Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook

Tadas Limba, Aurimas Šidlauskas

▶ **To cite this version:**

Tadas Limba, Aurimas Šidlauskas. Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook. Entrepreneurship and Sustainability Issues, 2018, 5 (3), pp.528 - 541. 10.9770/jesi.2018.5.3(9) . hal-01773973

HAL Id: hal-01773973
https://hal.science/hal-01773973

Submitted on 5 Jun 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2018 Volume 5 Number 3 (March)
http://doi.org/10.9770/jesi.2018.5.3(9)

Publisher
http://jssidoi.org/esc/home

SECURE PERSONAL DATA ADMINISTRATION IN THE SOCIAL NETWORKS: THE CASE OF VOLUNTARY SHARING OF PERSONAL DATA ON THE FACEBOOK

Tadas Limba[1], Aurimas Šidlauskas[2]

[1,2] Mykolas Romeris University, Ateities g. 20, 08303 Vilnius, Lithuania

E-mails:[1] tlimba@mruni.eu; [2]aurimas868@gmail.com

Received 16 November 2017; accepted 20 February 2018; published 30 March 2018

Abstract. In view of the changes taking place in society, social progress and the achievements of science and technology, the protection of fundamental rights must be strengthened. The aim of the article is to analyse the principles and peculiarities of safe management of the personal data in social networks. In this scientific article, methods of document analysis, scientific literature review, case study and generalization are used. Consumers themselves decide how much and what kind of information to publicize on the Facebook social network. In order to use the third-party applications, users at the time of authorization must confirm that they agree to give access to their personal data otherwise the service will not be provided. Personal data of the Facebook user comprise his/her public profile including user's photo, age, gender, and other public information; a list of friends; e-mail mail; time zone records; birthday; photos; hobbies, etc. Which personal data will be requested from the user depends on the third-party application. Analysis of the legal protection of personal data in the internet social networks reveals that it is limited to the international and European Union legal regulation on protection of the personal data in the online social networks. Users who make publicly available a large amount of personal information on the Facebook social network should decide on the issue if they want to share that information with third parties for the use of their services (applications). This article presents a model for user and third party application interaction, and an analysis of risks and recommendations to ensure the security of personal data of the user.

Keywords: personal data, third-party applications, social network, security of the data

Reference to this paper should be made as follows: Limba, T.; Šidlauskas, A. 2018. Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook, *Entrepreneurship and Sustainability Issues* 5(3): 528-541. https://doi.org/10.9770/jesi.2018.5.3(9)

JEL Classifications: D80, D83, M15

Additional disciplines information and communication; informatics

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2018 Volume 5 Number 3 (March)
http://doi.org/10.9770/jesi.2018.5.3(9)

1. Introduction

A social network is generally defined as a system with a set of social actors and a collection of social relations that specify how these actors are relationally tied together (Wasserman, Faust, 1994). Authors Boyd and Ellison (2007) define social network sites as web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. Social networking has become one of the most important communication tools among people nowadays (Zaidieh, 2012). Virtual social networks present the constantly changing and extremely dynamic platform. By competing with each other, virtual social networks create an ever-increasing number of functionalities for the users in order to create the most convenient modes for communication. Facebook is the most popular social network in the world with a monthly number of active users of over 2 billion. The popularity of social networks is constantly increasing. According to the data, today 2.62 billion users are involved in virtual social networks, and it is expected that in 2019 the number of such users will reach 2.77 billion, and in 2020 – 2.9 billion (Statista, 2018). The social network users every day participate in creating a huge global database by presenting their own and other personal information publicly, and searching for various information. The more people use social networking services, the greater is the likelihood of violations of the rights of the data subject (Šišulák 2017; Menshikov et al., 2017). Malinauskaitė-van de Castel (2017) admits that virtual social networks are among the world's largest personal data administrators who collect, compile, store, use, destroy or perform other actions with the personal data of users. Data administrators determine the purposes and means of personal data processing.

Specifically, updating profile information, posting status updates, sharing photos and videos, and commenting on others' posts - to name a few - are behaviors that reveal aspects of one's personal identity. However, this escalating personal exchange on social networking sites also raises questions about privacy risks and consequences (Fogel, Nehmad, 2009; Zeman et al., 2017; Korauš et al., 2017). Users do not understand the importance of personal data, and voluntarily agree to share their personal information in exchange for third-party applications. Users also lack the knowledge of what rights they have as data subjects in order to ensure the security of their personal data.

Object of the research. Rights of the data subjects of social network. The aim of the article is to analyse the principles and features of the secure administration of personal data in social networks. The following objectives were set for the achievement of the purpose: to examine the theoretical aspects of the protection of personal data; to determine which personal data and how users can publicize on the Facebook network; to provide a model for user interaction with a third-party application; to propose recommendations that would better ensure the protection of personal data of data subjects.

With the development of information technology and electronic services, more and more often personal user data are stored and processed on the internet. Illegal collection and misuse of these data may pose a serious threat to the privacy of such individuals.

2. Personal data administration principles and features of social networks

Westin (1968) defined the right of a person to private life as an opportunity to "control, edit, manage, and delete information about him/her and decide when, how, and to what extent this information could be accessed by other persons". Parent (1983), when examining privacy, indicates that privacy is possible when personal data are not known or are not confidential. Kang (1998) states that information privacy is realisation of the individual's need to control the conditions under which personal information, which is identifiable to an individual, is received, disseminated or used. At present, privacy is often identified with the protection of personal data. Data protection

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2018 Volume 5 Number 3 (March)
http://doi.org/10.9770/jesi.2018.5.3(9)

is commonly defined as the law designed to protect your personal information, which is collected, processed and stored by "automated" means or intended to be part of a filing system (Privacy International's public engagement platform, 2018).

The Organisation for Economic Co-operation and Development (next – OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, for the first time established the basic principles of the protection of personal data (Table 1).

Table 1. Basic principles of national application

Principle	**Description**
Collection limitation	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
Data quality	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
Purpose specification	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
Use limitation	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with except: a) with the consent of the data subject; b) by the authority of law.
Security safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
Openness	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
Individual participation	An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
Accountability	A data controller should be accountable for complying with measures which give effect to the principles stated above.

Source: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980

The OECD Guidelines are generally universally recognized at international level as a set of privacy protection measures, and they apply to any information related to the data subject. The Dictionary of the European Data Protection Ombudsman's Office describes the data subject as the person whose personal data are collected, stored and processed. Regarding the process of personal data processing, the following basic rights of the data subject can distinguished: (Štitilis et al., 2016):

1. To know (to be informed) about the processing of his/her personal data;
2. To review the personal data, and know how they are processed;
3. To require correction, destruction of the personal data or suspension (except for storage) of the personal data processing operations when the data are processed violating provisions of the law;
4. To give no agreement on the processing of the personal data;
5. To obtain compensation from the administrator for data losses.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2018 Volume 5 Number 3 (March)
http://doi.org/10.9770/jesi.2018.5.3(9)

The data subject in order to avoid violations related to the personal data should participate as an active participant in the process of personal data protection, and not only as a passive observer of the implementation of personal data protection law. With the entry into force of the European Charter of Fundamental Rights (2012/C 326/02) in 2009, the protection of personal data is included in the list of basic human rights. Part 1 of Article 8 of the Charter states everyone has the right to the protection of personal data concerning him or her. Provisions of Part 2 of Article 8 of the Charter enable data subjects to verify the control of their personal data and the lawfulness of processing: "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".

Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter – the Data Protection Directive 95/46/EC) lays down the fundamental rights and freedoms of natural persons, and in particular their privacy with regard to the processing of personal data including the virtual social networking environment. Provisions of the Data Protection Directive 95/46/EC do not restrict or prohibit the free movement of personal data between Member States for reasons relating to the protection of personal data. The following regulatory principles established by the Data Protection Directive 95/46/EC can be distinguished:

1. Data quality (article 6). Personal data must be:
   - Processed fairly and lawfully;
   - Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
   - Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
   - Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
   - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.
2. Data processing leditimate (article 7). Personal data may be processed only if:
   - The data subject has unambiguously given his consent;
   - Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
   - Processing is necessary for compliance with a legal obligation to which the controller is subject;
   - Processing is necessary in order to protect the vital interests of the data subject;
   - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;
   - Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.
3. Special categories of data (article 8). Prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life, except in certain cases.

As regards online social networks, the document of the Working Party on Data Protection which was set up on the basis of Article 29 of Directive 95/46 / EC – the Opinion No. 5/2009 on the online social networks (hereinafter – "the Opinion") is of utmost importance. The Working Party on Data Protection established by Article 29 of Directive 95/46/EC identifies two main categories of danger to privacy and personal data protection: the lack of

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2018 Volume 5 Number 3 (March)
http://doi.org/10.9770/jesi.2018.5.3(9)

control of data stored by remote computing; lack of information on data processing operations. Users who submit their personal data to social networks or third parties operating in social networks lose control of these data and do not know which tools are used to ensure the availability, confidentiality and integrity of personal data. Consumers due to the lack of data processing information may be exposed to threats and risks as the personal data can be processed by multiple administrators; personal data can be stored in different geographic areas; personal data can be transferred to third parties which may not provide a sufficient level of protection of the personal data.

Summarizing the material presented in the Opinion, the Working Party presents specific guidelines for providers of online social networking services. These can be distinguished:

- Social network service should inform users of their identity, and provide comprehensive and clear information about the purposes and different ways in which they intend to process personal data;
- Social network service should offer privacy-friendly default settings;
- Social network service should provide information and adequate warning to users about privacy risks when they upload data onto the social network service;
- Users should be advised by social network service that pictures or information about other individuals, should only be uploaded with the individual's consent;
- At a minimum, the homepage of social network service should contain a link to a complaint facility, covering data protection issues, for both members and non-members;
- Marketing activity must comply with the rules laid down in the Data Protection and ePrivacy Directives;
- Social network service must set maximum periods to retain data on inactive users. Abandoned accounts must be deleted;
- Users should, in general, be allowed to adopt a pseudonym.

It should be noted that although the opinion of the Article 29 Data Protection Working Party is not legally binding, however, considering the aim of creating a separate legal regulation of online social networks in the future, its contribution is undoubtedly significant. Despite the fact that legal regulation is under the constant pressure to follow the technological progress, and perhaps in general is not able to react in a timely manner to rapid changes, the progress made by the Data Protection Working Party is significant and is likely to continue to be successful (Štitilis et al., 2012).

The Berlin International Working Group on Data Protection in Telecommunications (2008) adopted a document called the Rome Memorandum (hereinafter referred to as "Memorandum"). This is a set of guidelines where, assessing the potential risks of online social networking services, recommendations are also made to the legislator, data controller and individuals using social networking services. The following risks identified in the Memorandum, and related to the use of social networks can be distinguished:

- Data, once published, may stay there literally forever - even when the data subject has deleted them from the "original" site, there may be copies with third parties;
- Users are not openly informed about how their profile information is shared and what they can do to control how it is shared;
- For many providers of social networks user profile data and the number of unique users is the only real asset these companies have, this may create additional risks for proportional collection, processing and use of users' personal data;
- Giving away more personal information than you think you do: For example, photos may become universal biometric identifiers within a network and even across networks;
- Misuse of profile data by third parties: This is probably the most important threat potential for personal data contained in user profiles of social network services.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2018 Volume 5 Number 3 (March)
http://doi.org/10.9770/jesi.2018.5.3(9)

Recommendations of the Memorandum emphasize that internet social service providers would implement transparent data processing policies, provide an opportunity and encourage users to register by pseudonyms. Particular attention is paid to default privacy settings describing them as playing the essential role in ensuring the user privacy protection measures. Providers of the social network services should ensure prompt cooperation with users who are defending data subject's rights. It is also appropriate to provide disciplinary measures against users who act abusively or otherwise maliciously in the environment of online social network. The social network users should think twice before disclosing personal information, not register on the social networks using their true name and surname, respect the privacy of other users, check privacy policies, and use privacy settings to restrict access to their personal data to the maximum extent possible.

Having analysed the legal regulation of social networks at the international and European level, it is possible to conclude that although there is not yet a special binding regulation on the internet social networks, various non-binding legal acts exist, and are essential for gradual achieving of such a goal. Self-regulation plays a large role. In order to avoid violations related to the personal data, the data subject should be involved in the process of personal data protection as an active participant, and not remain a passive observer of the implementation of personal data protection laws.

3. Personal data of Facebook users on the social network

Facebook is a multi-semiotic media environment where users communicate with text, links, photos, videos, and sound – using different features such as chat, messages, status updates, and the wall (Valtysson, 2012). To register on Facebook social network, the user must submit the following details - name, surname, e. mail or telephone, year of birth, and gender. In addition the data subject shall create the password. The person in the electronic space can be identified by the unique title (name) and password (Štitilis et al., 2016). In order to login to the Facebook network, the user must enter the password and e-mail or phone number. Carminati defining the virtual social networks described the following determining features: 1. The internet service based platform were user social links and relations are developed; 2. The users can share interests, likes, activities, and contacts; 3. Each user has the personal account with his/her social contacts, links and other services. Facebook users create a profile page that contains information pertinent to them which can then be viewed by their friends. Such information varies from personal status updates, personal posts and photographs which have either been uploaded by a user or a user's friend. Facebook also provides access to third party applications that a user can add to their page. (Comer et al., 2012). On the virtual social network platform, the operation of services is based on the collection of immense amount of data about the data subject. Information that the user can optionally place on the Facebook social network (Table 2).

Table 2. User data on Facebook

Work and Education	**Work**. Company (Where have you worked?), Position (What is your job title?), City/Town, Description, Time Period. **Education**. Professional skills, College, High school – School (What school did you attend?), Time Period, Graduated, Description, Concentrations, Attended for (College or Graduate School).
Places You've Lived	**Current city and hometown.**
Contact and Basic Info	**Contact information**. Mobile Phones, Email, Facebook. **Websites and social links.** **Basic information.** Birth Date, Birth Year, Gender, Languages, Interested In, Religious Views, Political Views.
Family and Relationships	**Relationship**. Relationship Status (Single, In a realatioship, Engaged, Married, In a civil union, In the domestic partnership, In an open relationship, It's complicated, Separated, Divorced, Widowed). **Family Members**. Family Member (Daughter, Son, Child, Mother, Father, Sister, Brother,

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2018 Volume 5 Number 3 (March)
http://doi.org/10.9770/jesi.2018.5.3(9)

	Aunt, Uncle, Niece, Nephew, Granddaughter...).
Details About You	**About you** (Write some details about yourself). **Other's names** (Add a nickname, a birth name...). **Favorite quotes** (Add your favorite quotations).
Life Events	**Life Events**. Work & Education, Family & Relationships, Home & Living, Health & Wellness, Travel & Experiences.
Likes	**Likes**. Movies, TV Shows, Music, Books, Sports Teams, Athletes, People, Restaurants. Apps and Games...
Other information	**Friends, Photos, Videos, Events, Groups**...

Source: authors

What information users share with the Facebook social network is an individual choice, some of them alone provide a lot of information about themselves and the whole surrounding reality, and others strive to protect their privacy and publish only minimal information. Facebook is often depicted as a platform to see and to be seen (Pempek et al., 2009), to express an identity (Lee, 2012), and to help highlight otherwise obscure and seemingly mundane aspects of one's life (Yau, Schneider, 2009). For users, it is very important to manage their privacy. The Facebook social network enables its users to decide independently how much and what information to make available to different individuals or interest groups. This is done with privacy settings. Privacy settings are often criticized because of their complex management. It is also possible to identify specific individuals and interest groups with which information will not be shared. Information of the user-generated profiles may be public, semi-public, and private depending on the needs of the user (Table 3).

Table 3. Types of the user data publicity

Public information	Information which is publicly available to all Facebook users.
Closed information	Information which is publicly available to all Facebook users or individual friends and specific interest groups.
Secret information	Information which is available only to the Facebook account administrator.

Source: authors

Once a profile is created, the new user can start looking for friends and send friend requests. When accepted, Facebook connects the two individuals by allowing them to see each other's profile page and by adding their activities to one another's news feed (Caers et al., 2013). Users are encouraged to find their acquaintances and thus expand their virtual network. Early research by Lewis and West (2009) found that users with a large number of Facebook friends do not necessarily have the same number of close friends in everyday life, which supports the claim mentioned above. The most common strategy for privacy protection - decreasing profile visibility through restricting access to friends - is also a very weak mechanism; a quick fix rather than a systematic approach to protecting privacy. Most users do not seem to realize that restricting access to their data does not sufficiently address the risks resulting from the amount, quality and persistence of the data they provide (Debatin et al., 2009).

Joinson (2008) identified seven reasons for using the Facebook social network to help the active Facebook users achieving goals that provide emotional support and information sources:

1. Establishment, maintenance and restoration of social contacts;
2. Group joining, organizing events and communicating with like-minded people;
3. Photo viewing and publicizing;
4. Use of applications – games, gadgets, quizzes, etc;
5. Establishing contacts with people who are not in the electronic space as well as tracking them in order to find out more about them;

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2018 Volume 5 Number 3 (March)
http://doi.org/10.9770/jesi.2018.5.3(9)

6. Browsing the social network by reviewing profiles of people who are not acquaintances;
7. Publication of new information and reviewing of information updated by the other users.

Virtual social networks have changed consumer behaviour, thinking and actions. In the modern world, social networks became a part of everyday activities without which life is hard to imagine. It should be stressed that the Opinion expresses considerable concern about the default privacy settings used for the internet social networks. Only a small percentage of users make any changes to the default settings when registering on the internet social networks. Accordingly, the Working Party considers that online social service providers should provide privacy-friendly default settings enabling users to freely and explicitly allow any access to their profile content beyond the reach of their chosen addressees in order to reduce the risk of unlawful processing of data by the third parties.

4. Consumer interaction with third parties

The virtual social network model is primarily based on the collection and sharing of personal data by the data subject. All of these actions are often accompanied by third parties. As we already know, one of the reasons for using Facebook is applications. Facebook applications are programmes that work in the Facebook environment, use the functions of this social network, and there can be two types of applications, namely those created by the Facebook including events, groups, offers, etc., and those created by the third parties. The Facebook social network has thousands of apps created by the third parties with tens of millions of users for some of them. Users voluntarily share their personal data provided for Facebook in exchange for the third-party services acquired through the Facebook's third-party applications. It is enough to double-click with the button of the "mouse", and an approved (identified) user can already use the services of the website. Not going into details, everything seems quick, uncomplicated, and convenient; however, not all users responsibly evaluate what their personal data are "going" to the third parties providing services. In the case of a Facebook user's standard authentication, if data provided to the third-party are not edited, the user clicking on the “Continue as (User name)” button confirms that he/she agrees to transfer to the third party the maximum amount of personal data that are requested. The problem is that many users due to lack of attention or knowledge or simple laziness share the maximum amount of their personal data. The third-party application administrators selectively determine which personal data will be requested from users, and the public profile data submission is mandatory (Fig. 1).

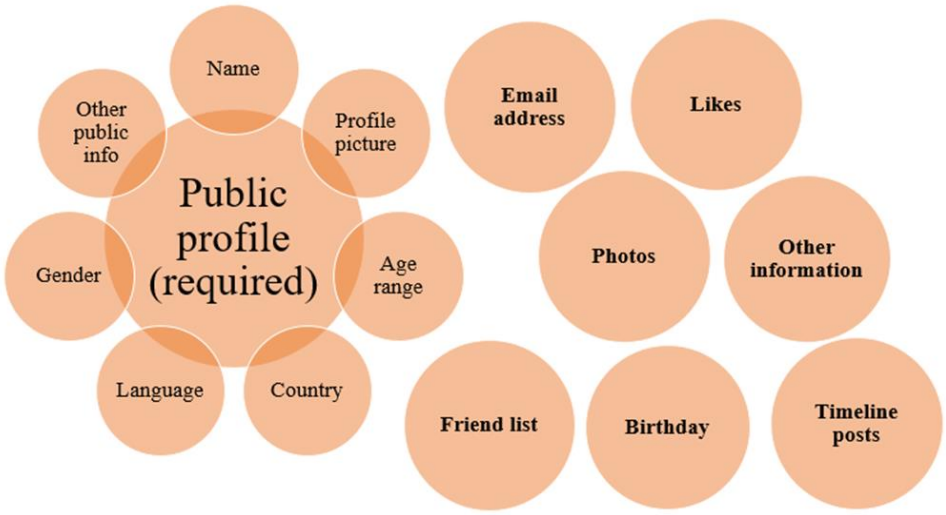

Fig. 1. Third-party may requested personal data from the user

Source: designed by the authors

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2018 Volume 5 Number 3 (March)
http://doi.org/10.9770/jesi.2018.5.3(9)

Hull et al. (2011) suggest visualization enhancements of the third-party apps information accessing and publishing practices. In doing so, users might have a better awareness how the app will use their information and thus users might be able to avoid some undesirable information leakage. Without the user's consent, the third-party applications do not have the right of access to the user's personal data. To limit third-party apps' information access, Facebook primarily relies on the OAuth 2.0 protocol which is used for third-party authentication and authorization. In the traditional client-server authentication model, the client can access a protected resource on the server by authenticating with the server using the resource owner's credentials. OAuth 2.0 adds an authorization layer and separates the role of the client (third-party application) from that of the resource owner (Facebook user) (Hammer-Lahav et al., 2011). The flow of the OAuth 2.0 protocol is shown in Fig. 2.

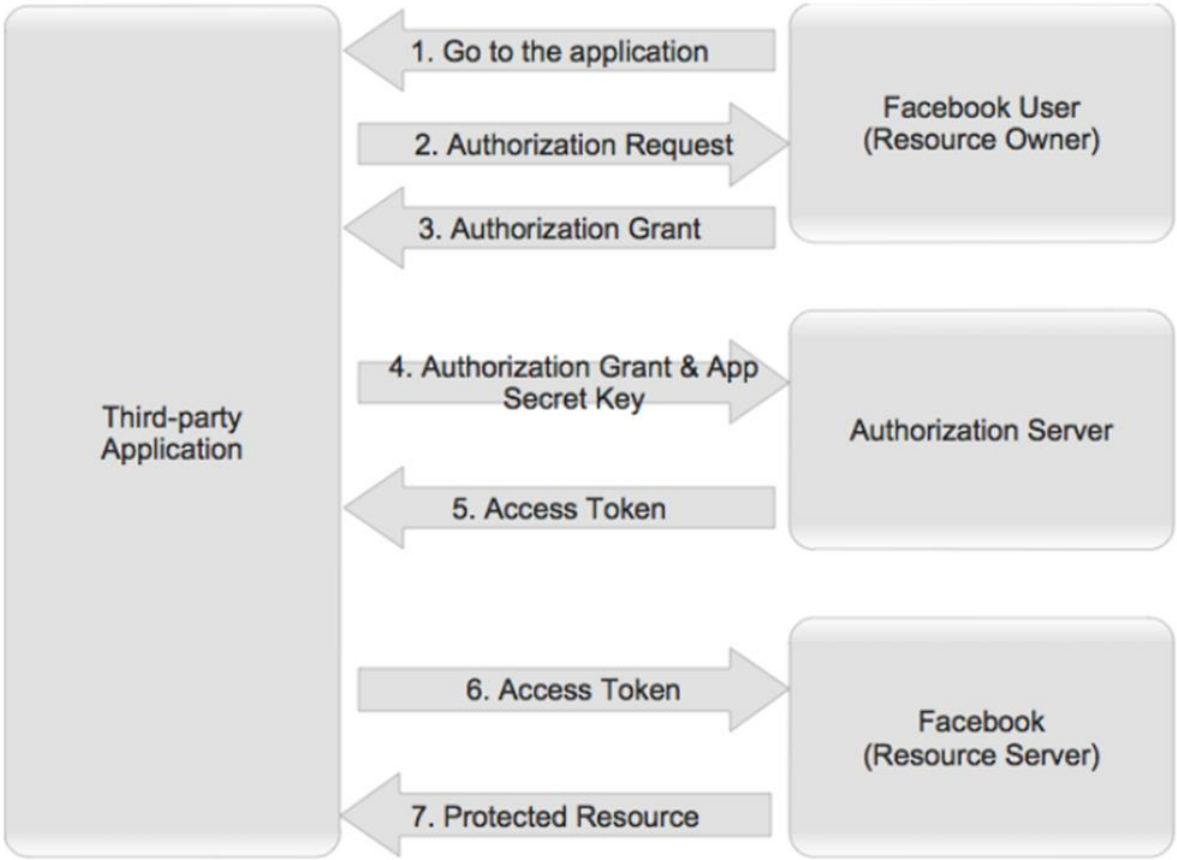

Fig. 2. The flow of the OAuth 2.0 protocol

Sourse: Wang et al., 2011

Users are interacting, competing, communicating, and entertaining themselves. And their privacy concerns are centered around sharing data with other people on the social network, with almost no understanding of the data sharing that occurs with the application developers. The end result is that there are serious risks of applications maliciously harvesting profile information, and users are not truly understanding and consenting to these risks. (Besmer, Lipford, 2010). Third-party application developers provide social network user privacy policies that specify the terms that the user must accept prior to using the application. Privacy policies are often overlooked due to their complexity and scope. In this case, consumers become vulnerable because they do not know if their

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2018 Volume 5 Number 3 (March)
http://doi.org/10.9770/jesi.2018.5.3(9)

rights of personal data subjects are guaranteed. When a user launches a third-party application, there are three possible scenarios (Fig. 3).

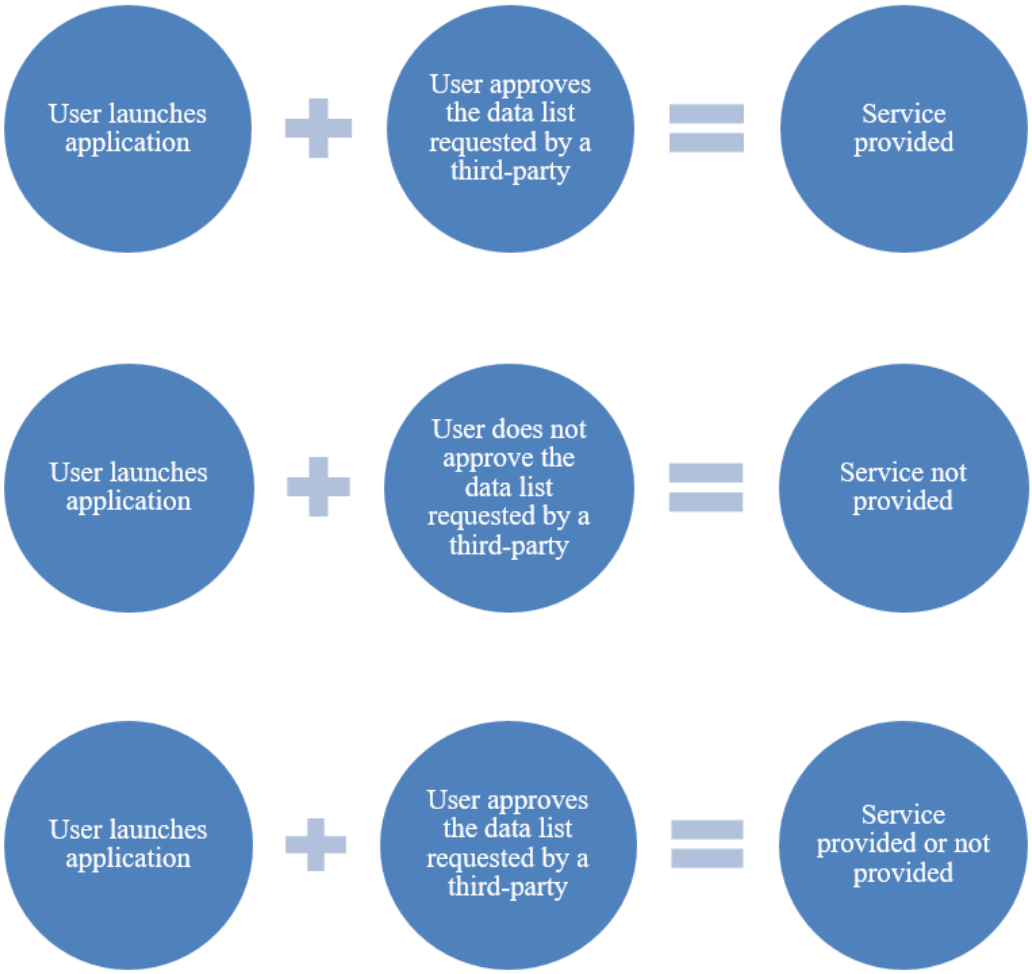

Fig. 3. User and the third-party application interaction model

Source: designed by the authors

Adding to these concerns, a Wall Street Journal study found numerous third-party applications (apps) on Facebook extracting identifiable user information from the platform and sharing this bounty with advertising companies (Steel, Fowler, 2010). The main problem with the virtual social network Facebook, as well as other virtual social networks, is that the purpose of data collection and administration is either obscure or too broadly defined (Karg, Fahl, 2011). Users should focus on the third-party privacy policies and only after thorough review initiate the user identification process. They should not immediately give consent to a third party's request and provide access to the personal data before performing data editing. Editing allows denying access to data that you do not want to share with the third party. Choosing not to provide access to the third party may result in the service denial, in which case it is always possible to repeat the procedure and grant access to the requested data.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2018 Volume 5 Number 3 (March)
http://doi.org/10.9770/jesi.2018.5.3(9)

Conclusions

Having analysed the legal regulation of social networks at the international and European level, it is possible to conclude that there is not yet a specific binding regulation on the internet social networks; nevertheless various non-binding legal acts are essential for ensuring the security of personal data. Social networks are continually developing and improving their functionality, and addressing various issues related to the protection of user personal data. Self-regulation plays a large role. The data subject should be involved as an active participant in the personal data protection process in order to avoid violations related to the personal data.

Users of various virtual social network services often overlook possible risks or even do not expect them on the virtual social networks. Also a part of the users simply ignore the perceived risks. Users are solely responsible for uploading information on the Facebook social network as well as for the use of third-party applications. Without the user's consent, the third-party applications do not have the right of access to the user's personal data, which is because of the OAuth 2.0 protocol.

Guidance on what actions should be taken or avoided by individual data subjects in order to better ensure the protection of personal data:

1. Do not share on the Facebook the information that could cause damage in case of information leakage or sharing.
2. Use the nicknames instead of your real name and surname registering on the Facebook network. In this way, users will retain their privacy as their true identity is not revealed.
3. Review the default privacy settings of the Facebook and personalize them to ensure enhanced personal data security. The default Facebook settings are customized by the standard for users who are willing to publicize a lot of personal information.
4. Evaluate the reliability of a third-party application before giving access to your personal data. The Facebook social network is a platform providing possibility to operate third-party applications. With a large number of third-party applications, the user has the freedom to choose.
5. Read privacy policies before you start using third-party applications, and note for what purposes the particular website uses personal data from the user and how long the data are stored/ processed; whether the personal data administrator ensures the security of the user's personal data; what terms are for the website privacy policy and service provision changing and what modes for informing the user when they are changed; what responsibility of the website administration is envisaged regarding the service they provide and what risks are being taken by the user of website.
6. Perform editing for personal data in order to avoid the maximum data sharing with third parties during user authentication when you launch a third-party application on the Facebook.

References

Besmer, A.; & Lipford, H. 2010. Users' (mis)conceptions of social applications, *Proceedings of Graphics Interface.* Retrieved from https://pdfs.semanticscholar.org/b5e4/fb0eec3457cacf24ddfa0e6d38e98975edec.pdf

Boyd, D.; & Ellison, N. B. 2007. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer–Mediated Communication* 13(1): 210-230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Caers, R.; Feyter T. D.; Couck M. D.; Stough, T.; Vigna, C.; Bois, C. D. 2013. Facebook: A literature review. *New Media & Society* 15(6): 982-1002. https://doi.org/10.1177/1461444813488061

Carminati, B.; Ferrari, E.; Viviani, M. 2014. *Security and trust in online social networking*. Morgan & Claypool publishers. https://doi.org/10.2200/S00549ED1V01Y201311SPT008

Comer, R.; Kelvey, N. M.; Curran, C.2012. Privacy on Facebook. *International Journal of Engineering and Technology* Volume 2(9): 1626-1630. https://doi.org/10.1080/15536548.2014.912909

Debatin, B.; Lovejoy, J. P.; Horn A-K.; Brittany, N.; Hughes, B. N. 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication* 15(1): 83-108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

EUR-Lex, 1995 October 24, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

EUR-Lex, 2012 October 26, *Charter of Fundamental Rights of the European Union*. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

European Commission, 2009 June 12. *Article 29 Data Protection Working Party: Opinion 5/2009 on online social networking*. Retrieved from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_lt.pdf

European Data Protection Supervisor, *Data Subject definition*. Retrieved from https://edps.europa.eu/node/3099#data_subject

Fogel, J.; & Nehmad, E. 2009. Internet social network communities: risk taking, trust, and privacy concerns, *Computers in Human Behavior* 25(1): 153-160. https://doi.org/10.1016/j.chb.2008.08.006

Hammer-Lahav, E.; Recordon, D.; Hardt, D. 2011. *The OAuth 2.0 authorization protocol draft-ietf-oauthv2-12*. Retrieved from https://tools.ietf.org/html/draft-ietf-oauth-v2-10

Hull, G.; Lipford, H. R.; Latulipe, C. 2011. Contextual gaps: Privacy issues on Facebook. *Ethics and Information Technology* 13(4): 289-302. https://doi.org/10.1007/s10676-010-9224-8

Yau, N.; & Schneider, J. 2009. Self-surveillance. *Bulletin of the American Society for Information Science and Technology* 35(5): 24-30.

International Working Group on Data Protection in Telecommunications. 2008. *Report and Guidance on Privacy International Working Group on Data Protection in Telecommunications.* Retrieved from https://icdppc.org/wp-content/uploads/2015/03/International-Working-Group-on-Data-Protection-in-Telecommunications.pdf

Joinson, A. N. 2008. 'Looking at', 'looking up' or 'keeping up with' people? Motives and uses of Facebook. In Proceedings of the 26th Annual SIGCHI Conference "on Human Factors in Computing Systems" Florence, Italy, April 05-10 2008, CHI '08, ACM, New York, 1027–1036. https://doi.org/10.1145/1357054.1357213

Kang, J. 1998. Information privacy in cyberspace transactions. *Standford Law Review* 50(4): 1193-1294. https://doi.org/10.2307/1229286

Karg, M.; Fahl, C. 2011. Rechtsgrundlagen für den Datenschutz in sozialen Netzwerken. *Komminakation und Recht* 7(8): 456-458.

Korauš, A.; Dobrovič, J.; Rajnoha, R.; Brezina, I. 2017. The safety risks related to bank cards and cyber attacks, *Journal of Security and Sustainability Issues* 6(4): 563-574. https://doi.org/10.9770/jssi.2017.6.4(3)

Lee, E. 2012. Young, black, and connected: Facebook usage among African American college students. *Journal of Black Studies* 43(3): 336-354. http://journals.sagepub.com/doi/pdf/10.1177/0021934711425044

Lewis, J.; & West, A. 2009. 'Friending': London-based undergraduates' experience of Facebook. *New Media & Society* 11(7): 1209-1229. https://doi.org/10.1177/1461444809342058

Malinauskaitė-van de Castel, I. 2017. Duomenų subjekto teisės virtualiuose socialiniuose tinkluose. *Mykolo Romerio universitetas*. Retrieved from https://vb.mruni.eu/object/elaba:23456482/23456482.pdf

Menshikov, V.; Lavrinenko, O.; Sinica, L.; Simakhova, A. 2017. Network capital phenomenon and its posibilities under the influence of development of information and communication technologies, *Journal of Security and Sustainability Issues* 6(4): 585-604. https://doi.org/10.9770/jssi.2017.6.4.(5)

Oecd.org, 1980 September 23, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved from http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Parent, W. A. 1983. Privacy, Morality, and the Law. *Philosophy & Public Affairs* 12(4): 269-288. Retrieved from http://www.jstor.org/stable/2265374

Pempek T. A.; Yermolayeva Y. A.; Calvert S. L. 2009. College students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology* 30(3): 227-238. https://doi.org/10.1016/j.appdev.2008.12.010

Privacy International.org, Data protection definition. Retrieved from https://www.privacyinternational.org/explainer/41/101-data-protection

International Working Group on Data Protection in Telecommunications. 2008. *Report and Guidance on Privacy in Social Network Services "Rome Memorandum".* Retrieved from http://194.242.234.211/documents/10160/10704/1531476

Statista.com, 2018. *Number of social network users worldwide from 2010 to 2021 (in billions)*. Retrieved from https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users

Steel, E.; & Fowler, G. 2010 October 18. Facebook in privacy breach. *The Wall Street Journal*, Retrieved from https://www.wsj.com/articles/SB10001424052702304772804575558484075236968

Šišulák, S. 2017. Userfocus - tool for criminality control of social networks at both the local and international level, *Entrepreneurship and Sustainability Issues* 5(2): 297-314. https://doi.org/10.9770/jesi.2017.5.2(10)

Štitilis, D.; Gustauskas, V.; Malinauskaitė, I. 2012. Asmens duomenų apsaugos virtualiuose socialiniuose tinkluose teisinė aplinka [The legal environment for personal data protection in virtual social networks]. *Societal Innovations for Global Growth* 1(1): 288-308. Retrieved from http://etalpykla.lituanistikadb.lt/fedora/objects/LT-LDB-0001:J.04~2012~1367188641078/datastreams/DS.002.0.01.ARTIC/content

Štitilis, D.; Kiškis, M.; Limba, T.; Rotomskis, I.; Agafonov, K.; Gulevičiūtė, G.; Panka, K. 2016. *Internet and Technology Law*. Vilnius:

Valtysson, B. 2012. Facebook as a Digital Public Sphere: Processes of Colonization and Emancipation. *Cognition, Communication, and Co-operation* 10(1): 77-91. Retrieved from https://www.triple-c.at/index.php/tripleC/article/view/312/339

Wang, N.; Xu, H.; Grossklags, J. 2011. Third-Party *Apps on Facebook: Privacy and the Illusion of Control*. In Proceedings of the ACM Symposium on Computer Human Interaction for Management of Information Technology (CHIMIT). Boston, MA.

Wasserman, S.; & Faust, K. 1994. *Social network analysis: methods and applications*. New York: Cambridge University Press.

Westin, A.1968. Privacy and Freedom, *Washington and Lee Law Review* 25(1): 166-170. Retrieved from https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?referer=https://www.google.lt/&httpsredir=1&article=3659&context=wlulr

Zaidieh, A. J. Y. 2012. The Use of Social Networking in Education: Challenges and Opportunities. *World of Computer Science and Information Technology Journal* 2(1): 18-21. Retrieved from http://wcsit.org/pub/2012/vol.2.no.1/The%20Use%20of%20Social%20Networking%20in%20Education%20Challenges%20and%20Opportunities.pdf

Zeman, T.; Břeň, J.; Urban, R. 2017. Role of Internet in Lone Wolf Terrorism, *Journal of Security and Sustainability Issues* (2): 185-192. https://doi.org/10.9770/jssi.2017.7.2(1)

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2018 Volume 5 Number 3 (March)
http://doi.org/10.9770/jesi.2018.5.3(9)

Tadas LIMBA is the Professor at Mykolas Romeris University, Lithuania. He has published over 30 articles in Lithuanian and foreign scientific journals, monograph, textbook, focused on e-government and e-business. His additional areas of research and expertise are – IT law regulation and policy; digital content, digital media, privacy and data protection issues. Tadas Limba is a member of Lithuanian Computer Society since 2007. Since 2013 he is Asia Center Board Member, South Korea's representative at Mykolas Romeris University. He is visiting professor at Zaragoza University in Spain. He plays an active role in international communication and development of joint double degree studies program with South Korea Dongseo University.
ORDCHID ID: orcid.org/0000-0003-2330-8684

Aurimas ŠIDLAUSKAS. He got two Master's degrees in Electronic Business Management (Cybersecurity Management in 2018 and Electronic Business Management in 2015) from Mykolas Romeris University. His areas of interest are cybersecurity, data protection, IT systems, and entrepreneurship.
ORCID ID: orcid.org/0000-0003-4580-2173

Copyright © 2018 by author(s) and VsI Entrepreneurship and Sustainability Center
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access