Facebook quit using this program, only after massive criticism from the Electronic Privacy Information Center – EPIC (Spinello, 2011).

Facebook policy of disrespect for privacy stirred in 2009 numerous activities aimed to protect users' privacy, insisting that this social network may not make public its users' data such as username, picture and gender. As a result of the activities of EPIC and under massive public criticism, Facebook changed its privacy policy in 2010, thus allowing its users to set their user accounts so as to restrain availability and visibility of their personal data.

Despite the progress which was made regarding privacy protection, Facebook still has several „weak points" that jeopardize privacy of their users' personal data. For instance, when searching for a specific name on Google, the first option that appears as a result is such person's full Facebook account, if any. One of the problems already suggested by EPIC (2011) is related to protection of users' addresses and telephone numbers, which are presently available to everyone, if mentioned in the user's profile (*Ibid.*).

In January 2015, Facebook introduced certain new rules regarding privacy of the personal data posted by their users and visible to a wide circle of other users. In the field of protection of users' privacy (Facebook - Basics), Facebook made an effort to provide a detailed explanation of the way the user sees his/her own profile, the way the same profile is seen by other users and the way users can communicate among themselves. The only improvement brought about by such changes concerned the issue of users' protection against other users, because it became possible to select the information to be available and visible. Also, such innovations gave users a chance to limit the number of users allowed to publish posts on someone's profile, as well as controlled tagging of people on the posted photos, thus somewhat preventing mocking posts and violence thus generated (Facebook – How others interact with you). Still, this only gave the users an explanation regarding the things they can do *themselves* in order to protect their own privacy from other users, but the problem of how this social network *itself* and *to what extent* can dispose of the personal data entrusted to it by its users for „safekeeping" by accepting Facebook conditions of use, remained unresolved.

LINKEDIN

When signing up to join LinkedIn, very much like in the case of Facebook or Twitter, user's information includes the name, e-address, profession, employer, user's country and password. Data can be collected even when the user does not give them explicitly, but already when viewing and using web pages from the same IP address, on which occasion it is also possible to get user's IP address, browser type and operating system used, as well as addresses of all visited sites with in-built technologies of LinkedIn platform.

It is interesting to notice a provision stating that LinkedIn cannot sell, lease out or share user's personal information with third persons without user's consent, unless it is necessary to LinkedIn partners for provision of services (LinkedIn - Privacy policy), LinkedIn disassociates itself from unauthorized use of users' personal data in the following way: "*We have implemented security safeguards designed protect the personal information that you provide in accordance with industry standards. However, since the Internet is not a 100% secure environment, we cannot ensure or warrant the security of any information that you transmit to us. There is no guarantee that information may not be accessed, disclosed, altered, or destroyed…*" (*Ibid.*). LinkedIn keeps the data as long as a user's account is active.

The data on registered users or information posted by users can be shared with third persons only on the basis of the user's explicit consent, in the following cases: (1) if they happen to be essential for court proceedings, issuance of a court order or pronouncement of any legal sanction; (2) if necessary in order to enforce the User Agreement; (3) if any other user reports breach of rules of behavior on the network; (4) in order to protect someone's rights, property or personal safety.

CONCLUSIONS

Although a large number of social network users are aware of the fact that their privacy can be violated or at least threatened on social networks, users keep posting their personal data on such networks.

Each user with an active account on any of the popular social networks must be aware that the danger of experiencing violation of the posted data is always present, and that it is on the user himself/herself to "dose" the quantity of posted personal data and decide which data will be shared with whom in the virtual world. The feeling of closeness among users offered by the virtual space can be very dangerous, because – on the one side – users are not always exactly the same as their presentations on the Internet and are not always benevolent, while – on the other side – social networks live on advertising companies with which they share users' personal data so that such companies could offer them their services.

The precautionary measures that reduce the possibilities for abuse of the posted personal data are available on several social networks, which fact reassures users, making them believe that their data and personal information will not become available to everyone without their consent. Adjusting the privacy settings is a mandatory step in using any social network, and each and every user has access to the benefit of using this option when posting personal information on the Internet.

REFERENCES

Spokeo. (2015). About Spokeo. Available from http://www.spokeo.com/blog/about. Retrieved 12.8.2012.

Catanese, A.S., De Meo, P., Ferrara, E., Fiumara, G., & Provetti, A. (2011). Crawling Facebook for Social Network Analysis Purposes. Availble from http://arxiv.org/pdf/1105.6307.pdf. Retrieved 15.02.2015.

DOI: 10.15308/Synthesis-2015-735-738

Facebook. (2015). Basics. Available from https://www.facebook.com/about/basics. Retrieved 29.11.2014.

Facebook. (2015). How others interact with you. Available from https://www.facebook.com/about/basics/how-others-interact-with-you/. Retrieved 29.11.2014.

Facebook. (2015). Privacy policy. Available form http://www.facebook.com/about/privacy/your-info#inforeceived. Retrieved 4.8.2012.

American Civil Liberty Union. (2011). Government Requests For Twitter Users' Personal Information Raise Serious Constitutional Concerns, Says ACLU. Available from http://www.aclu.org/technology-and-liberty/government-requests-twitter-users-personal-information-raise-serious-constitu. Retrieved 12.8.2012.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 71-80. Available from http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf. Retrieved 15.02.2015.

LinkedIn - Privacy policy. Available from http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv. Retrieved 4.8.2012.

McCown, F., & Nelson, M. (2009). What happens when facebook is gone? In Proceedings of the 9th ACM/IEEE-CS joint conference on Digital libraries, pp.251-254. Available from http://www.cs.odu.edu/~mln/pubs/jcdl09/archiving-facebook-jcdl2009.pdf. Retrieved 15.02.2015.

Rushe, D. (2011). Icelandic MP Fights US Demand for Her Twitter Account Details, The Guardian, http://www.guardian.co.uk/media/2011/jan/08/us-twitter-hand-icelandic-wikileaks-messages. Retrieved 4.8.2012.

Spinello, R. (2011) Privacy and Social Networking Technology. International Review of Information Ethics, 16 (12/2011), p. 43, http://www.i-r-i-e.net/inhalt/016/spinello.pdf. Retrieved 1.3.2013.

Twitter - Privacy policy. Available from https://twitter.com/privacy. Retrieved 4.8.2012.

DOI: 10.15308/Synthesis-2015-735-738