Aleksandra Powierska

Safety in social media – privacy policy using the example of Facebook

Security Dimensions and Socio-Legal Studies nr 8, 59-68

2012

Aleksandra Powierska, MA
Jagiellonian University in Kraków

Safety in *social media* – privacy policy using the example of Facebook

Abstract:
In the age of an increasing popularity of social networks, the issue of safety and the protection of shared personal data is constantly taking on significance. Facebook is a good example of a medium which grants the administrators of the service and also its advertising providers full access to a database of key information on its users. At the same time, the users of Facebook violate the right to the protection of personal data by sharing content which is the property of their friends. In 2012, Facebook's privacy policy was made available in Polish language. That, however, did not change the fact of the users' data being still unprotected and there are numerous cases when data is stolen or misused.

Key words: *Facebook, privacy policy, protection of personal data*

The contemporary media has become dominated by the Internet. New technologies are present in virtually every sphere of contemporary life. The last decade has witnessed an upsurge in popularity of social media, at the forefront of which are blogs, Internet forums, and platforms such as Facebook or Google+. *Social media* now constitutes an important means of establishing virtual communities, which – apart from being a community of interest – also become a target group for marketing. But it is their community character that makes social media foster their users' great trust. That is facilitated by an illusory perception of virtual reality, a belief that it guarantees anonymity and therefore also safety to its users. As a result, a large number of users who create profiles in a given service do not hesitate to share their personal data and private pictures. However, the protection

of the data gives rise to certain difficulties. According to Jan van Dijk, many difficulties arise from the fact that regulations binding on the *offline* reality are clearly inadequate to the *online* reality as well as to the problems which are conditioned by the latter. At the heart of this inadequacy lie undeniable differences that divide the above-mentioned spheres of life:

„Fundamental differences are derived from: the fact that one environment is virtual and the other physical or material, that the distinction between public and private is blurred in online environments, that the accountability of things that happen in these environments cannot clearly be ascribed to the technology or to human effort, that the division between collective and individual property rights in networks is not easily made"[1].

In the context of such defined diversity, the issue which remains to be of major significance is the protection of privacy, including the issue of personal data collection and processing. Some of the key instruments concerning the protection of personal data are the principles formulated by OECD and the European Council. Van Dijk enumerates four that are most significant of those:

– the use limitation principle,
– the purpose specification principle,
– the data quality principle,
– and the openness principle.

The first of the principles assumes proper utilization of personal data collected, i.e. that the data is used for the purpose given. The second one – that collection and processing of personal data is carried out for strictly specified purposes. The data quality principle prescribes that personal data must be accurate and complete, and that it should be well protected. The fourth principle assumes a general policy of openness: „the people involved have the right to know what personal data is collected, for what purpose, who has access to this data, what will happen to this data when it is passed on to others, and to whom it is passed on"[2].

[1] Van Dijk, J., *The Network Society: Social Aspects of New Media*, 2nd ed., Sage Publications, London 2006, p. 130.

[2] Ibid., p. 150.

As it is emphasized by the author, not only are those principles binding to the Internet service administrators and controllers, but they also necessitate individual involvement and specialist knowledge of the user in the same degree. The illusory perception of safety originates from one of the most characteristic features of virtual reality, that is anonymity and a sharp distinction between the Internet activity and a person's behaviour in the real word. The right to anonymity becomes a priority nowadays, but it is with increasing frequency that „[a]nonymity is (ab)used by all kinds of criminals and networkers displaying improper behaviour"[3]. One of the most popular social networking services of the present day is Facebook. It aggregates information on millions of people worldwide and for that reason, it appears well-founded to examine the principles of Facebook's privacy policy.

Facebook was created in 2004 by Mark Zuckerberg. The project was initially launched as a social network for students. Facebook has presently over one billion users,[4] half of whom log in daily.[5] Facebook's database contains 219 billion pictures shared by its users, who have also established 140 billion friendships since the service is in operation[6]. Arguably, those numbers testify to the fact that the service constitutes a database of immense proportions. Facebook's servers contain virtually all data that has ever been uploaded by its users, e.g. email addresses, IP addresses used to log in, and graphic materials. The information concerning the users and its possible utilization are described in Facebook's privacy policy, but these descriptions are rather imprecise.

The information which Facebook collects from its users is principally divided into two categories: user information and public infor-

[3] Ibid., p. 154.

[4] Motyka, A., Facebookowi nie straszne konta widma. Zuckerberg ma już miliard, *http://media2.pl/internet/96698-Facebookowi-nie-straszne-konta-widma.-Zuckerberg-ma-juz-miliard.html*, (2.12.2012)..

[5] Shih, C., *Era Facebooka*, Helion, Gliwice 2012, p. 32.

[6] Motyka, A., Facebookowi nie straszne konta widma. Zuckerberg ma już miliard, *http://media2.pl/internet/96698-Facebookowi-nie-straszne-konta-widma.-Zuckerberg-ma-juz-miliard.html*, (2.12.2012)..

mation. The first category includes registration information (name, surname, email address, place of residence, and gender) and information the user chooses to share, such as status updates, uploaded photos, comments on friends' stories or news articles that use the comments plugin, as well as birthdays, or information indicating whether the user is in a relationship. It needs to be emphasized, however, that apart from collecting data on online activity of each user, the system also registers all activity of other users which is related to him or her. The following provision is particularly worthy of mentioning: „When people use Facebook, they may store and share information about you and others that they have accepted, such as when they upload and manage their invites and contacts"[7]. This means that the user ceases to be the sole controller of his or her personal data (excluding, of course, server administrators, who are also in control of the data) the very moment the user decides to invite friends. The first category also includes „other information", that is: the user's IP address, the type of browser, GPS or other location information, metadata related to other activities, such as the place and time of taking the uploaded photograph. Furthermore, the principles of privacy policy includes the following provision:

„We receive data about you whenever you interact with Facebook, such as when you look at another person's timeline, send or receive a message, search for a friend or a Page, click on, view or otherwise interact with things, use a Facebook mobile app, or purchase Facebook Credits or make other purchases through Facebook"[8].

The provision makes it justified to infer a conclusion that every single trace of the user's interaction with Facebook is registered and stored. This, in turn, allows the administrators to retrace the entire history of each person who has ever had a Facebook profile, including the most frequent location of logging in. The second category of information collected by Facebook servers is public information, that is: name

[7] Facebook website, http://www.facebook.com/about/privacy/your-info, (1.12.2012).

[8] Facebook website, http://www.facebook.com/about/privacy/your-info, (1.12.2012).

and surname, username and user ID, gender, profile picture and so-called cover photo, as well as a network, i.e. a network of friends who the user provides with access to additional information. These types of information are publicly available by default and visible in the interface. The user can choose to make the information concerning his or her interaction with Facebook public, meaning that also people off of Facebook will be able to see it. But those are the initial settings that need to be personalized after creating a profile and, in practice, a considerable number of profiles are not protected at all. According to the results of Consumer Report, 13 million Americans are unaware of the fact that the data they upload to Facebook is publicly available[9].

The service privacy policy also specifies the means of utilizing data received by Facebook about particular users. The policy includes the following provision:

„We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers who purchase ads on the site, and the developers that build the games, applications, and websites you use"[10].

That being so, it can be inferred that the data shared by the users may reach a wide group of recipients, given the fact that while the concepts of an „advertising provider" and an „application developer" do not raise any doubts, the concept of a „partner" is neither defined nor specified in any way. Another issue that may give rise to doubts is the unspecified goal for which information is used. Facebook privacy policy quotes a few examples of their use, but these are not very precise and are largely based on a high degree of generality of the applied concepts. The first example is the security of „Facebook products, ser-

---

[9] Nowak, A., *Miliony ludzi nie mają pojęcia z kim dzielą się wpisami na Facebooku*, http://di.com.pl/news/45065,0,Miliony_ludzi_nie_maja_pojecia_z_kim_dziela_sie_wpisami_na_Facebooku.html, (30.11.2012).

[10] Nowak, A., *Miliony ludzi nie mają pojęcia z kim dzielą się wpisami na Facebooku*, http://di.com.pl/news/45065,0,Miliony_ludzi_nie_maja_pojecia_z_kim_dziela_sie_wpisami_na_Facebooku.html, (30.11.2012).

vices and integrations"[11]. This passage lacks any explanation as to how the user should interpret the phrase „integrations". Similar vagueness characterizes also another provision: „to protect Facebook's or others' rights or property"[12]. Both of the aforementioned expressions provide the administrator with a wealth of freedom in utilizing the data, since the user does not know what „integrations" or „others" the platform will de facto be associated with. The user's data can also be used to keep statistics, to conduct group targeting, or to facilitate the user's interaction with the service by suggesting friends and *fan page* websites (official websites of companies, organizations, and brands). It is emphasized in the privacy policy that the user remains the owner of the uploaded data, and that it is only voluntarily that he or she grants Facebook the permission to process the information. In practice, this takes place the very moment the user creates his or her account and accepts the terms of service.

In the context of the protection of uploaded data, one of the more dangerous forms of using Facebook can be associated with its applications. At present, any user willing to participate in a contest or play a game that uses Facebook platform has to consent to his or her personal data being processed. On one hand, it is made clear that by accepting the terms, the user consents to his or her data being sent to the owner of the application. On the other hand, it does not mean that the data will not be publicized any further. According to the Symantec 2011 Report, in April 2011, it was possible to obtain access to users' private data through over 100,000 applications. That concerned primarily descriptions, photos, and contact information[13]. What also deserves to be highlighted is the provision that can be found in many applications, according to which the user grants his or her permission to publish information on his or her behalf. By accessing such an application, not

[11] Facebook website, http://www.facebook.com/about/privacy/your-info, (1.12.2012).

[12] Facebook website, http://www.facebook.com/about/privacy/your-info, (1.12.2012)

[13] Długosz, D., *Czy dane z Facebooka wyciekają?*, http://www.komputerswiat.pl/nowosci/internet/2011/19/czy-dane-z-facebooka-wyciekaja.aspx , (2.12.2012).

only does the user transfer to the developer of the said application his or her personal data, but also the user IDs of his or her friends. The privacy policy includes the following provision regarding this matter:

„Your friend list helps the application make your experience more social because it lets you find your friends on that application. Your User ID helps the application personalize your experience because it can connect your account on that application with your Facebook account, and it can access your basic info, which includes your public information and friend list. This includes the information you choose to make public, as well as information that is always publicly available. If the application needs additional information, such as your stories, photos or likes, it will have to ask you for specific permission"[14].

In practice, Facebook applications constitute an incredibly powerful machine for obtaining data. It is important to emphasize that even after the user stops using an application, the previously uploaded data remains registered in the database of that particular application. To remove it, it is necessary to contact the administrator of a given game. Furthermore, the removal of the application does not result in securing the data also in the case when other people, who were granted access to the user's data, still use that application. Applications are then often used to distribute unwanted content. According to the Megapanel PBI/Gemius research conducted in August 2012, ten most popular applications contain a tool considered by specialists to be a „data extorting and spam distributing" mechanism[15]. „My Calendar" application is a program which annotates birthdays of the user's friends in order to remind him or her about them – but the invitations and inquiries are sent without the user's consent. When the invitation is accepted, the program is automatically installed to the user's profile. It then starts sending unwanted content to the user's friends while simultaneously collecting

[14] Facebook website, https://www.facebook.com/about/privacy/your-info-on-other, (1.12.2012).

[15] „Polska Times" newspaper website, http://www.polskatimes.pl/artykul/683499,top-10-aplikacji-na-facebooku-na-czele-rankingu-program,id,t.html, (30.11.2012).

various types of information, such as the users' places of residence, email addresses, and the websites they visit most frequently[16].

That being so, it can be argued that the protection of data received by Facebook does not depend solely on the owner of the account, but also on the network of his or her friends, as well as their online activity. It is, therefore, extremely important to make cautious and informed decisions when accepting any invitations. According to Sophos, 46% of Facebook users are likely to accept a friend invitation from a complete stranger (often a fictitious person or somebody impersonating someone else), ipso facto granting that person access to his or her personal data[17]. In 2012, 83 million fake accounts have been created on Facebook, a number which constitutes nearly 9% of all existing profiles[18]. They are mainly duplicated accounts, which means that one person has at least two profiles in the service, or they are accounts that belong to companies or organizations, but which are not fan pages, ergo they have been wrongly created as profiles of private users. Spam-sending accounts are also included in this group[19].

The issue of the protection of personal data received by Facebook poses a problem also for the Inspector General for the Protection of Personal Data in Poland (GIODO). Until 2012, Facebook has not been under the jurisdiction of Polish law due to the fact that the company has not had its post in Poland and has not been using Polish technologies in its activities. As a result, the provisions regarding privacy policy has not been translated to Polish and the service itself has not been subject to the Polish Personal Data Protection Act[20]. Polish Facebook office

[16] „Polska Times" newspaper website, http://www.polskatimes.pl/artykul/683499,top-10-aplikacji-na-facebooku-na-czele-rankingu-program,id,t.html, (30.11.2012).

[17] Sikorska, K., *Kradzież danych na Facebook*, http://www.egospodarka.pl/47857,Kradziez-danych-na-Facebook,1,12,1.html, (3.12.2012).

[18] „Polska Times" newspaper website, http://www.polskatimes.pl/artykul/630359,na-facebooku-83-mln-martwych-dusz-to-zla-wiadomosc-dla,id,t.html, (30.11.2012).

[19] „ChipNews" website, http://www.chip.pl/news/internet-i-sieci/witryny-internetowe/2012/08/ponad-83-miliony-falszywych-kont-na-facebooku, (30.11.2012).

[20] Official site of Generalny Inspektor Ochrony Danych Osobowych, http://www.giodo.gov.

was opened in Warsaw in September 2012. It is intended to manage 30 countries of East-Central Europe, but formally it is still subject to its European headquarters in Ireland. Inspector General for the Protection of Personal Data points out that such activities as „tagging friends" in uploaded photos or placing a link to a friend's profile in shared content qualifies as revealing personal data and can be considered a violation of privacy[21].

Facebook is a social networking service, a fact that causes substantial complications as regards the principal responsibility for data protection – on one hand, the service administrator is responsible for all the users, but on the other – each user controls his or her own account. Given these conditions, it is necessary to be particularly cautious when uploading content, using applications, and inviting other users as friends. One of the basic tools for the protection of personal data is the privacy settings panel which allows every user to determine in detail the groups of users that are given access to his or her personal data. However, it is essential to remember that regardless of the restrictions of accessibility, all uploaded information is registered by Facebook servers, a fact which always poses the danger of it being utilized in an undesirable way.

Bibliography:

Shih, C., *Era Facebooka*, Helion, Gliwice 2012.

Van Dijk J., *The Network Society: Social Aspects of New Media*, 2nd ed., Sage Publications, London 2006.

pl, (2.12.2012)

[21] Official site of Generalny Inspektor Ochrony Danych Osobowych, http://www.giodo.gov.pl, (2.12.2012).

Netography:

„Chip News" website, http://www.chip.pl, (30.11.2012).

Długosz, D., *Czy dane z Facebooka wyciekają?*, http://www.komputerswiat.pl/nowosci/internet/2011/19/czy-dane-z-facebooka-wyciekaja.aspx , (2.12.2012).

Facebook website, https://www.facebook.com, (1.12.2012).

Motyka, A., *Facebookowi nie straszne konta widma. Zuckerberg ma już miliard*, http://media2.pl/internet/96698-Facebookowi-nie-straszne-konta-widma.-Zuckerberg-ma-juz-miliard.html, (2.12.2012).

Nowak, A., *Miliony ludzi nie mają pojęcia z kim dzielą się wpisami na Facebooku*,http://di.com.pl/news/45065,0,Miliony_ludzi_nie_maja_pojecia-_z_kim_dziela_sie_wpisami_na_Facebooku.html, (30.11.2012).

Official site of Generalny Inspektor Ochrony Danych Osobowych, http://www.giodo.gov.pl/, (2.12.2012).

„Polska Times" newspaper website, http://www.polskatimes.pl, (30.11.2012)

Sikorska, K., *Kradzież danych na Facebook*, http://www.egospodarka.pl/47857,Kradziez-danych-na-Facebook,1,12,1.html, (3.12.2012).