A PRIVACY BASED MONEY MAKING MODEL PROPOSAL ON SOCIAL NETWORKS

Uğur YOZGAT [*]
Ahmet Murat ÖZKAN[**]
Ömer Faruk OKTAR[***]

Abstract

With the development of information technologies companies can interact much easier and efficiently with their customers. In many cases; such as social networks, companies have the chance to create unique products / services for each customer where the information provided by users are actually essential part of the service. This is useful to maintain customer satisfaction and / or interaction, but on the other hand, there are concerns about privacy of personal information. In this paper we try to develop a model to demonstrate how personal information can turn into money on social networks and talk about privacy issues. We argue that privacy issues are an important barrier among social networks' money making efforts.

Keywords: social networks, privacy, money making, personal data

Özet

Bireyleri arkadaşları, aileleri ve/veya ortak ilgi alanlarına sahip oldukları diğer insanlar ile birbirine bağlayan sosyal ağların kullanıcı sayıları giderek artmaktadır. Özellikle 2000'li yılların ortalarında yükselişe geçen ve son yıllarda akıllı mobil cihazların yaygınlık kazanması ile hayatın her alanına ve anına giren sosyal ağların karlılıkları ve gelir modelleri de tartışılır olmuştur. Bu çalışmada, sosyal ağların veri tabanlarında tuttukları üyelere ait kişisel bilgilerin gizliliği baz alınarak basit bir model geliştirilmiş ve modele ilişkin sorgulamalar, bu ağları kullanan çeşitli gruplara uygulanan bir anket ile test edilmiştir. Anket uygulaması sonucunda, kişilerin sosyal ağlar ile paylaştıkları bilgilerin üçüncü taraflar ile paylaşılması ya da ele geçirilmesinden rahatsızlık duydukları ve sosyal ağlar ile daha az bilgi paylaşma eğilimine girdikleri gözlenmiştir. Bunun bir sonucu olarak, kişisel veriler ile uyumlu reklam ve içerik sunan sosyal ağların gelir modelleri sekteye uğrayabilmektedir.

Anahtar Kelimeler : sosyal, ağ, sosyal medya, network, gelir, kar

Introduction

Nowadays, more and more people join multiple social networks on the Web, such as *Facebook*, *Linkedin*, *Livespace* etc. to share information and updates of their lives and at the same time to monitor or participate in different activities (Chen, Yuan and Yu, 2010:141).

In the past decade, social networking sites have become a mainstream cultural phenomenon. Social networking has become one of the most popular activities on the web, with the top sites boasting hundreds of millions of users, and social networking sites representing 16 of the world's 100 most-visited web sites. Their popularity amongst younger generation is even higher, with studies finding more than 80% of American university students active social network users, commonly spending at least 30 minutes every day on social networks. The ubiquity of social networking in youth culture has been likened to an addiction (Bonneau & Preibusch, 2009:4).

Scholarship on social networking on world wide web is flourishing, much of it focusing on Facebook (Boyd, 2008; Cohen & Shade, 2008; Mazer, Murphy, & Simonds, 2007; Papacharissi, 2009; Sawchuk & Shade, 2010; Stern & Taylor, 2007; Tong et al., 2008;

* Prof. Dr. Uğur Yozgat, Faculy of Business Administration, Marmara University, Turkey, uguryozgat@marmara.edu.tr
** Postgraduate, Ahmet Murat Özkan, Faculty of Economics and Administrative Sciences, Cumhuriyet University, Turkey, amozkan@cumhuriyet.edu.tr
*** Ömer Faruk Oktar, Faculy of Business Administration, Marmara University, Turkey, omer.oktar@marmara.edu.tr

Walther et al., 2008, 2009). Privacy issues can be considered as a popular topic on these studies (Boyd, 2008; Lenhart & Madden, 2007; Moscardelli & Divine, 2007; O'Neil, 2001; Tyma, 2007).

Also, debates about profitability of these social networks are popular, since these networks are mostly free to join and use despite their operating costs. Recently, these debates have seen a climax with the I.P.O. of popular social network *Facebook*. Many investors, analysts and experts discussed the future of company, mostly based on revenues and profitability. Based on comments of market experts, we try to develop a simple model of money making on social networks. This model mainly relies on accurate personal data.

Social networks have also obtained a poor reputation for protecting users' privacy due to a continual flow of media stories discussing privacy problems. Popular media angles include the disclosure of embarrassing personal information to employers and universities, blackmail using photos found online, social scams, and user backlash against newly introduced features (Bonneau & Preibusch, 2009:4). We propose that, as more personal data is shared with social networks, profitability efforts will be more successful. To make this possible, social networks have to invest more on data protection technologies and act more responsibly for using private information of users.

1. Social Networking on World Wide Web

Since their introduction, social network services (SNSs) such as *MySpace*, *Facebook*, *Cyworld*, and *Bebo* have attracted millions of users, many of whom have integrated these sites into their daily practices. As of this writing, there are hundreds of SNSs, with various technological affordances, supporting a wide range of interests and practices. While their key technological features are fairly consistent, the cultures that emerge around SNSs are varied. Most sites support the maintenance of pre-existing social networks, but others help strangers connect based on shared interests, political views, or activities. Some sites cater to diverse audiences, while others attract people based on common language or shared racial, sexual, religious, or nationality-based identities. Sites also vary in the extent to which they incorporate new information and communication tools, such as mobile connectivity, blogging, and photo/video-sharing (Boyd & Ellison, 2007).

A social network service (site) can be defined as; a web-based service that allows individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site (Boyd & Ellison, 2007). Terms such as social network site, social networking services/sites are also used for this phenomenon.

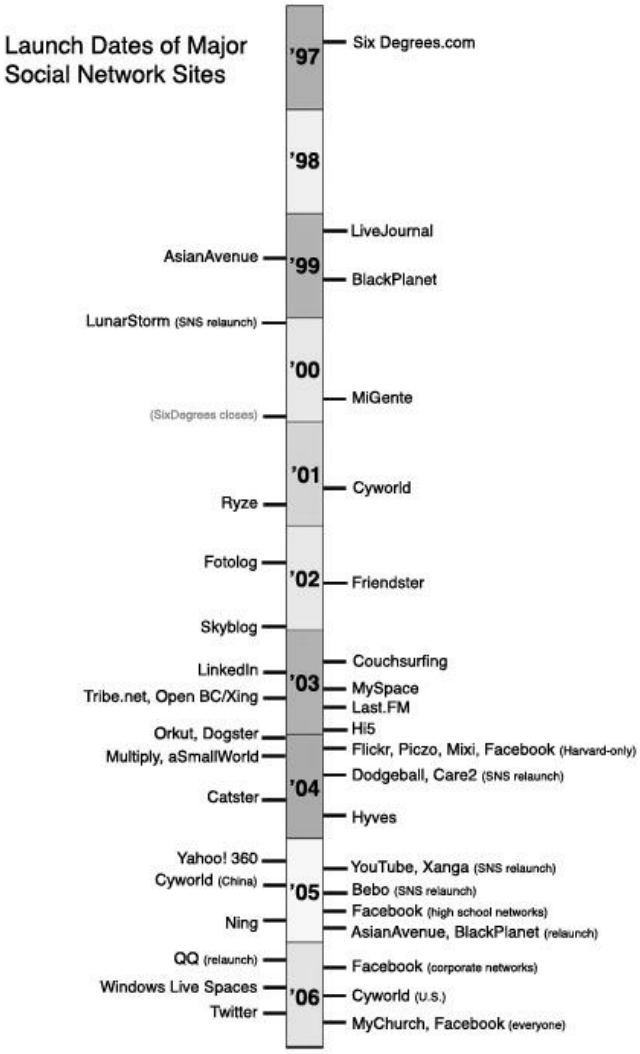
While boundaries are blurred, most online networking sites share a core of features: through the site an individual offers a "profile" - a representation of their self[ves] (and, often, of their own social networks) - to others to peruse, with the intention of contacting or being contacted by others, to meet new friends or dates (*Friendster, Orkut4*, *Facebook, myspace*), find new jobs (*LinkedIn*), receive or provide recommendations (*Tribe*), and much more (Gross & Acquisti, 2005). Members use these sites for a number of purposes. The root motivation is communication and maintaining relationships. Popular activities include updating others on activities and whereabouts, sharing photos and archiving events, getting updates on activities by friends, displaying a large social network, presenting an idealized persona, sending messages privately, and posting public testimonials (Dwyer et al., 2007).

While social networking sites share the basic purpose of online interaction and communication, specific goals and patterns of usage vary significantly across different

companies. The most common model is based on the presentation of the user's digital profile and the visualization of his/her network of relations to others - such is the case of *Friendster, Facebook etc.*.

While SNSs have implemented a wide variety of technical features, their backbone consists of visible profiles that display an articulated list of "*Friends"* who are also users of the system. Profiles are unique pages where one can "type oneself into being". After joining an SNS, an individual is asked to fill out forms containing a series of questions. The profile is generated using the answers to these questions, which typically include descriptors such as age, location, interests, and an "about me" section. Most sites also encourage users to upload a profile photo. Some sites allow users to enhance their profiles by adding multimedia content or modifying their profile's look and feel. Others, such as *Facebook*, allow users to add modules ("Applications") that enhance their profile (Boyd & Ellison, 2007).

Figure 1: A timeline of some well known social networks



Source : Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), article 11.

The public display of connections is a crucial component of social networking. Friends list contains links to each friend's profile, enabling viewers to traverse the network graph by

clicking through the friends lists. On most sites, the list of friends is visible to anyone who is permitted to view the profile, although there are exceptions. For instance, some *MySpace* users have hacked their profiles to hide the Friends display, and *LinkedIn* allows users to opt out of displaying their network (Boyd & Ellison, 2007). *Facebook* also have some tools to disable friend list publicity.

In addition to above image, we can add *Google Plus*, which was launched in 2011 with huge marketing efforts from Google. Also *Instagram* and *Pinterest*, deserve to be mentioned, which is a social network based on photo sharing from users. Instagram and Pinterest have been huge social networking phenomenons with their ability to be used with modern smartphones with well equipped cameras.

From 2003 onward, many new SNSs were launched, prompting social software analyst Clay Shirky (2003) to coin the term YASNS: "Yet Another Social Networking Service." Most took the form of profile-centric sites, trying to replicate the early success of *Friendster* or target specific demographics. While socially-organized SNSs solicit broad audiences, professional sites such as *LinkedIn, Visible Path*, and *Xing* (formerly openBC) focus on business people. "Passion-centric" SNSs like Dogster help strangers connect based on shared interests. *Care2* helps activists meet, Couchsurfing connects travelers to people with couches, and *MyChurch* joins Christian churches and their members. Furthermore, as the social media and user-generated content phenomena grew, websites focused on media sharing began implementing SNS features and becoming SNSs themselves. Examples include *Flickr* (photo sharing), *Last.FM* (music listening habits), and *YouTube* (video sharing) (Boyd & Ellison, 2007). *Facebook, Twitter* and *Google Plus* has been popular social networks during 2010's. While *Twitter* is a micro blogging service that allows 140 character messages to be posted only with a lite design, *Google Plus* and *Facebook* are more traditional social networks with customizable profile pages and friend system. *Twitter* has been a very special tool for users, allowing them to communicate briefly for a mutual goal, as seen during Arab Spring (2010–2011).

1.1. Profitability Issues of Social Network Sites and a Money Making Model

As seen above, *SixDegrees*.com; a pioneer service on social networking sites had to close down at 2000, because it failed to create a sustainable business model. A social network site, after receiving attention of public needs a lot of hardware and software investment to keep going. Hardwares are servers around the world (if global), connectivity infrastructures and other computers to keep the development ongoing. Software investments are required to ensure the security of network, network codes, web site software and development studies. Additionally, these services have to be developed by skilled and creative human resources which are expensive to hire.

Some social network sites are launched by major corporations such as Google (Orkut, Google Plus) and Microsoft (Windows Live Spaces). Others are mostly backed by venture capitals. After the launch and settlement in market, a social network service is expected to make money to survive. Below are some basic money making methods of social network sites.

Advertisements

If you open your *Facebook* profile, you will see that the right hand side of the page is full of ads. You can give the *thumbs up* to the ad or the *thumbs down*. The thumbs down will remove the ad and it will not come back (Buzzle.com). Facebook will also want to learn why you disliked the ad to provide better advertisements for you in the future. *Facebook* being a decidedly smart social networking institution knows which ad to put where. Like the *Google AdSense*, it too provides ad to the pages based on the interests and the overall profile of the

user. So, if you mention in your profile that you are a fan of Nike or any other sportswear brand, the related ads will appear on the right hand side of the page for companies and websites selling them. Facebook ads are not intrusive and hence, people do not get annoyed with them, unlike those super-irritating pop-up ads (Kulkarni, 2012). At this point, we have to add that accurate user information is important to provide the right ad to the right customer. If you like "*Nike*" official page despite being an *"Adidas"* fan, *Nike* ads on the right hand side of your profile might be meaningless. Same thing is valid for demographic info. If you tell your social network that you are 90 years old even though you are 25, you shouldn't be surprised when you see nursing home ads on your profile page.

Gifts

Ever sent a virtual gift on someone's birthday? You must have at some point, if you knew how to use *Facebook*. You do pay for some of them and a big slice of it goes into coffers of the company. While simply writing 'happy birthday' suffices for some, the 'send a gift tab' on your friend's wall encourages others to send a virtual gift - paid for online. All the money almost always goes to the company, but if the gift is provided by an outsider, then a portion of it goes there. But much of it is still retained by the website. At the cost of $1 for each gift, Facebook Virtual Gift Shop is a very lucrative business which earns the company almost $200 million every year (Kulkarni, 2012). Remember, for the gift system to work properly, data related to user birthdays, anniversaries etc. should be accurate.

Applications & Games

Many social network services are also serving as platforms for applications and games. Application topics vary; such as weather, movies, trivial informations, notepads, discussion boards, local information, news etc. Most of them are provided for free as the social network service itself and uses advertisements or facebook credits (described below) to make money. Games are also an important part of social networks, where you can compete with your friends for the high score, to have the highest level character etc. Games mostly developed under Flash technology on social network sites, can be addictive and time consuming. These games sell extra features and bonuses with facebook credits. Some of them also use advertisements on game dashboards. A social network site takes it's fair share for providing a ground for these applications and games.

Credits / Virtual Currencies

Facebook credits is the official currency in the world of *Facebook*. This virtual currency enables users to purchase items in various gaming and non-gaming applications. With $1, a user can buy 10 Facebook Credits. Of all the revenue earned through Credits, the website keeps 30% and the developers get 70% (Kulkarni, 2012). For example, US Facebook users have been enjoying a selection of Warner Bros blockbusters streamed through the site in exchange for about $4 (£2.45) in Facebook credits (BBC, 2011). Users can purchase these through their cards but the most popular purchasing option is PayPal. The Credits can also be bought as gift cards in Target, Walmart and other stores across the US. Although the amount of revenue generated by ads is highest, Facebook credits is supposed to cross that in the coming years (Kulkarni, 2012).

User Data and Trends

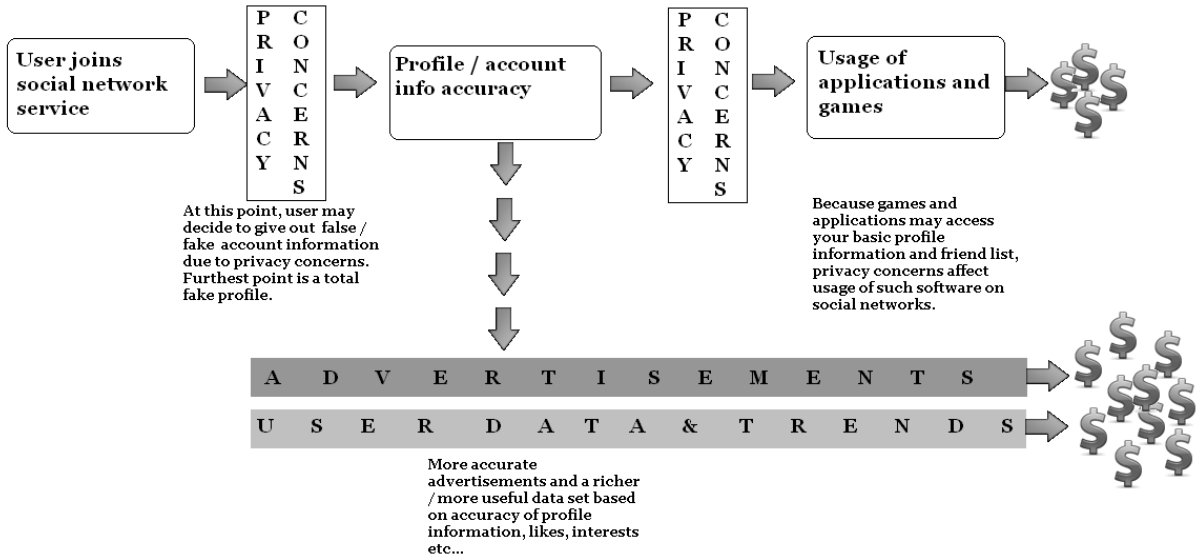
Users are usually asked to fill out a profile or account information page during signing up process to social network services. Age, gender, location, interests, profession, employer, education and similar information is collected from users by social network services. Protecting the anonymity of users, networks can sell this rich data sets to marketing agencies,

brands, governments and other corporations. This rich data set can be useful for market planning, product placement etc.

On social networks, usually there is a "shout" feature where user can say what is on his/her mind. This can be a *tweet* on *Twitter*, *status update* on *Facebook*. For example, *Twitter* licenses its complete feed - what they call "the firehose". Every message that gets sent out can be used by companies like Microsoft and Google to analyse trending topics and what people are talking about right now (BBC, 2011). Basically, every status update, every tweet can be sold by social networks, without exposing real name / account name of users. This updates may be useful for firms to learn what is trending around the world, at a certain age group, gender, profession etc.

According to Haque (2008), the idea that online social networks will make money selling eyeballs (advertising) or products is missing the entire value proposition of a social network. The real opportunity is in harnessing the rich data that is created by those participating in conversations and interacting with each other. Haque's research is based on two healthcare social networks. Both social networks commercialize their value of relationship data by aggregating and anonymizing it, and then finding third parties that benefit from, and are willing to pay for the rich data created by the community. In the case of these healthcare communities, the third parties are pharmaceuticals, insurance companies, and financial services firms. Both companies do this in a completely transparent way that is clear to users. Unlike the traditional advertising model, the conversations and interactions create the value, not the number of members.

Figure 2: Money making model of social network services



As seen on Figure 1, privacy concerns are important barriers among money making model of social networks. Because this issue is about privacy, it is important to consider what the term means (Margulis, 2003:244–246). Privacy is an elastic concept (Allen, 1988). The psychological concept subsumes a wide variety of definitions (Margulis, 1977). The psychological concept, as well as studies of everyday meanings of privacy, emphasize privacy as control over or regulation of or, more narrowly, limitations on or exemption from scrutiny, surveillance, or unwanted access (Allen, 1988; Margulis, 1977)., sharing, and analyzing large amounts of information easier than ever before''.

The less personal information is shared on social networks, the harder it will be to make money. Privacy concerns may also prevent people from signing up to social network services. Not everyone has same amount of privacy concerns on social networks. While some people just tries to protect their financial information (credit card number, bank accounts), some focuses on personal information of himself / herself and his/her close acquaintances. Others may completely stay away from social networks or use fake profiles which is full of false information, pictures etc… Part two of this study will focus on privacy issues on social networks.

2. Study Methodology

2.1. Sample

We administered the survey to 247 participants. The participants were 60.3% male and 39.7% female and their age ranges were 37.2% for 18–24 year old, 53% for 25-34 year old and 9.3% 35-49 year old. More than 60% of them have a bachelor degree (151 respondent or 61.1%), 50 of participants have a (20.2%) master's degree, 18 have (7.3%) associate's degree, 26 are(10.5%) high-school graduates. The experience of internet usage was 2% for 1–3 year range, 16.2% for 4–6 year range, 36.8% for 7–10 year range and finally 44.9% for more than 10 years. The frequency of participants' daily internet usage were 6.1% for less than one hour, 24.7% for 1–3 hours, 23.5% for 4–5 hours and 45.7% of participants use internet more than five hours daily.

Sample group can also be noted as the main limitiation of our study. Sample of participants were randomly selected with an online survey tool and our money making model is currently a simple one which needs developments through several different research processes.

2.2. Instrument Development

Individuals' concerns about privacy on social networks are measured using the scale of information privacy: measuring individuals' concerns about organizational practices scale (Smith, Milberg and Burke, 1996). The instrument used in this study is composed of 3 dimensions. The first dimension deals with unauthorized secondary use and protection against errors. Second dimension is about data collecting and finally third dimension deals with information accuracy. Each dimension of individuals' concerns about privacy on social networks were measured on a five-point Likert Scale in which -1- indicated "strongly disagree", -2- indicated "disagree", -3- indicated "neither agree nor disagree", -4- indicated "agree", -5- indicated "strongly agree".

2.3. Results and Analysis

Results of our field research can be summarised as below.

2.3.1. Factor Analysis

Exploratory factor analysis results showed that individuals' concerns about privacy on social networks items loaded on three factors. First factor refers to the "unauthorized secondary use and protection against errors" dimension, second factor consists of "data collecting items" and third factor refers to the "information accuracy" dimension.

Table 1. Factor Analysis Results for Individuals' Concerns About Social Networks Scale

Factor Name	Item	Factor Loadings	Factor Explained (%)
Unauthorized secondary use and protection against errors	C. Social networks should not use personal information for any purpose unless it has been authorized by the individuals who provided the information	.866	33.394
	I. Social networks' databases that contain personal information should be protected from unauthorized access-no matter how much it costs	.823	
	M. Social networks should never share personal information with other companies unless it has been authorized by the individuals who provided the information	.817	
	D. Social networks should devote more time and effort to preventing unauthorized access to personal information	.787	
	N. Social networks should take more steps to make sure that unauthorized people can not access personal information in their computers	.769	
	G. When people give personal information to social networks for some reason, the social networks should never use the information for any other reason	.743	
	B. All the personal information in computer databases should be double-checked for accuracy- no matter how much this costs	.540	
Data collecting	J. It bothers me to give personal information to social networks.	.847	21.591
	A. It usually bothers me when social networks ask me for personal information.	.844	
	E. When social networks ask me for personal information, I sometimes think twice before providing it.	.750	
	O. I am concerned that social networks are collecting too much personel information about me	.731	
Information accuracy	F. Social networks should take more steps to make sure that the personal information in their files is accurate	.885	16.157
	L. Social networks should devote more time and effort to verifying the accuracy of the personal information in their databases.	.816	
	H. Social networks should have better procedures to correct errors in personal information	.689	
		Total	71.141
	Kaiser-Meyer-Olkin Measure of Sampling Adequacy	.908	
	Bartlett's Test of Sphericity Approx. Chi-Square	2224.479	
	df	91	
	Sig.	.000	

Factor analysis has been carried out to determine the sub dimensions of scale used in our research. To examine the evaluation and factors of the Scale on our sample, which was developed by Smith (1996) and consists of four dimensions, we have used factor analysis method. As a result of factor analysis, it is seen that three dimensions are visible within our sample. "Errors" and "Unauthorized Secondary Use" dimensions in the original scale have been merged into one dimension. This new dimension is named as "Errors and Unauthorized

Secondary Use". The other dimensions in this study resulted as the same in original scale. The only exception is question B from "collection" dimension, which ended up in "unauthorized secondary use and protection against errors" dimension. If this question is examined, we can see that the situation described in the question is relevant to "unauthorized secondary use and protection against errors" dimension. Results of factor analysis can be seen on Table 1.

To check the compatibility of data collected for factor analysis, Kaiser-Meyer-Olkin test ve Bartlett tests have been carried out. Results of the tests are higher than %0,05 significancy level and this proves that our data is valid compatible with factor analysis.

2.3.2. Reliability Analysis

The internal reliability of the items was verified by computing the Cronbach's alpha (Ahsan et al., 2009: 126; Nunnally, 1978). Nunnally (1978) suggested that a minimum alpha of 0.6 sufficed for early stage of research. The Cronbach alpha estimated for current individuals' concerns about privacy on social networks scale is 0.904. First dimension's alpha is 0.928, data collecting dimension's alpha is 0.866 and finally information accuracy's alpha is 0.774. As the Cronbach's alpha in this study were all much higher than 0.6, the constructs were therefore deemed to have adequate reliability.

2.3.3.Descriptive Statistics

Descriptive stats for our dimensions are on Table 2.

Table 2. Descriptive Statistics of Factor Dimensions

Factor Name	Number	Mean	Std. Deviation
Unauthorized secondary use and protection against errors	247	4,5772	0,7337
Data collecting	247	4,1406	0,8887
Information accuracy	247	3,7368	1,035

2.3.4. Hypotheses Tests

To test our hypotheses SPSS 20.0 was used.

- Hypothesis 1 suggests that individuals' concerns about social networks are related to gender.
- Hypothesis 2 suggests that individuals' concerns about social networks are related to age.
- Hypothesis 3 suggests that individuals' concerns about social networks are related to experience of using internet.
- Hypotheses 4 suggests that individuals' concerns about social networks are related to education level.

Table 3. One-Sample Kolmogorov-Smirnov Test

		Unauthorized secondary use and protection against errors	**Data collecting**	**Information accuracy**
N		247	247	247
Normal Parameters[a,b]	Mean	4,5772	4,1407	3,7368
	Std. Deviation	0,73374	0,88872	1,03573
	Absolute	0,282	0,182	0,127
Most Extreme Differences	Positive	0,282	0,167	0,111
	Negative	-0,282	-0,182	-0,127
Kolmogorov-Smirnov Z		4,436	2,861	1,990
Asymp. Sig. (2-tailed)		0,000	0,000	0,001

a. Test distribution is Normal. b. Calculated from data.

To determine the available analysis for this study, our data has been checked to see if it is compatible for normal distribution. For normal distribution test, One-Sample Kolmogrov Smirnov analysis has been used. Significancy line shows that our data has a value smaller than 0,05 and is not normally distributed. For these kind of data, non-parametric tests should be used. Therefore in our study, we have used Mann-Whitney U test and Kruskal Wallis analysis to test our hypothesis.

Table 4. Mann-Whitney U Test Between Dimensions of Individuals' Concerns About Privacy on Social Networks, Based on Gender

Dimensions	Gender	N	Mean Rank	Mean	p
Unauthorized secondary use and protection against errors	Male	98	116,98	4,577212	0,199
	Female	149	128,61		
	Total	247			
Data collecting	Male	98	120,32	4,140688	0,506
	Female	149	126,42		
	Total	247			
Information accuracy	Male	98	128,72	3,736842	0,396
	Female	149	120,90		
	Total	247			

Table 4 describes individuals' concerns about privacy social networks based on gender. Highest values are on unauthorized secondary use and protection against errors, data collecting and information accuracy, respectively. Gender variable on Table 4 shows that males are more concerned about information accuracy while women are mostly concerned about unauthorized secondary use and protection against errors. But difference between these groups are statistically irrelevant because of $p>0,05$. We can say that hypothesis one is falsified.

Table 5. Kruskal Wallis Test Regarding Individuals' Concerns About Privacy on Social Networks Dimensions Based on Age

Dimensions	Age	N	Mean Rank	Chi-Square	Asymp. Sig.
Unauthorized secondary use and protection against errors	18-24	93	116,45	2,017	,365
	25-34	132	128,17		
	35-49	22	130,89		
	Total	247			
Data collecting	18-24	93	120,17	2,407	,300
	25-34	132	123,06		
	35-49	22	145,86		
	Total	247			
Information accuracy	18-24	93	122,25	,256	,880
	25-34	132	124,11		
	35-49	22	130,75		
	Total	247			

Table 5 demonstrates that, older people are more concerned about privacy on social networks. As people grow older, they get more concerned for their privacy. On the other hand, value ($p<0,05$) suggests that this differentiation based on age is statistically irrelevant and hypothesis two is falsified.

Table 6. Kruskal Wallis Test Regarding Individuals' Concerns About Privacy on Social Networks Dimensions Based on Education

Dimensions	Educational Level	N	Mean Rank	Chi-Square	Asymp. Sig.
Unauthorized secondary use and protection against errors	Elementary	2	154,75	5,125	0,275
	High School	26	95,98		
	College	18	127,19		
	Under Grad.	151	127,99		
	Post Grad.	50	124,15		
	Total	247			
Data collecting	Elementary	2	180,00	3,101	0,541
	High School	26	125,94		
	College	18	136,47		
	Under Grad.	151	119,05		
	Post Grad.	50	131,20		
	Total	247			
Information accuracy	Elementary	2	182,00	11,684	0,020
	High School	26	91,86		
	College	18	93,36		
	Under Grad.	151	128,98		
	Post Grad.	50	134,17		
	Total	247			

Table 6, which shows relationship between participants' education level and individuals' concerns about privacy on social Networks can be interpreted that, no significant relationship exists between variables and our dimensions. However, a significant relationship between information accuracy and education level has been detected. Concern levels of participants are 93,33 for high school graduates, 91,86 for college, 128,98 for undergrads and 134,17 for post graduates. Based on this data, we can postulate that as education level improves, concerns will increase. We can argue that fourth hypotheses is validated with this statistical data.

Table 7. Kruskal Wallis Test Regarding Individuals' Concerns About Privacy on Social Networks Dimensions Based on Internet Experience

Dimensions	Internet Experience	N	Mean Rank	Chi-Square	Asymp. Sig.
Unauthorized secondary use and protection against errors	1–3 Years	5	108,50	5,519	0,138
	4–6 Years	40	107,34		
	7–10 Years	91	119,26		
	More Than 10 Years	111	134,59		
	Total	247			
Data collecting	1–3 Years	5	135,20	6,402	0,094
	4–6 Years	40	109,76		
	7–10 Years	91	115,05		
	More Than 10 Years	111	135,96		
	Total	247			
Information accuracy	1–3 Years	5	176,60	4,396	0,222
	4–6 Years	40	113,11		
	7–10 Years	91	129,36		
	More Than 10 Years	111	121,16		
	Total	247			

Table 7, which shows relationship between participants' internet experience and individuals' concerns about privacy on social networks can be interpreted that, no significant relationship exists between variables and our dimensions. Since value (p) is lower than 0,05 for all dimensions, we can argue that internet experience is not related with individuals' concerns about privacy on social networks and third hypothesis is falsified.

Table 8. Kruskal Wallis Test Regarding Individuals' Concerns About Privacy on Social Networks Dimensions Based on Internet Usage

	Internet Usage (Daily)	**N**	**Mean Rank**	**Chi-Square**	**Asymp. Sig.**
Unauthorized secondary use and protection against errors	Less than 1 hour	15	100,83	1,865	0,601
	1–3 hours	61	124,77		
	4–5 hours	58	123,51		
	More than 5 hour	113	126,91		
	Total	247			
Data collecting	Less than 1 hour	15	100,10	4,073	0,254
	1–3 hours	61	136,64		
	4–5 hours	58	118,22		
	More than 5 hour	113	123,32		
	Total	247			
Information accuracy	Less than 1 hour	15	148,93	7,249	0,064
	1–3 hours	61	135,65		
	4–5 hours	58	129,32		
	More than 5 hour	113	111,67		
	Total	247			

Table 8, which shows relationship between participants' internet usage and ındividuals' concerns about privacy on social networks can be interpreted that, no significant relationship exists between variables and our dimensions. Since value (p) is lower than 0,05 for all dimensions, we can argue that internet experience is not related with individuals' concerns about privacy social networks. More internet usage does not reflect a significant change on individuals' concerns about privacy on social Networks.

Conclusion

As a result of proliferation in technology usage, it is now easier for private information to be accessed without individual consent. Accessing this kind of information is known to be unethical by almost any party involved. On the otherhand, with profit maximization goal in mind, organizations can sometimes ignore this ethical questions.

Participants has answered a questionnaire about security breaches for their personal information. They were told about social networks' (e.g. *facebook, Twitter, Linkedin*) personal information storage and their ability to make money of this. People noticing this policies and applications feel less secure with their information on social networks and modify their tendency towards sharing of personal information on social networks. As a result of the study, we can argue that unauthorized use of private information by social networks

causes discomfort and mistrust among users. We propose that, to improve money making efforts of social networks, better privacy policies should be implemented.

In this study, relationship between privacy concerns on social networks and gender, daily internet usage, age, education, internet experience has been checked, respectively. Concern factor, felt while personal information is shared consists of three dimensions. These dimensions are unauthorized secondary use and protection against errors, data collecting and information accuracy.

Our study demonstrates that there is a significant relationship between information accuracy dimension and education level. As education level rises, concerns about private information sharing on social networks rise up. Contemporary marketing approaches are increasingly adopting electronic and digital environments including social networks. At this point, whether it is ethical or not, unauthorized usage of personal information on social has raised serious question marks and caused mistrust.

On the other hand, our model stil needs developments and yet to be widely tested. Further studies may focus on advanced money making models for social networks which can take privacy concerns of users into consideration. Another suggestion for further research is testing the model on different demographic sample groups. Based on age, education, profession and lifestyle, model might provide different useful results for decision makers and can be modified for economic use.

References

Ahsan, N., Abdullah, Z., Gun Fie, D. Y. and Alam, S. S. 2009, 'A Study of Job Stress on Job Satisfaction among University Staff in Malaysia: Empirical Study', *European Journal of Social Sciences*, 8(1), pp.121–131.

Allen, A. L. 1988, 'Uneasy access: Privacy for women in a free society', Totowa, NJ: Rowman &Littlefield.

BBC. 2011, 'How can social networks make money?' Online, http://news.bbc.co.uk/2/hi/programmes/click_online/9457946.stm, Accessed on: 02.06.2012.

Becker, J. & Chen, H. 'Measuring Privacy Risk in Online Social Networks', Online, http://www.cs.ucdavis.edu/~hchen/paper/w2sp09.pdf, Accessed on:30.05.2012.

Bonneau, J. & Preibusch, S. 2009, 'The Privacy Jungle: On the Market for Data Protection in Social Networks', *WEIS The Eighth Workshop on the Economics of Information Security.*

Boyd, D. M., & Ellison, N. B. 2007, 'Social network sites: Definition, history, and scholarship', *Journal of Computer-Mediated Communication*, 13(1), article 11. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html, Accessed on: 28.05.2012.

Boyd, D. M. 2008, 'Facebook's privacy trainwreck: Exposure, invasion, and social convergence', *Convergence*, 14, pp.13 – 20.

Cohen, N. S., & Shade, L. R. (2008). 'Gendering Facebook: Privacy and commodification', *Feminist Media Studies*, 8(2), pp.210 – 214.

Dubrofsky, R.E. 2011, 'Surveillance on reality television and facebook: from authenticity to flowing data', *Communication Theory*, 21, pp.111– 129

Dwyer, C., Hiltz, S.R. & Passerini, K. 2007, 'Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace', *Proceedings of the Thirteenth Americas Conference on Information Systems*, Keystone, Colorado August 09 – 12 2007.

Gross, R. & Acquisti, A. 2005, 'Information Revelation and Privacy in Online Social Networks (The Facebook case)', Pre-proceedings version. *ACM Workshop on Privacy in the Electronic Society* (WPES).

Haque, N. 2008, '*How social networks make money… listen up Facebook*. Wikinomics', Online, http://www.wikinomics.com/blog/index.php/2008/04/29/how-social-networks-make-money-listen-up-facebook/, Accessed on: 02.06.2012

Kulkarni, A. 2012, '*How does Facebook Make Money?'* Online, http://www.buzzle.com/articles/how-does-facebook-make-money.html, Accessed on. 02.06.2012

Margulis, S. T. 1977, 'Conceptions of privacy: Current status and next steps', *Journal of Social Issues*, 33(3), pp.5–21.

Margulist, S.T. 2003, 'Privacy as a Social Issue and Behavioral Concept', *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 243–261.

Mazer, J. P., Murphy, R. E., & Simonds, C. J. 2007, 'I'll see you on ''Facebook'': The effects of computer-mediated teacher self-disclosure on student motivation', affective learning, and classroom climate. *Communication Education*, 56(1), pp.1 – 17.

Nunnallym J.C. 1978, '*Psychometric theory'*, New York: McGraw-Hill.

O'Neill, N. 2010, '*The secret to how Facebook makes money'*, Online, http://allfacebook.com/facebook-makes-money_b9896, Accessed on: 29.05.2012.

Papacharissi, Z. 2009, 'The virtual geographies of social networks: A comparative analysis of Facebook, LinkedIn and AsMallWorld', *New Media & Society*, 11(1 – 2), pp.199 – 220.

Sawchuk, K., & Shade, L. R. 2010, 'Trial by Facebook: The court of public opinion in the era of social media version 1.0', *IAMCR 2010: Communication Policy and Technology Section: Session 6: Internet, Privacy and Surveillance*.

Shirky, C. 2013, 'People on page: YASNS… Corante's Many-to-Many', Accessed on: 20.05.2012 http://many.corante.com/archives/2003/05/12/people_on_page_yasns.php

Stern, L. A., & Taylor, K. 2007, 'Social networking on Facebook', *Journal of the Communication, Speech & Theatre Association of North Dakota*, 20, pp.9 – 20.

Tong, S. T., Van Der Heide, B. 2008, 'Too much of a good thing? The relationship between number of friends and interpersonal impressions on Facebook', *Journal of Computer-Mediated Communication*, 13(3), pp.531 – 549.

Walther, J. B., Van Der Heide, B., et al. 2008, 'The role of friends' appearance and behavior on evaluations of individuals on Facebook: Are we known by the company we keep?', *Human Communication Research*, 34(1), pp.28 – 49.

Walther, J. B., Van Der Heide, B., et al. 2009, 'Self-generated versus other-generated statements and impressions in computer-mediated communication: A test of warranting theory using Facebook', *Communication Research*, 36(2), pp.229 – 253.

Yuan, M., Chen, L., Yu, P.S. 2011, 'Personalized privacy protection in social networks', *37th International Conference on Very Large Databases, August 29th - September 3rd 2011*, Seattle, Washington. Proceedings of the VLDB Endowment, Vol. 4, No. 2.