Privacy in Social Networks

Evidence Monday

University of Trento

Privacy and Intellectual Property Rights

5th December, 2018

Abstract

With a fast growing economy and a speedy increase in popularity of social networks like Facebook, Instagram, Twitter, Google plus and so on, users on social networks have been experiencing threats in privacy of their personal data. The simplest form of data breach occurs when an unauthorized user gains access to the account of another user. However, users' behavior and awareness to the network's terms and conditions affect privacy and security issues. A well-informed user will not disclose sensitive data such as address, phone number or financial information for public access. One of the ways to reduce data privacy issue is to limit the amount of data that is shared publicly by users. Also, a good understanding of legislation and laws concerning data privacy rights in social networks is necessary. This paper briefly addresses some threats to privacy, past privacy issues in some social networks, using Facebook, Instagram and Twitter as case studies, the inherent dangers of social network. We also look briefly at the General Data Protection Regulation (GDPR) and its relationship with users, privacy relating to intellectual property on social networks, some precautions and tips to avoid data breach.

Keywords: Social Networks, Privacy, GDPR, Intellectual Property, Data breach.

1. Introduction

We are experiencing a continuously revolving world of an informative age where digital technologies (or a touch of it) have taken over almost everything. Impacts are widely seen in the banking sector, the power sector, agriculture, social networks and the likes and are in no doubt implemented to improve our daily productivity and in some cases, sociology. Some examples of the impacts of these technologies include: shopping being made easy with online accessibility to a customer's bank details, the use of ATM cards and credit cards, the recent machine learning-based approach for detecting infected agricultural products and so on. Social Networks have made huge marks in this sphere, largely improving communication and seamless transfer of data. Despite these tremendous impacts and benefits on culture and the society, there are drawbacks owing to privacy of users' data. With vast exposure of personal information on these networks internet, a privacy of a user's data is threatened. Since users are mostly concerned about protection of their data, however insignificant it may be, the issue of privacy can never be over-emphasized. Hence, data analysts, law personnel and security expert have been working so hard to proffer solutions to this raging situation.

2. Literature Review

The issue of privacy has been plaguing our society and culture for centuries and it is deeply rooted in our ancient societies. Traditionally, we can say that the idea of privacy comes from the difference between public and private i.e the distinction an individual makes between him/her and the outer world. In the 19th century, there were only issue of mental and physical privacy but the birth of real privacy issues came with urbanization. As population growth increases, people started to live in cities and crowded places, hence, a breach in physical privacy. Also the emergence of social networks has caused huge concern in data privacy and protection. *Samuel D. Warren* and *Louis D. Brandeis* in their article *The Rights to Privacy* (1890) first recognized the threats to privacy by technological and societal developments.

2.1 Privacy Definitions

There have been several claims that privacy is universal yet there has been no proper universal definition of privacy. Privacy largely depends on what people consider private and the context of information sharing. *Alan Westin*, an American Law professor claimed that privacy can be affected in three aspects: the socio-cultural, the political and the personal aspect. Here, he explains that the individual plays a vital role in privacy, that is, the individual can dictate the limit between him/her and the outside world. However, *Daniel Sloove* saw a limitation to this reasoning and defined privacy in six categories: The right to be let alone, intimacy, secrecy, control of personal information and limited access to self. *Ruth Gavison* an Israeli law professor defines privacy as a concern of a user's accessibility: to what extent is a user known or what extent does a user has physical access to others. *Charles Fried* defined privacy as the control a

user has over his/her information. An Hungarian Jurist, *Máté Dániel Szabó* argued that privacy is the right of a user to make decisions for himself. All these definitions point out some salient points about privacy. Having an understanding that the definition of privacy must be in alignment with current socio-economic standard and structure, it has therefore proven to be an herculean task for the law and legal practitioners to come up with a concrete and generally accepted definition for privacy. However, it therefore begs the question: Since the subject at hand (privacy) is not explicitly determined, can there be a possibility of an effective legal protection?

2.2 History and Evolution of Data Privacy in Social Networks

As the years go by, we have experienced a great evolution of privacy each associated with distinct issues.

a.) Early 1990s: The first true Acknowledgement of Privacy issues online

In the early emergence of World Wide Web, users had to set up profiles online and since an average user at that time did not have a computer of his own, he/she had to make use of dialed-up internet access. There were consumers who found it fascinating to publish identifiable personal information online never knowing privacy will be an issue. Also, some facilities at that time, who were able to comfortably access the internet through controlled portals like America Online (AOL) and The Microsoft Network (MSN) gave opportunities to individuals to share their personal data in a way that could impose threats. We might just say that in this age, privacy was not a serious issue for both the consumer and business providers. But we would not say privacy as an issue was completely ignored here because, in early 1994, the Electronic Privacy Information Centre built for itself a newsletter that covered online privacy and civil liberties issues.

b.) Mid-Late 1990s: Children as Unfortunate Targets

In this era, it was no doubt that privacy was centered around preventing children from exposure to pornographic content on the media, its proliferation and forbidding of online exploitation of children under the age consent. On October 21, 1998, *The Children's Online Privacy Protection Act (COPPA)* was enacted and in 2000, commercial websites were required to obtain parental consent before collecting, using or disclosing personal information of any child below the age of 13. COPPA went further stating the contents of the website operators' online privacy, how to seek parental consent and their (website operators) responsibilities towards the children.

c.) Early 2000s: Extension of Privacy to Adults

Then came web2.0, the ability of web browsers to process on their own, some powerful servers and of course, the emergence of social networks. Here, users were able to create profiles

that had all or some of their personal information, build businesses online and are able to network with diverse individuals from different demographic location. The big break of social network privacy came in 2003 after the launch of *MySpace.* In October 2004, the California Online Protection Act came to effect and it centres on educating a user of his/her rights to disclosure. This act imposed on all commercial operators who had dealings with users' personal information to include on their website, a visible and clearly identifiable link to the privacy policy. The law simple tenets were established: disclosed to the user how his/her personal information will be used and their ability to make required changes to the information provided.

d.) The 2010s: The Right to be Forgotten and Explicit User Control

Here, users are able to control (especially to stop usage) the amount of their personal data being used by website operators via cookies or other online trackers. In 2011, the *Children's Online Privacy Law* was amended by US representatives, Edward Markey and Joe Barton; it is called *"The Do Not Track Kids Act of 2011".* This contained regulations that stated the immediate removal of information of every minor from public view upon request. In October 2013, Assembly Bill # 370 was signed into law by Governor Jerry Brown. It stated that business owners must allow users the rights to freely exercise the collection or retraction of their data and allow a level of involvement of some third party-websites.

The Right to Be Forgotten has recently been a topic of exploration for legislators in the United State, the European Union and the world at large. Several laws have been passed as to the right to delete any online foot print or data. In January 2015, *The Eraser Bill;* an amendment of the Children's Online Privacy Law was enacted. This allowed minors the right to delete their previously posted content on any website. The European Court of Justice in 2014 ruled against Google for violating *The Right to be Forgotten Act.* Just recently, Cambridge Analytica ruled out Facebook for huge data breach and breach of trust which brought to light the essence of consumers to properly educate themselves on how Social Networks and Online Businesses use their data.

3. Discussion

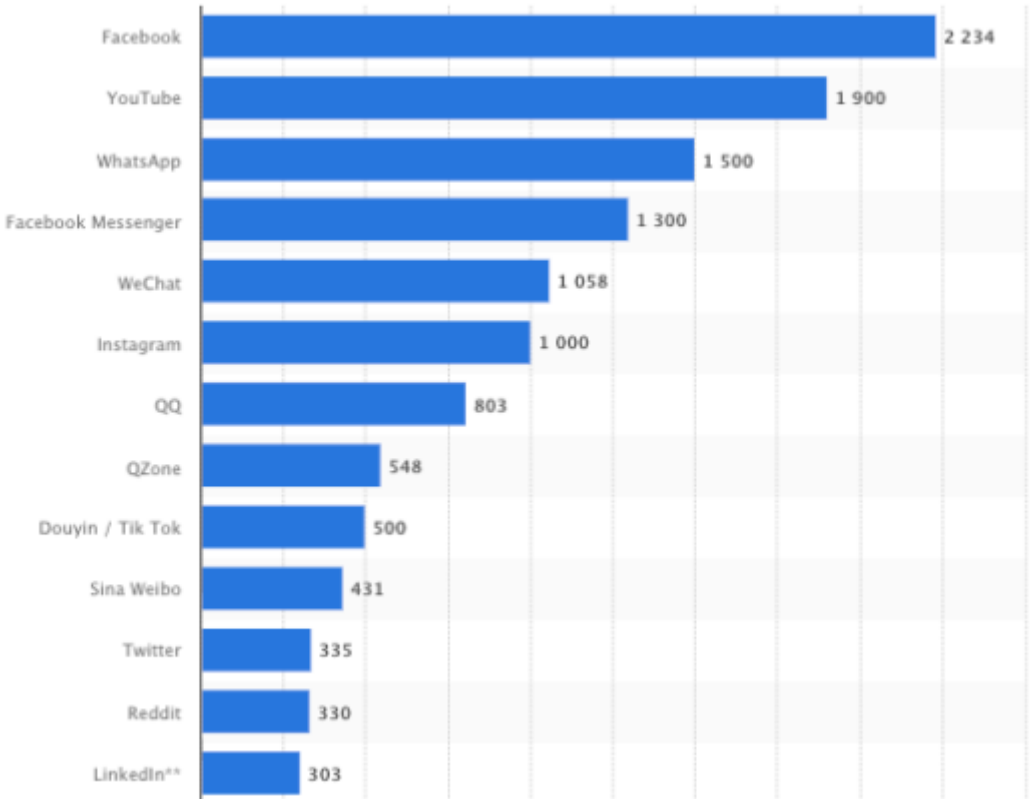
3.1 **Social Networks, Usage and Some Privacy Issues and inherent dangers**

Social networks and it is usage is a huge topic of discussion in this age. Over the years, we have experienced a sky-rocketing increase in usage of social networks by a large majority of youths, teenagers and adult. In targeting specific audience, there is need to also understand the difference in popularity of different social media and the number of account usage not just the number of accounts opened. Before going into the popularity of various social networks, it is worthy to answer the following questions: *How much of the world's population have access to the internet? How much of the world's population use Social networks? How much of the world's population use mobile phones?* So in answering these critical questions we observed that, in 2018, the number of internet users is about 4.021 billion users (7%), the number of social

network users is 3.196 billion users (13%) and the mobile phone users include 5.135 billion users (4%). 2017 had the highest increase of social media users in the years with Saudi Arabia with an increase of 32% making them the biggest break in the year. India, Indonesia and Ghana are other countries with fast growing social media user increase in the world. However, in terms of daily usage, Facebook has an average of 10.7% posts and 26.8% paid posts reach in total, making them the highest number of daily active users amongst all other social network platform. Some considerable statistics on usage of some social network platforms over the years is discussed below:

3.1.1 Most popular Social Networks (by Active Users)

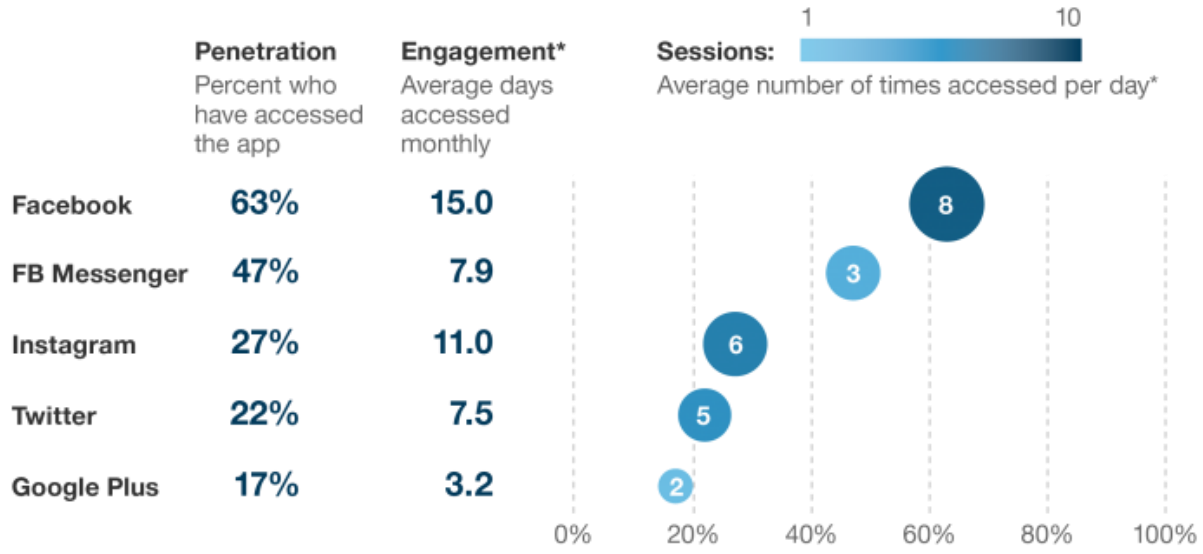
This demographic is based on statistics carried out in October 2018 by Statista and here we consider the following countries: India, Italy, US, Spain, Argentina, Ukraine, France, Germany, Mexico, Brazil, Malaysia, Indonesia, UK. This gives the number of active users (in million).



Insight from Statista

3.1.2 Most Engaging Social Network

Here we consider the penetration and engagement of the audience and social networks in terms of the amount of time the audience spends on the platform. The demographic display below is based on statistics gathered on December 2015 and the target audience was smart phone users above the age of 18 in the US.



Compiled by comScore

3.2 Privacy Issues in Social Networks and some inherent dangers

Following the demographic compiled by different sources above, we see a remarkable dominance of Facebook and other social platforms worthy of mention. In this part of the paper, we will briefly consider past privacy issues relating to Facebook, Instagram and Twitter.

a.) Facebook

Facebook being the most popular social network platform in the world, having over 2.271 billion active users has experienced series of unfortunate data privacy issues. Users, in the first four years experienced great dissatisfaction in its design and privacy issue but Facebook progressed through it all. In 2006, Facebook introduced a feature called 'News Feeds' of which users claimed it was intrusive. Users said they would not allow a feature blast their personal lives on their friends' timelines. This issue dies down as the 'News Feed' feature became a major break on the Facebook application. In 2007, Facebook experienced a huge set back in advertising privacy when users noticed that their online purchased can be tracked by companies and notifications were sent to their friends without any user's consent. This was salvaged as Facebook CEO; Mark Zukerberg created an option for users to opt out.

1. In 2011, the Federal Trade Commission claimed Facebook was violating its privacy of its users' private. The claim was that third party applications were allowed access to virtually all users' private information at will. This privacy issue died down as Facebook agreed to an independent privacy evaluation every year in the next 20 years.
2. In 2013, the users of Facebook experienced a threat to their data privacy as a bug in the application exposed the phone numbers and email addresses of over 6 million users. Facebook claimed this was done in a bid to match similar users and proffer recommendation to new users.

The bug was fixed and a notification was sent to users whose information might have been affected.

3. In 2014, Facebook experimented on a mood detection tool on its application using about half a million user accounts as test cases. As users expressed their displeasure towards this tool, it was pull out and a note of apology was sent by Facebook data scientists who claimed the purpose of the tool was to study and show the spread of emotions on social media.
4. In 2018, Cambridge Analytica exposed Facebook for the illicit collection of users' personal information. The claim was that Facebook violated some data protection laws by exposing users' details to politicians for campaign purpose and some mobile device manufacturing companies. This issue was the biggest fallout of the privacy issue of Facebook. It was resolved as an apology tour towards users affected and a change in data policy in favour of users' data protection.

b.) Instagram

Instagram is the social network platform for local and amateur photographers. It supports a host of features like real time video chat, networking with other users from verse geographical location and a host of others. There is a wrinkle in the idea of data protection on Instagram because of the known relationship between Facebook and Instagram and this is a big bother on privacy on this platform. In 2013, after the acquisition of Instagram by Facebook, users could only create Ads using Facebook's Ad Manager even if a business is intended to run on Instagram and not Facebook. This gives Instagram the liberty to use a user's Facebook personal data to target Ads at him/her. Just recently, Instagram released a feature that allows user save photo of another user on their profile with just one click. This has become a threat to privacy as users are questioning the safety of their photos. Also, there have been recent claims by users of Instagram about their account being hacked. Users complained about being locked out of their account as their personal information was changed by the hackers and efforts to reverse this change upon reports to Instagram proved to abortive.

c.) Twitter

Twitter is a social network that provides user a less intrusive privacy policy on their personal data. This does not exempt twitter from some privacy issues. In 2018, twitter admitted that locations of some of its users' tweets were revealed without their consent due to a bug. Some affected users reported that the location indicated on the tweet was false as it was either part of their search on the application or some place they have visited prior to the happening. The company sent out apology to affected users, claiming the bug has been fixed but it raised some doubts in the minds of users as two days after Google claimed to have gathered some locations of android smartphone users.

Some inherent dangers include:

i.) *Cyber stalking*: since it is easy to be connected with a host of friends and acquaintances and with disclosure of vast information (photos, videos, whereabouts) about oneself, it exposes a user to being stalked or bullied by another user on the network. Cyber stalking has been considered a grave offense and anti-stalking laws have been implemented to curb this menace. Penalty could be a restraining order or probation.

ii.) *Identity theft*: this becomes a threat when a user discloses certain private information like social security number on social platforms. It could also involve photographs; many celebrities have complained about breaches to their accounts. In order to curb this, users were advised to hide sensitive information as such from the public.

iii.) *Online victimization*: this happens when certain users on social platforms exhibit unethical mannerisms, making other users have a bad online experience. Research shows that majority of users affected by this menace are adolescence and teens and such victimizations are geared towards sexual harassments. To curb this, positive online behavior was largely promoted.

iv.) *Exposure to sexual predators*: research has shown that social networking sites with an ability to accommodate pseudo-users have been trolled with online prostitutes. To further emphasize on this, the lack of age verification on these sites prospered the growth of sexual prostitutes. Unfortunately, a large population of children has been lured to pedophiles because of this.

4. Results

4.1 LEGAL ACTIONS TO ENSURE DATA PRIVACY

4.1.1 General Data Protection Regulation (GDPR)

The GDPR is a regulation of data protection for users within the European Union (EU) and European Economic Area (EEA). It is targeted at giving individuals control of their personal data. It was adopted on 14th April, 2016 by the European Parliament and the Council of the European Union but implemented on 25th May, 2018. The GDPR also covers regulation of transfer of data outside EEA or EU region. It comprises two participants: the data controller and the data processor. *The data controller* is responsible for collection of data and must assign technical and organizational techniques used for collection. *The data processor* states the purpose of data processing, must also state how much time the data is being retained and must indicate if data is being shared with other third parties outside of the EEA.

The proposal brought about different issues as to many amendments were made. IT professionals expressed that compliance will require an increase in budget investment. It was observed that small businesses will be unable to fully participate as opposed to larger international technology companies like Facebook and Google. The GDPR proposal gained huge

support from businesses that saw the opportunities in making profit out of the data management strategy. Facebook and European Consumer Organisation were big supporters of this regulation.

International companies' adoption of the GDPR privacy standards was huge and this is an example of the Brussel Effect. In *The Brussel effect*, European Laws and regulations are being used globally as the basis of operation due to their gravities.

Some key changes in GDPR that differentiates it from previous privacy directives include:

a.) *Extraterritorial Applicability:* This is the biggest upgrade in the data privacy directive because it applies to all companies that deals with processing of private information of its users regardless of their location (European Union or otherwise). It also applies to controllers and processors processing personal data, goods or services in the EU, whether in the European Union or not. In the cases of Non-EU businesses, there is need to employ an EU representative for data processing.

b.) *Penalties:* An organisation can be fined 4% or € 20 million of its annual global turnover for GDPR breach. It is the maximum fine which can be paid as it is imposed on companies found guilty of a serious infringement. An example of a serious infringement is having insufficient consent from customers before processing their data while a minor offence could be when a company's data is not in order. This rule is applicable to both controllers and processors ('clouds' are no exception).

c.) *Consent:* Companies are now prohibited from using long and illegible terms and conditions rather, the form must be easily accessible, legible and understandable, having the purpose of data usage attached to it. Also, withdrawal of consent should be seamless.

d.) *Data Subject Rights*

- *Breach Notification:* Notifications of data breach is now mandatory in the GDPR and this must be done under 72 hours of breach awareness.
- *Right to Access:* The expanded rights of GDPR here require the data subject to seek confirmation from the controller concerning the purpose of the use of data. The controller needs to provide a form having this content. This has helped in improving data transparency across boards.
- *Right to be forgotten:* This is also called Data Eraser and it is the right granted to data subject to have their personal data to be erased by data controllers to prevent further usage by third paty applications. It is outlined in article 17.
- *Data Portability:* this is the right given to data subject to receive previously provided information and the right to give this information to another data collector.
- *Privacy By Design:* this rule is outlined in article 23 and it is requires data collectors to hold and process data only when it is absolutely necessary for completion of duties and it strictly limits access to personal data to those who need data for other purpose aside processing.

- *Data Protection Officers:* the appointment of DPOs is only mandatory when data collectors need to be under regular monitoring and in cases where large set of data subjects in relation to criminal cases are being dealt with.

4.2 Laws on Intellectual Property

One of the areas that have been on growing interest for a vast majority of persons has been privacy of intellectual property on social media. Since we are well aware that a small business can grow rapidly using social network tools as a means, there have been massive threats on intellectual property over the years. Therefore, some measures were promoted to in order to avoid future threats of intellectual property on Social networks. Here, businesses are required to include their employees in intellectual property strategies and intellectual property theft avoidance plans. This includes modifying the privacy policy of social networks and making sure employees adhere to it. The policy should explain sufficiently: Information about the confidential and proprietary agreements and how it is managed by the company, the use of the company's intellectual property rights, information about intellectual property rights, valid steps to be taken in cases of infringements, etc.

4.3 Other ways to ensure privacy

Other ways to ensure data privacy in social networks are: (a) Using Strong Password (b) Using Two factor Authentication (c) Ensure proper privacy setting of any social profiles (d) Avoid accepting requests from unknown users (e) Be sure of a link before clicking it (f) Be sure of an application before installation (g) Be sure of users you want to share your details with (h) Read thoroughly the privacy agreement. Here are some points what to look out for when reading privacy agreement:

- What happens to provided data when account is closed
- How long will one's personal data be stored
- How will a change in privacy policy be made aware to users
- In cases of data breach, how can a user complain

5. Conclusion

The issue of privacy in social networks is not one that will be resolved easily as social networks are experiencing a growing number in population of usage. Different users have unique reason for protection of their personal data; some are concerned about freedom of expression while other are concerned about access to their personal account. We see a wide variety of user experiences and expectations of data privacy as it varies with users of different age brackets. Social networks has changed the way users act on the internet. It is important for users to understand that no social network is perfect therefore; onus lies on users to adequately research on an application before installation or carefully read through the privacy policy provided by the application itself.

References

1. Souvik, B. (2018, January 12). *Five Privacy & Security Risks of Social Media & How to Prevent Those*. Retrieved from https://www.rswebsols.com/tutorials/internet/privacy-security-risks-social-media
2. Ladan, Ibrahim M., (2015). Social Networks: Privacy Issues and Precautions, *Haigazian University, Beirut – Lebanon*, (pp. 65&68-69).
3. Adams, Brittney L., (2012). Social Media and its effects on Privacy, *University of Central Florida, Orlando, Florida*, (pp. 51-54).
4. EU GDPR Portal. (2018). *GDPR Key Changes*, Retrieved from https://eugdpr.org/the-regulation/
5. WIKIPEDIA. (2018). *General Data Protection Regulation*, Retrieved from https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
6. IANS. (2017, November 26). *Privacy issues: Twitter admits to revealing location of users without consent*, Retrieved from https://cio.economictimes.indiatimes.com/news/social-media/privacy-issues-twitter-admits-to-revealing-location-of-users-without-consent/61803018
7. Yaqoob J., (2016, December 19). *Instagram's Update Causing Privacy Issues*, Retrieved from https://www.theodysseyonline.com/instagrams-update-causing-privacy-issues
8. Kosik H., (2018, March 29). *Is Instagram Collecting Data? Here's What To Know If You're Worried About Your Privacy*, Retrieved from https://www.bustle.com/p/is-instagram-collecting-data-heres-what-to-know-if-youre-worried-about-your-privacy-8631780
9. Newcomb A., (2018, March 24). *A timeline of Facebook's privacy issues — and its responses*, Retrieved from https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651
10. Caffey D., (2018, November 23). *Global social media research summary 2018*, Retrieved from https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

11. Pasierbinska-Wilson Z., (2015, February 26). *The History of Data Privacy in Social Data and its Milestones*, Retrieved from http://blog.datasift.com/2015/02/26/the-history-of-data-privacy-in-social-data-and-its-milestones/
12. Lukács A., (2012). What is Privacy? The History and definition of Privacy, *Faculty of Law and Political Sciences, University of Szeged*, (pp. 256-259).
13. Klinck R., (2018). *Intellectual Property Issues On Social Media*, Retrieved from https://www.klinckllc.com/ip-plan/social-media-ip/
14. WIKIPEDIA. (2018). *Privacy concerns with social networking services*, Retrieved from https://en.wikipedia.org/wiki/Privacy_concerns_with_social_networking_services