Master Thesis

-Privacy in Social Networking Sites-

Leonardos Giorgos

Student ID : MTE-1322

grleonardos@hotmail.com

Supervisors : Christos Xenakis, Christoforos Dadoyan

University of Piraeus

Department of Digital Systems

Postgraduate Programme : "Techno-economic Management & Security of Digital Systems"

Acknowledgements

I would like to thank all my professors, for the inspiration, the motivation and the guidance they gave me.

Also, i would like to thank all my classmates. Our discussions, the cooperation and the exchange of views were very beneficial for me .

Last but not least, I would like to thank my family and my friends for their support.

~ "To be left alone, is the most precious thing one can ask of the modern world" ~

Anthony Burgess

Table of Contents

Abstract

The purpose of this study is to explore the aspects of privacy over the use of social networks web sites. More specific, we will show the types of social networks, their privacy mechanisms that are different in each social network site, their privacy options that are offered to users.

We will report some serious privacy violations incidents of the most popular social networks sites such as Facebook, Twitter, LinkedIn. Also, we will report some important surveys about social networks and preferences of their users.

There is no denying that social networking has become a huge part of today's information society. SNSs(Social Networks) are almost everywhere, examples include the largest ones; Facebook, Twitter, LinkedIn, Youtube.

Driving the development of such services are often the anticipation of new features, cool tools, access to all sorts of data in all kinds of ways. People and enterprises are sharing more and more personal and sensitive data in search for social and organizational benefits or other ways to exploit these services fully. There are benefits to be reaped, but there are also negative consequences when it comes to privacy. Seeing as these services will handle vast amounts of personal and sensitive data they should have correspondingly strict access control requirements to protect the privacy of its users. When new features drive the development of these services, and there is a race for deploying them as fast as possible, privacy often suffers.

Lack of privacy in some shape might even be a requirement for a service or feature to be able to work properly. This leads to the pattern where services are deployed without much concern for privacy, and when such concerns are raised, at a later point in time, privacy will be more or less addressed. This pattern exists because the developers of SNSs do not have adequate incentives for implementing strict access and privacy control, seeing as large portions of the public seems to not understand the risks or do not care about this kind of privacy (or they might not consider it an important enough factor in the choice of whether or not to use different kinds of SNSs).

That is why one important further research area is a way to make the public understand privacy and the risks involved when sharing personal or sensitive information through SNSs. In addition to understanding the risks, the public should be able to check the privacy policies of an SNS (e.g. by using P3P plus easily understandable GUI interfaces to display a website's privacy policies in a browser). This might create incentives for the developers of SNSs to include more strict access and privacy control in their product.

Keywords :Privacy, Social Networking Sites, Privacy Violation, Privacy Preferences, Mobile Social Networks, User Privacy Settings

Introduction

When people say that "does not exist protection of private life", it is usually for two reasons: Either they believe that the secrecy is irrelevant or unfeasable in in favour-connected world today or that they do not become enough for the protection of private life, after enormous quantities of personal information go up in the internet.

Even if it could done more for the protection of private life in the internet, the protection of private life is not impossible, simply it changes form. While it is true that we share more information in the internet than ever before, it does not mean that we did not interest in protecting our privacy.

On the contrary, certain curious tendencies in the way that the users share information in the social means of networking show that we became actually always more careful. In the beginning of decade 2000, when the first social networks appeared, such as MySpace and Facebook , the users were more "open" with their personal information. Most of the users had "common" profile, in which could have access anyone, and few users cared about protecting their private life. However, as many incidents of violation of privacy happened people became more careful with sharing their private information and began to think seriously the dangers of bad management of their private life on the internet. Last years most of the users of Facebook, have become more protective with their personal elements. Also, recent researches proved that the persons take limitation more and more about the data that are shared among other users of Facebook. Despite these tendencies, the parents of adolescents today, are highly concerned to find appropriate ways so as to manage their presence in the internet.

The report of PEW in 2013, (Research centre of behaviors and tendencies), researching about the problems that concern adolescents, or social media and the private life, has shown that only 9% of total adolescents worry about the access of a third person in their data in Facebook, while the 80% of parents expressed high levels of concern for this fact. Young people share many information about their selves on a social media network and sometimes they get in troubles for this reason.

Recently, a boy, 14 - year - old, sent photograph to a girl in “snapchat”(mobile application). showing him naked. The incident had been recorded by the police. Researches also prove that 74% of adolescents had erased and 58% had had blocked other users so as to avoid sharing of information. Also 60% of adolescents maintain their profile private, 58% said that share funny or messages with some hidden way, 57% decided not to publish something in the internet, because of possible negative consequences and 26% reported false information in order to protect their private life.

Simultaneously, there are some problems about protecting privacy in social media networks that cannot be solved simply, by adapting regulations of user. At the present moment, the privacy policies of social networking offers the option, only in those who upload photos . For example, if “George” uploads his photo with John, George is the person that choose who can see the photograph. But if George does not want to be shown by his friends of John, then he has tell John and in case of denying he can to report it to the administrator of web page.

Many Studies are constantly carried out about searching thousand users of Social Media, in order to help they develop the next generation in the tools of private life and the intensification of users that is found in these scripts. The protection of personal data will continue changing in the future and the biggest challenge will be to ensure that the users have all the tools that they need in order to they keep pace with changes of life, and to protect their private life in the way they want.

1.Privacy

1.1. What is Privacy?

Alan Westin, one of the ringleaders of field, had declared that “no definition of privacy is not feasible, because the subjects of privacy are from foundations question of values, interests and power”. It becomes comprehensible, consequently, that the definitions of privacy differ depending on the sociopolitical frame and the environment in which they are fixed (Westin 1969).

Today, in a lot of countries of the world the significance of privacy is located in laws on the protection of data, placing him in the frame of management of personal information. Outside from this narrow, but important for our season frame, the protection of privacy is often translated as a way is determined how many can a society will invade in the personal aphorisms of individual. The lack of however unique definition should not foreshadow in the reader that the subject of it is minor importance (Mendel et al 2012).

As Fernando Volio Jiménez observed: “with some significance, the all human rights are aspects of right in the privacy”. The discussion that opens here has her bases in collective imaginary the ancient societies, but mainly in a concrete social-historical creation. The pre-requisite social creation that allows us to make reason for privacy, is located in the substance of property and, more specifically, in the delimitation of regions of different householder. The characteristic element of this of creation is observed for first time in the ancient Greek cities-state. Characteristically, in the Aristotle’s theory of city, is reported the segregation between the public ball of policy and activation in the private space - the house (Mendel et al 2012).

The significance of privacy is transported in the passage of centuries from the medieval British county courts up to the reason of William Pitt the Elder in 1763: “The poorest man may in his cottage bid defiance to all the forces of the crown. It may be frail –

its roof may shake- the wind may blow through it -the storm may enter, the rain may enter- but the King of England cannot enter. ” Thus, the discrimination of public/private life, that is reported in the space of exercise of governmental power and respectively in that of self-governing, is impressed in 1869 from JohnStuart Mill in the essay “Peri Eleftheria”. Certain decades later, in 1890, Brandeis and Warren in their meaning article “The Right to Privacy” used the phrase “the right to be left alone” (“the right you remain alone”), in order to they describe the right in the privacy of individual. Stimulus for the writing of article was the continuously more frequent appearance of incidents of public - printed distribution of details relative with the personal life of individuals (cf. celebrities of season), because the appearance of portable photographic machines. This phenomenon led the authors to the perception that the significance of privacy concerns the protection of private discussions, the expression of thoughts and sentiments. (Moreham 2008).

The optics, however, by which was approached the institution of right in the privacy was different. For their Brandeis and Warren the right in the privacy should not instituted as countermeasure for the protection individual (intellectual or not) property, but have been supposed it is based on the more general right of immunity of person or, differently, on the «right of personality of individual”. They expressed, consequently, the opinion that the beginning of protection of privacy, was already part of customary right, but because the developments of technology of season was important her explicit and exclusive statements “right in the privacy”.

Thus, they lead to defend the privacy as one from the more important freedoms in a democracy and to propose her explicit expression in the American Constitution. The proposals of Brandeis and Warren, were expressed finally in fourth revision (4thAmendment) the American Constitution, which prohibits the not-permit researches at home and upgrades him in interrogative action. The revision was judged satisfactory for the recognition of right in the private life and was used as means for the legal extension of right few years later at the institution of secrecy of communications. In the configuration of significance of privacy, they have offered occasionally scientists from different fields. Ruth Gavison recognizes three sovereign elements in the nature of privacy: the secrecy (secrecy), the anonymity (anonymity) and the loneliness (solitude), underlining that it is a fluid situation which, depending on the choices of each individual, can be lost (Mendel et al 2012).

Edward Bloustein judges the right of privacy asessential condition for the human dignity, while other commentators, as James Rachels, as necessary for the growth of diversity and meaning in the human interpersonal relations. Certain students are defended the right in the privacy as the means with which we can check the ways addressed to third in our person or as means of personal expression and choice. According to report of committee of United Kingdom under David Calcutt, that opined about the behavior of press concerning the personal life (report of the committee on privacy and related matters), it cannot "[…] was found completely satisfactory legislated definition for the privacy", however, was adopted the following definition: "The right of individual be protected adverse the invasion in his personal life or his affairs, or those of his family with immediately natural means or with publication of information". Lawrence Lessig, known academic and political activist for the human rights in the Society of Information, reports "that most persons today with the significance of privacy mean the right of choice of notification of their personal information in third person". The himself points out that the privacy is based on four decisive factors: law (law), the market (market), (social) habits (norms) and the architecture (architectures) systems (social/technological) (Moreham 2008).

Finally, a modern opinion of definition gives Robert Ellis Smith, author of newspaper Privacy Journal, horizon the privacy as "the wish of each one us for a natural space in which we are free each interruption, invasion, embarrassment or responsibility" as well as "the effort to check per year also the way of notifications of personal information on ourselves".

1.2. Aspects of Privacy

Generally, the aspects of privacy, as they are met in the report of Electronic Privacy Information Center (EPIC) and Privacy International:

• **Informational privacy**: It includes the establishment of rules that conditions the collection and the treatment of data of personal character, as financier information, medical and governmental files. Is this aspect that we call and “protection(personal) given”

• **Physical privacy** : which concerns the protection of natural self of persons against interventional processes, as genetic and pharmaceutical controls or bodily gropingly

• **Telecommunications privacy**: which covers the safety and the privacy of correspondence, telephone communications, e-mail and other communication forms

• **Territorial privacy** : that concerns the delimitation of private spaces, but also spaces as the environment of work or the public ball. The follow-up via circuits of television (CCTV) and the verifications of elements, are questions hat concern the territorial privacy. A relative form of privacy, that acquires meaning today with the development of Technologies of Information technology and Communications(ICT), concerns in the locality of individual (Ghiglieri 2012).

• **Locational privacy** ("location privacy") refers to the the ability of an individual to move in public space with the reasonable expectation that their location will not be systematically and secretly recorded for later use. For instance, naive implementations of automated tolling, congestion pricing, and automated traffic enforcement violate locational privacy --- they inadvertently create a pervasive surveillance infrastructure that cheaply and silently aggregates tremendous amounts of data about drivers' locations. Data that could be used for all sorts of unpleasant applications, later. Modern cryptographic protocols allow us to build systems which both satisfy the needs of the tolling agencies and/or law enforcement but also respect locational privacy (Ghiglieri 2012).

2.Social Networks

2.1.What is a social Network?

A social networking website is an online platform that allows users to create a public profile and interact with other users on the website. Social networking websites usually have a new user input a list of people with whom they share a connection and then allow the people on the list to confirm or deny the connection. After connections are established, the new user can search the networks of his connections to make more connections. A social networking site may also be known as a social website or a social networking website (Boyd & Ellison 2007).

Social networking sites have different rules for establishing connections, but they often allow users to view the connections of a confirmed connection and even suggest further connections based on a person's established network. Some social networking websites like LinkedIn are used for establishing professional connections, while sites like Facebook straddle the line between private and professional. There are also many networks that are built for a specific user base, such as cultural or political groups within a given area or even traders in financial markets Social networking websites are easy to confuse with social media sites. A social networking site is any site that has a public or semi-public profile page, including dating sites, fan sites and so on. A social media site has profiles and connections, combined with the tools to easily share online content of all types (Boyd & Ellison 2007).

2.2. Types of social network sites

The increasing sophistication of information technology with its capacity to collect, analyse and disseminate information is posing significant threats to social networks users privacy. It is argued that the changes and the impacts of information technology are big and accelerating so quickly. Privacy issues are totally concern users about potential invasions all over the Internet world.

There many categories of social network sites where users like to register. Photo sharing between profiles, ambient location sites, uploading of videos sites, sites that can locate our GPS position, blogs discussions, forums. All these activities are exposed to the danger of privacy violation. Many social networks can be broken up into many categories and most networks fall into more than one category. Here are some statistics, so as to understand the size of danger: (“thesocialskinny”, 2016)

- Every minute of the day: 100,000 tweets are sent
- 684,478 pieces of content are shared on Facebook
- 2 million search queries are made on Google
- 48 hours of video are uploaded to YouTube
- 47,000 apps are downloaded from the App Store
- 3,600 photos are shared on Instagram
- 571 websites are created $272,000 is spent by consumers online (“AllTwitter”, 2016).

In case we should categorized them, below are the seven major Categories :

- **Social Connections**

Keeping in touch with friends and family members is one of the greatest benefits of social networking.

- **Multimedia Sharing**

Social networking makes it easy to share video and photography content online.

- **Professional**

Professional social networks are designed to provide opportunities for career-related growth. Some of these types of networks provide a general forum for professionals to connect, while others are focused on specific occupations or interests.

- **Informational**

Informational communities are made up of people seeking answers to everyday problems. For example, when you are thinking about starting a home improvement project or want to learn how to go green at home, you may perform a web search and discover countless blogs, websites, and forums filled with people who are looking for the same kind of information.

- **Educational**

Educational networks are where many students go in order to collaborate with other students on academic projects, to conduct research for school, or to interact with professors and teachers via blogs and classroom forums. Educational social networks are becoming extremely popular within the educational system today.

- **Hobbies**

One of the most popular reasons many people use the Internet is to conduct research on their favorite projects or topics of interest related to personal hobbies. When people find a website based on their favorite hobby, they discover a whole community of people from around the world who share the same passion for those interests. This is what lies at the heart of what makes social networks work, and this is why social networks that are focused on hobbies are some of the most popular.

- **Academic**

Academic researchers who want to share their research and review results achieved by colleagues may find academic-specific social networking to be quite valuable.

(http://socialnetworking.lovetoknow.com/What_Types_of_Social_Networks_Exist)

2.3. Popular Social Network websites

The most popular Social Network websites are:

1. **Twitter:** Perhaps the simplest of all social media platforms, Twitter also just happens to be one of the most fun and interesting. Messages are limited to 140 characters or less, but that’s more than enough to post a link, share an image, or even trade thoughts with your favorite celebrity or influencer. Twitter’s interface is easy to learn and use, and setting up a new profile only takes minutes (“Socialmediatoday”, 2015).

2. **Facebook**: Considered to be synonymous with "social media" by some, Facebook is the one site where you're likely to find friends, colleagues, and relatives all floating around. Although Facebook is mainly centered around sharing photos, links, and quick thoughts of a personal nature, individuals can also show their support to brands or organizations by becoming fans.

3. LinkedIn. One of the only mainstream social media sites that's actually geared towards business, LinkedIn is to cyberspace what networking groups once were to local business communities. It's great for meeting customers, getting in touch with vendors, recruiting new employees, and keeping up with the latest in business or industry news.

4. Xing. Another professional networking and recruitment site, Xing has the global presence and focus that LinkedIn lacks. Although it can be mistaken for a job search portal, the site actually has a number of features and communities that make it easy to develop relationships with suppliers, colleagues and even thought leaders within industry.

5. Renren. Literally translating into "everyone's website," Renren is China's largest social platform. Hugely popular with the younger crowd, it works in a way similar to Facebook, allowing users to share quick thoughts, update their moods, connect with others, and add posts or ideas to a blog-like stream.

6. Google+. Social media's big up-and-comer has really arrived over the past few years. By combining the best of Facebook and Twitter into one site – and backing it by the power of the world's largest search engine, Google has given users a social site that has a little something for everyone.

7. YouTube. As a video sharing service, YouTube has become so popular that its catalog of billions and billions of videos has become known as "the world's second-largest search engine" in some circles. The site has everything from first-person product reviews to promotional clips and “how-two” instruction on virtually any topic or discipline. Users have the ability to share, rate, and comment on what they see.

8. Instagram. A quick and convenient connection between the camera feature on your smart phone and all social profiles, then Instagram is the answer. Not only will allow to user to share via Twitter, Facebook, and the Instagram website, but someone can choose from a variety of photo filters and invite friends to comment on his photos or ideas (“Socialmediatoday” 2015).

9. Foursquare. Started in 2009 , Foursquare has had a long running perception being a fun mobile app to use when checking in to a physical location. It gives to users the ability to unlock badges as check-ins occur and the potential to become Mayor of a venue. However this barely scratches the surface, there is much more to this location-based social network.

Foursquare has quietly been streamlining its focus towards proactively recommending where people can go in a given location rather than detailing the experience after the fact. This shift in focus has become a valuable reason for businesses to establish a presence as potential customers seek a real time reason to check in and check out what’s on offer (“Statista”, 2015).

The statistics about foursquare are the following :

- It is a community of over 30 million people worldwide.
- Over 3 billion check-ins, with millions more every day
- Over a million businesses currently using Foursquare

2.4. Statistics use of popular Social Networks

It is important to observe some statistics about the total number of users of certain social networks websites (“Statista”, 2015).

Facebook

The statistics below shows a timeline with the worldwide number of monthly active Facebook users from 2008 to 2015. As of the fourth quarter of 2015, Facebook had 1.59 billion monthly active users. In the third quarter of 2012, the number of active Facebook users had surpassed 1 billion. Active users are those which have logged in to Facebook during the last 30 days. Furthermore, as of that quarter the social network had 1.31 billion mobile MAU. The platform is also the most popular social network worldwide.

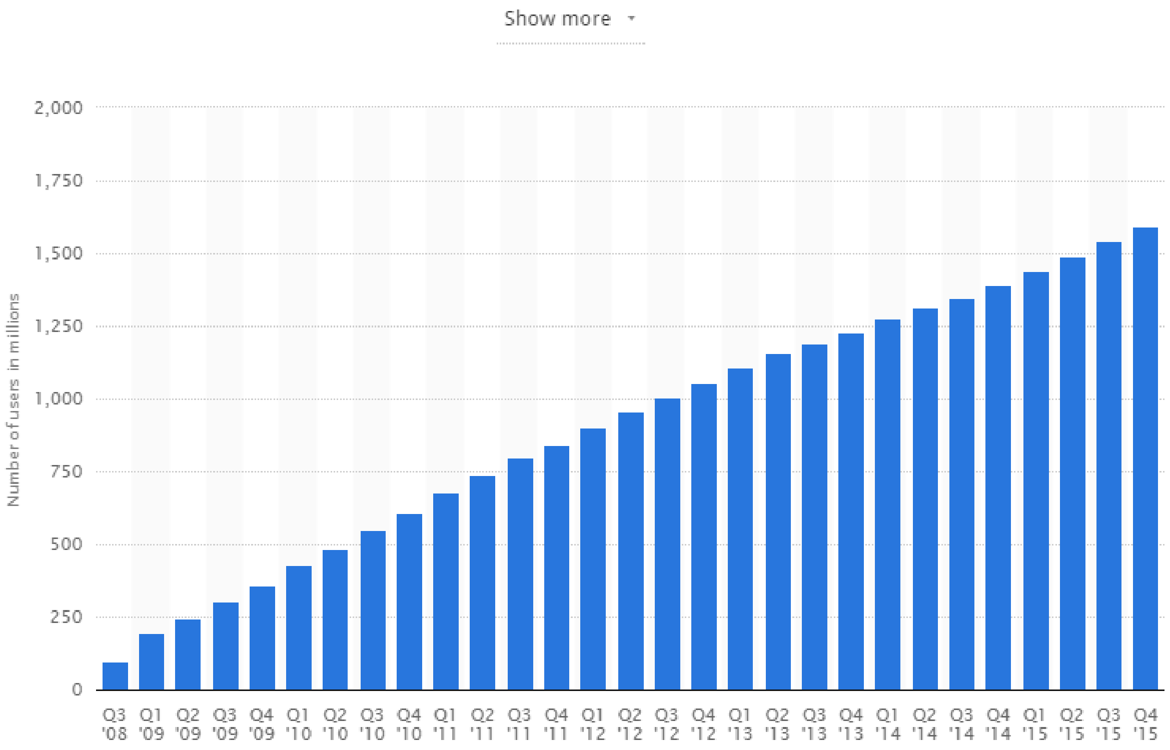


Table 1 – number of users “Facebook”

Twitter

This statistic below shows a timeline with the amount of monthly active Twitter users worldwide. As of the fourth quarter of 2015, the microblogging service averaged at 305 million monthly active users. At the beginning of the 2015, Twitter had surpassed 302 MAU per quarter (“Statista”, 2015).

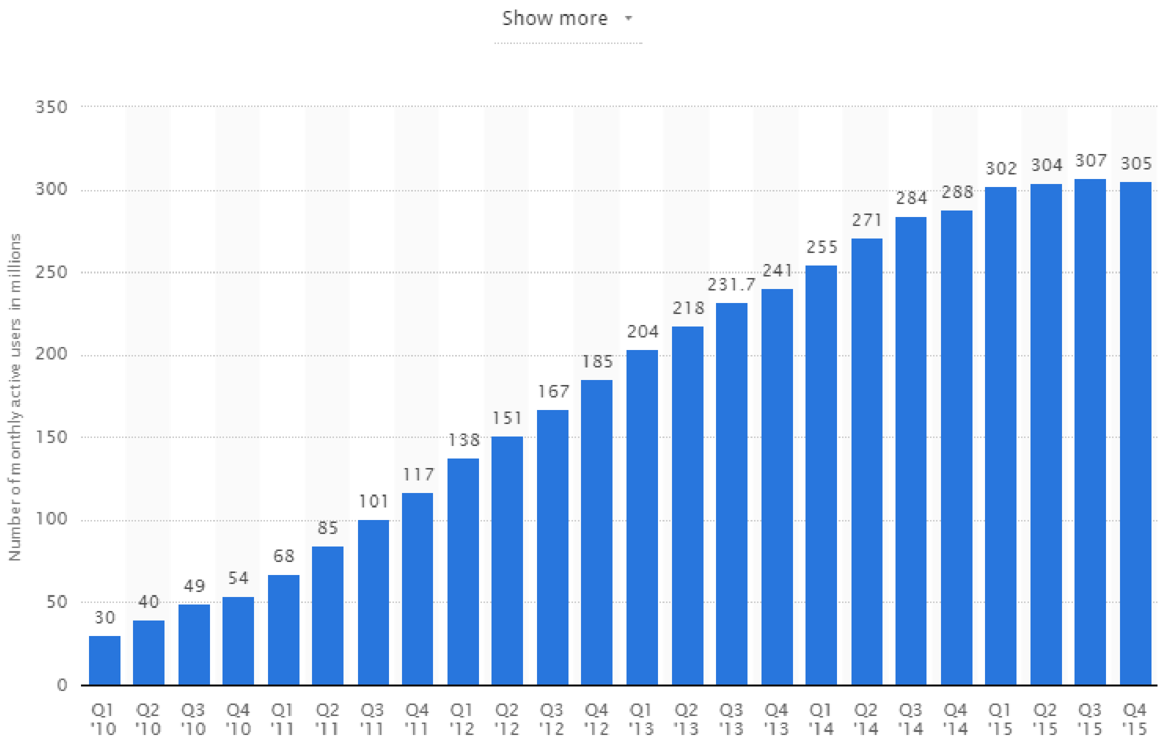


Table 2 – number of users “Twitter”

Instagram

This statistic gives information on the number of monthly active Instagram users as of December 2014. As of that month, the mainly mobile photo sharing network had reach 300 million monthly active users, up from 200 million in March 2014. The app is one of the most popular social networks worldwide (“Statista”, 2015).

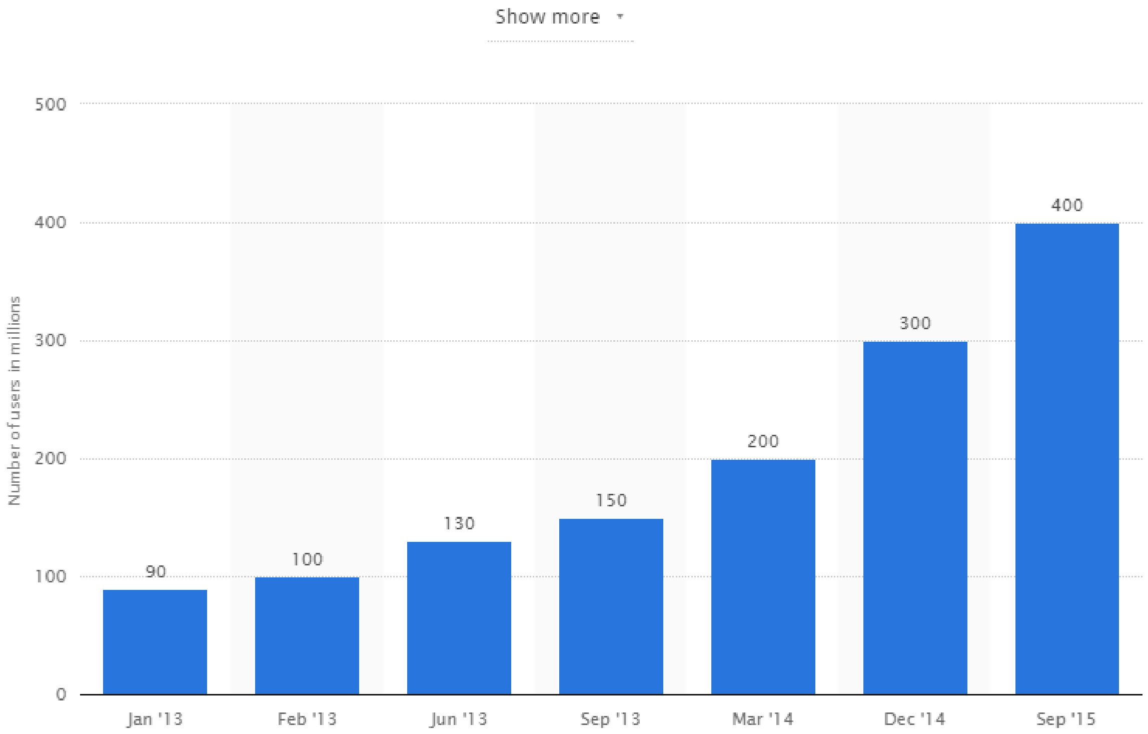


Table 3 – number of users “Instagram”

RenRen(china's biggest Social Network Site)

The graph shows monthly Renren.com user numbers in China from 2009 to 2014. By the end of December 2012, about 56 million unique users had logged on to the Renren.com platform.

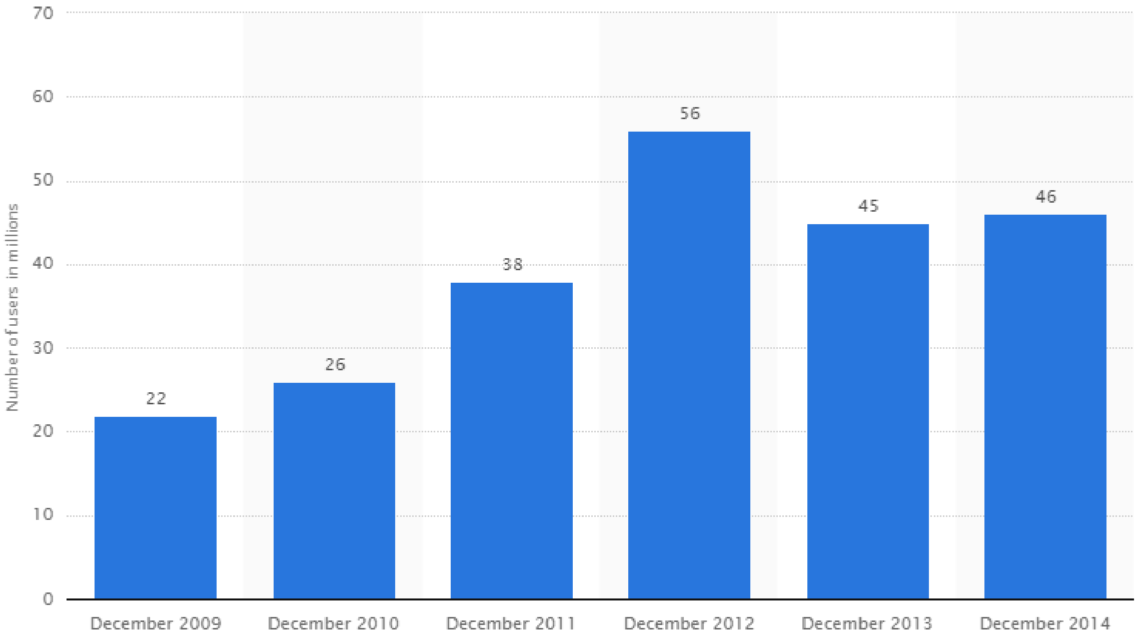


Table 4 – number of users "RenRen"

2.5. Social Networking and Privacy

This increased use of social network sites has led to increased concerns about users' privacy not only in terms of the data collected and used by the organization but also in light of the possible impact of mass sharing of personal information on social relations (Houghton & Joinson 2010).

Privacy and security

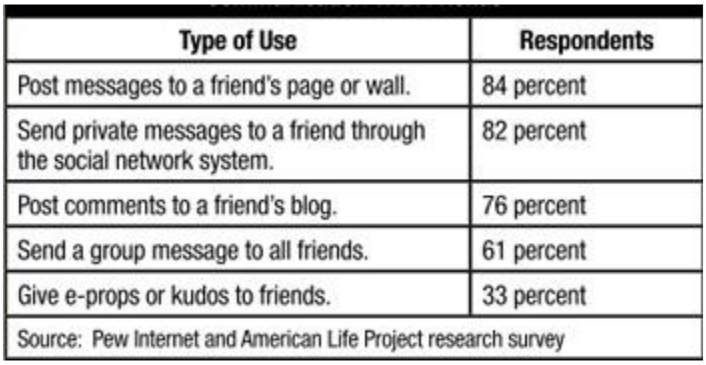
The idea of privacy in general dictates that no one should be able to observe things about a person without person’s permission. As for social networks, privacy is greatly ignored unwittingly. Many people perceive that rejecting a request to be your friend based on one of your other friends’ recommendations might be considered rude. It is important to recognize that friendships are dynamic (Badger 2011).

For example, A typical scenario in Facebook could be that a friend posts “Five Things About Me” and encourages the recipient to do the same. In response to this suggestion from a friend, the posting by the recipient states, “I attended Valley High,” and, “My cat’s name is Myra.” It is likely that the user has chosen these two answers as his/her challenge response for an online bank account. This simple scenario points to the vulnerability of exposing personal information unwittingly (Kirkpatrick 2010).

One type of serious privacy violation that occurs in social networks involves photos. A conscientious user might have placed appropriate controls on his/her settings concerning the ability to view photos posted on his/her wall. When a friend posts a photo on his/her wall without putting it in context and invites all mutual friends to view the photos, it could jeopardize the carefully crafted privacy settings of the first user. This kind of privacy violation is all too common in social networks. A similar experience was also discussed by Dwyer about a teacher feeling awkward after her students befriended her and posted some pictures. Another source of privacy violations on Facebook involves third-party applications. Users constantly subscribe to new and popular applications. Such applications find acceptance because they are referred by friends. Consider the following scenario in which the user has violated his/her own carefully crafted privacy settings: User downloads a phone app which finds t-he answer to the question, “Which 1970s movie reflects you?” Before this app is launched, the user is informed that in order to find the answer to the question the app needs access to the user’s profile and that of his/her friends. A whole host of privacy settings have been violated by the simple use of this one app. In the world of social networks, such apps are prevalent. Aaron Beach, Mike Gartrell and Richard Han have studied the role of applications in violating user privacy, thereby reinforcing the statement that applications have a way of bypassing some of the security controls (Badger 2011).

The ease of use in social networks significantly contributes to many privacy violations. Another example concerning Twitter is the following: two users participating in the update-and-reply feature of a Twitter conversation are unwittingly sharing their conversations with their friends unless they took specific steps to block the feeds. Twitter feeds are brief but contribute to some major privacy violations. A large corporation that allows the use of Twitter by employees could face a serious threat. An employee might tweet to one of his close confidants that a new system developed by the organization has a serious bug. Unfortunately, Twitter feeds are followed by many, and so a confidential organizational problem is now exposed. This example shows that privacy violations need not be at the individual level.

According to a 2011 research survey, social networks provide “a concentrated posse of easily contactable friends.” Given the large number of friends to communicate with on social networks, many use the networks in a variety of ways. The research survey results appear in figure below (Chen 2008).



Type of Use	Respondents
Post messages to a friend's page or wall.	84 percent
Send private messages to a friend through the social network system.	82 percent
Post comments to a friend's blog.	76 percent
Send a group message to all friends.	61 percent
Give e-props or kudos to friends.	33 percent

Source: Pew Internet and American Life Project research survey

Table 4 – user preferences

These statistics show how information gets posted and communicated among friends through social networks without much filtering. Potential users must be aware that what is posted on social networks will find its way to a very large audience quickly, so any information that could expose one's privacy should be guarded.

The benefits of social networks extend not only to individuals, but also businesses. In a survey of 72 business managers conducted at Texas A&M International University regarding the perception of the use of social networks in business, the respondents were skeptical of new technologies. However, they recognized that the introduction of both the Internet and email had significant benefits to business. With this experience, the analysis of the data shows that managers perceived that the use of social networks in business builds:

- Employee morale
- Satisfaction
- Commitment
- Enhanced performance

The survey showed that some managers perceived that allowing the use of social networks at work is essential because their competition allows it. This line of reasoning should be tempered by the fact that every business should assess its business goals in light of what technology has to offer.

Social networks realize the importance of security and provide some tools to protect the information. However, the overwhelming goal is ease of use and rapid dissemination of information. It is clear from various statistics on the use of social networks that younger people use it extensively. The prior comment concerning the goals of social networks comes as a result of this observation as well as the fact that older adults also use social networks for ease of use and rapid communication capabilities. These aspects pose an inherent security problem in social networks (Badger 2011).

A typical Facebook user's preferred device of choice is the cell phone. Even though setting a user ID and password are options from a cell phone, virtually all users ignore this aspect for the sake of convenience. Given this fact, if the cell phone is misplaced or lost, then anyone obtaining the device will have access to the Facebook account of the user. Someone with a criminal intent could post a damaging or misleading message.

A new security threat is emerging in social networks because of location tracking. Facebook has a feature called "check-in," which lets friends know one's GPS location. Since one's circle of friends sometimes gets very large simply by transference of friends, one must monitor one's privacy settings closely.

The login notification on Facebook is similar to Skype. Friends are notified when a user logs into their Facebook account. Facebook and other social networks let members link up to their account in other popular sites such as YouTube. Even though this feature allows for the setting up of user ID and password, many users simply ignore this security feature. Thus, a user logged into one social network potentially exposes all their other accounts as well (Badger 2011).

On Facebook, the update feature is a major security vulnerability. An innocuous message such as, "I am looking forward to my vacation in Europe next month," gets forwarded to a large circle of friends. Since some of the friends are basically acquaintances, the user has essentially broadcast a message that they are not going to be home, thereby creating an opportunity for someone to rob them. These simple instances illustrate the security threats widely prevalent in social networks.

3. Historical Analysis – Privacy Violations with big impact

The year of 2010 was a year full of violation of privacy rights. While a growing number of people and companies seem to be concerned about the issue of protecting the most intimate details of our lives, technology is making it harder and harder to do so. Whether it be something as innocent as Google "accidentally" collecting 600 gigabytes of unsecured private data while driving cars around the country in search of wifi networks, or something as sinister as tracking company RapLeaf using sophisticated technology to create incredibly detailed profiles of people (including names, email addresses, shopping habits, voting history, and so on) and then selling that data to advertisers; this has been a year full of headlines about privacy violations (“Top 5 Privacy Violations”, 2010).

3.1. Incidents of privacy violations of popular Social Network Sites

Foursquare — It is a very popular social networking tool that allows users to “check-in” and let their friends know where they are at any given moment ran into a real embarrassment in June. A programmer in San Francisco by the name of Jesper Anderson figured out that he could write a program to keep track of where Foursquare users were going by examining the pictures that Foursquare publishes every time someone checks-in at a location. He captured close to a million check-ins in just a couple weeks. This means that this simple program knew where thousands of Foursquare users were going at any given moment of the day. The program was able to know if they were out shopping, at home hanging out, at work, or just about anything else. This program was even able to get around Foursquare’s privacy settings that were supposed to only allow “friends” to know when someone was checking-in. It was a bit like he had a GPS on each Foursquare user in the San Francisco area. Foursquare was able to fix the bug and now has a setting that keeps your location private from outsiders.

Facebook has Changed Everyone’s Privacy Settings. In April of 2010, Facebook made many changes about its privacy settings and on every user’s account was set by default so as to make almost nothing private. As a result, unless someone change settings, details like birthday, gender, place of birth, religious beliefs, friends, family members, schools attended, and other intimate details would be available to anyone who wanted them. It was a terrifying decision to leak information from the organization that so many of us have trusted with the story of our lives, our likes, and so much more. Facebook quickly backpedaled and forced all users to choose their privacy settings, but the damage had already been done. Facebook, already with a sketchy reputation, soon became known as one of the worst privacy abusers.

LinkedIn Faces Lawsuit Over Privacy Violation

A federal district judge has ordered LinkedIn to face a lawsuit that alleges the social network violated user privacy by accessing their external email accounts and downloading their contacts' addresses.

The complaint was filed in September 2013 by four LinkedIn users seeking class-action status and accused the company of impersonating them in order to obtain access to their email contacts. The plaintiffs said that LinkedIn sends multiple emails endorsing its products, services, and brand to potential new users whose email addresses LinkedIn "surreptitiously obtained" as part of its effort to acquire potential new users, according to the complaint. They also claimed that the professional social network sends additional emails to those email addresses when those users don't sign up for a LinkedIn account. US District Judge Lucy Koh found that while LinkedIn users did consent to the company sending an initial email to attempt to recruit from their contacts, they did not consent to LinkedIn sending additional reminder emails (“LinkedIn Faces Lawsuit Over Privacy Violation”, 2014).

4. Privacy on Social Networking Sites

Privacy problems associated with digital communication and network technologies have been a major concern among Internet users over the past decade.

The emergence of social networks has even increased these concerns. People register to these SNSs and share images, videos, and thoughts because they perceive a great payoff in terms of friendship, jobs, and other opportunities . The popularity of SNSs attracts not only faithful users but third parties with adverse interest . If we consider the huge amount of private information uploaded to those SNSs and the persistence of it in the social networks, the privacy of SNS users can be threatened . Recent cases show that on-line thieves, stalkers, and bullies take advantage of the information available on SNSs and use it for purposes that were not the initially intended ones (Yao et al 2007).

Facebook Apps

The popular social media site has been plagued by privacy issues over the years. Its highest-profile problem was in October 2010, when Facebook admitted that its top 10 most popular applications including FarmVille and Texas Hold`em shared user data, including names and friends' names, with advertisers. A Wall Street Journal investigation uncovered the Facebook privacy breach and said it affected tens of millions of users, including some that had used Facebook's most stringent privacy settings. Facebook had previously been in trouble for transmitting user ID numbers to advertising companies when users clicked on ads. In November 2011, Facebook settled a case with the U.S. Federal Trade Commission about several incidents and agreed to 20 years of third-party privacy audits

Statistical use of social media networks

The success of social media networks growth is due to supported activities of society and the current researches shows that it there is no doubt of continuation and existence of social networks.

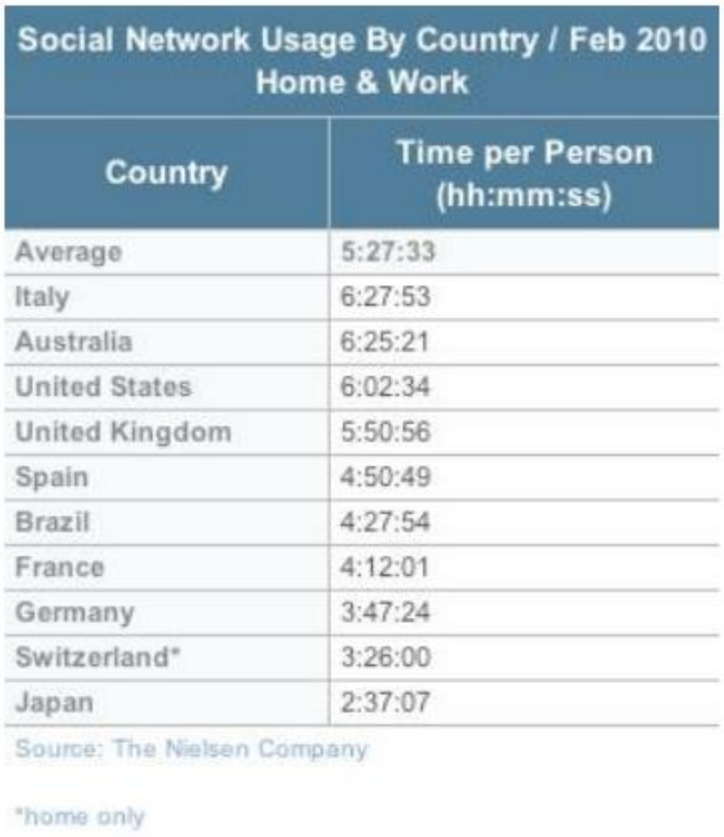
The rates of use are impressive. There are many companies that have made researches for example “Nielsen”. According to this research , in February 2010 each user spent roughly 5.5-hour per month in the web pages of social networking. Facebook is for sure, one from these web pages. Compared 2010 to year 2009, there is an increase of 2 hours in surfing on social networks sites.. This company has made this research in 10 countries worldwide.

In this research, it is remarkable that Facebook is out of comparison cause it has almost one billion users. It possesses the first place worldwide and it is calculated that each user – at mean spends six hours (5:52: 00) per month and makes more than 19 connections per month.

Users of Facebook are connected 5-hour more than users of MySpace. MySpace is second in classification and the user of this website finds in the network roughly one hour (0:59: 33) per month.

In USA the active users in these social networks was increased at 29%, from 115 millions in February 2009 to 149 millions in February 2010.Worldwide, the active public in this networks was increased roughly 30%, that is to say increase by 244,2 millions in 314,5 millions.

Below, is given the table, in which was recorded the monthly use of users in web pages of social networking in various countries. First place possesses Italy, with monthly use roughly 6:27: 33.



Social Network Usage By Country / Feb 2010 Home & Work	
Country	Time per Person (hh:mm:ss)
Average	5:27:33
Italy	6:27:53
Australia	6:25:21
United States	6:02:34
United Kingdom	5:50:56
Spain	4:50:49
Brazil	4:27:54
France	4:12:01
Germany	3:47:24
Switzerland*	3:26:00
Japan	2:37:07

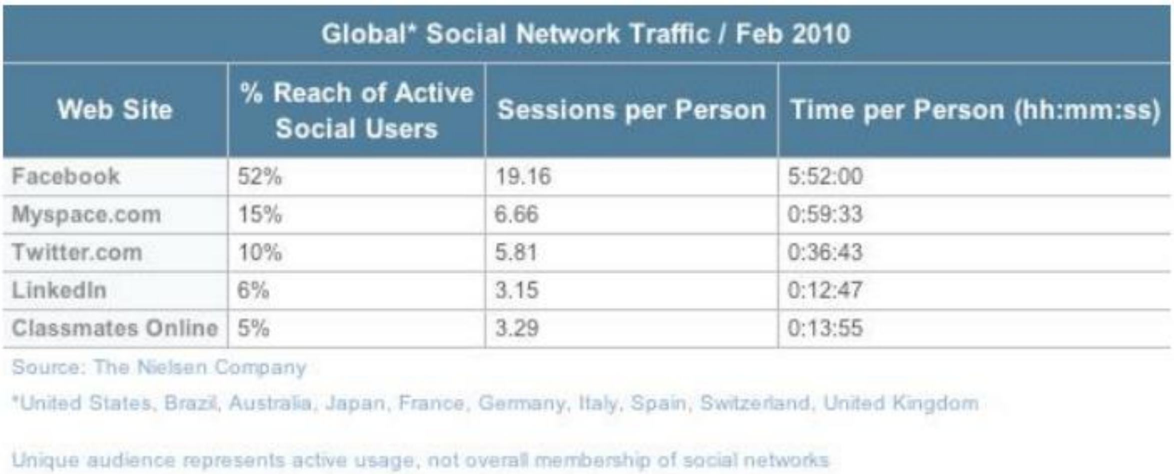
Source: The Nielsen Company

*home only

Table 5- Monthly use of social media networks (total hours)

(source : http://blog.nielsen.com nielsenwire)

The table above shows that Facebook is in the first place of use in total hours per month



Global* Social Network Traffic / Feb 2010			
Web Site	% Reach of Active Social Users	Sessions per Person	Time per Person (hh:mm:ss)
Facebook	52%	19.16	5:52:00
Myspace.com	15%	6.66	0:59:33
Twitter.com	10%	5.81	0:36:43
LinkedIn	6%	3.15	0:12:47
Classmates Online	5%	3.29	0:13:55

Source: The Nielsen Company

*United States, Brazil, Australia, Japan, France, Germany, Italy, Spain, Switzerland, United Kingdom

Unique audience represents active usage, not overall membership of social networks

Table 6 - use of social media websites

(source : http://blog.nielsen.com nielsenwire)

In February of 2010 other companies such as Hitwise, Nielsen, Comscore, Forrester, Royal, Pingdom, made researches that prove the results above:

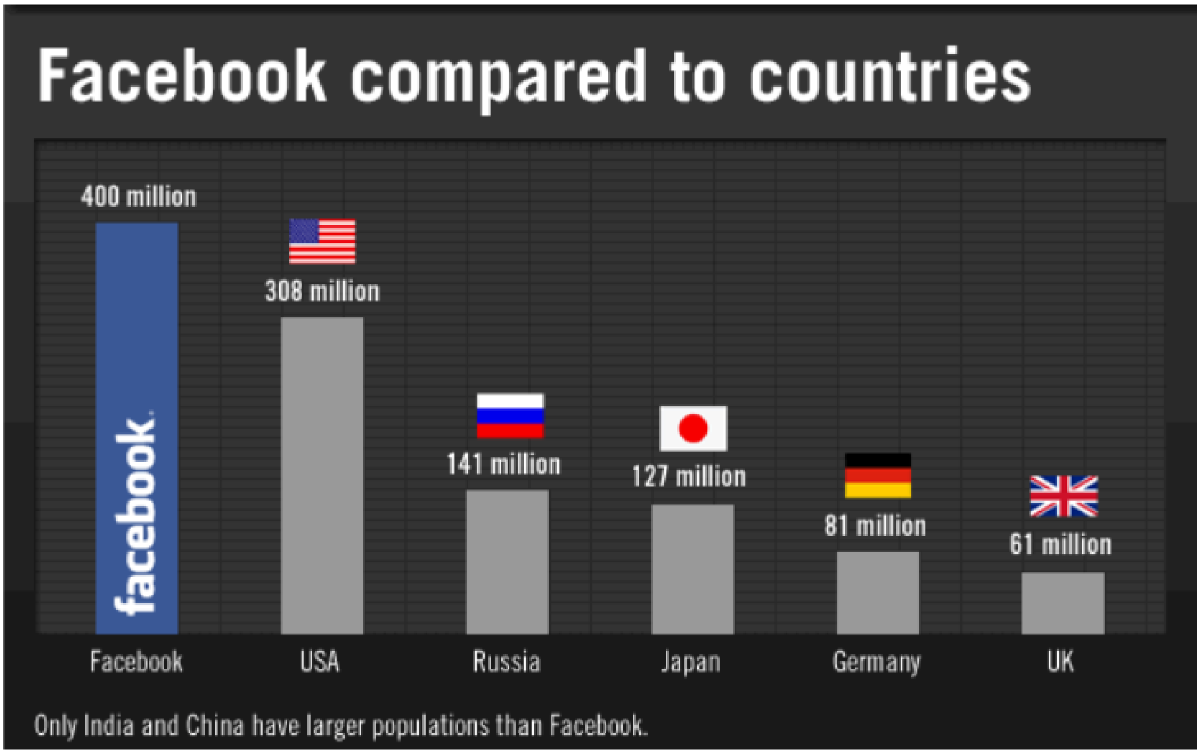


Table 7 : use of Facebook per Country

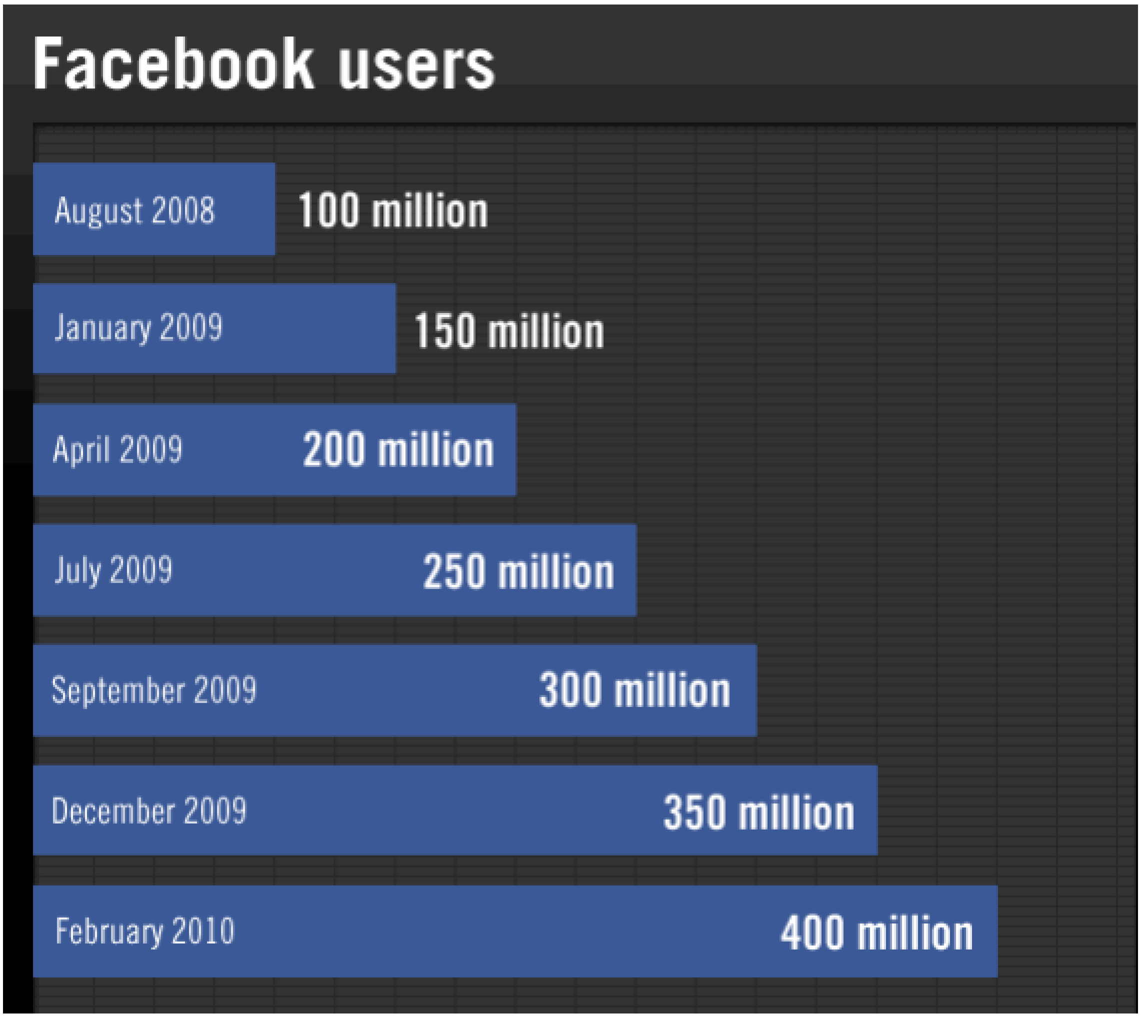
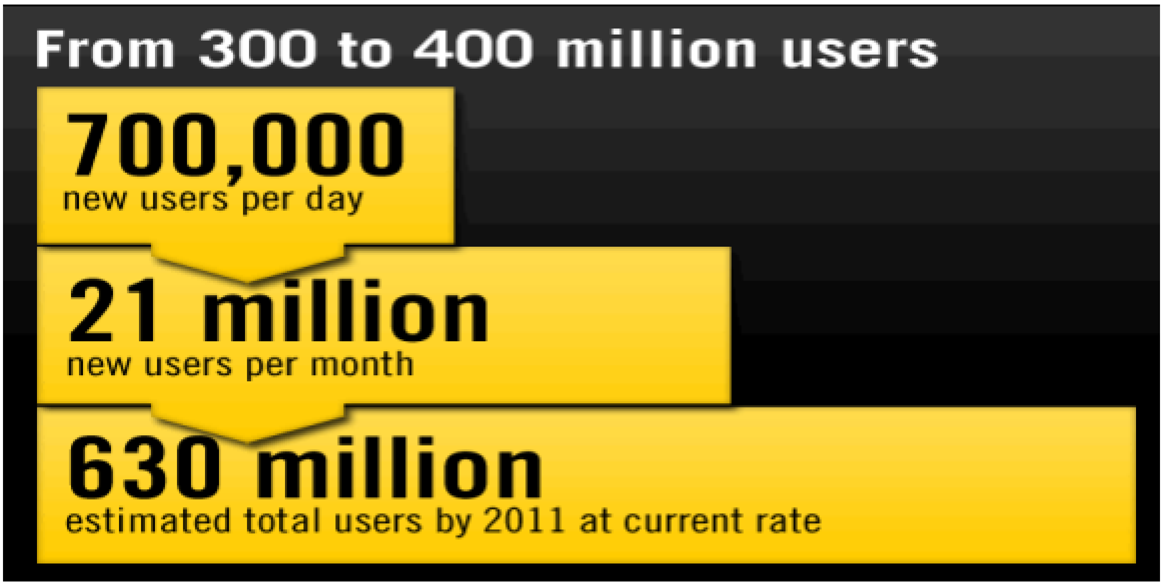


Table 8 : use of Facebook per Month



From 300 to 400 million users

700,000 new users per day

21 million new users per month

630 million estimated total users by 2011 at current rate

Table 9 : use of Facebook

(source : http://www.hitwise.com/uk/)

4.1.Privacy mechanisms on SNS

Privacy and Social Networks As pointed out more than a century ago by Warren and Brandeis , disclosure of private information and the misuse of it can damage people's feelings and cause considerable damage in people's lives.

In SNS where intimate information of the users is managed, privacy is of paramount importance. A research of Gross and Acquisti. In the early days of Facebook showed that the majority of users were unconcerned about privacy risks. They tended to use default privacy configurations and personal data were generously provided. More recent studies, like the one from Boyd and Hargittai , show that the privacy awareness of SNS users has increased lately.

The widespread media attention on SNS and on situations where the leakage of personal information of SNS users affected their lives has positively influenced the way SNS users manage their privacy . Nevertheless, the high number of privacy risks that affect SNS users leaves room for improvement in this field of study. The most important SNS users' privacy concerns are: identity theft , unauthorized access , misuse of personal information and stalking , and profiling . In this study we focus on misuse of personal information. This threat refers to the possibility of a malicious dissemination of previously collected information. For instance, users may face blackmailing situations when embarrassing data is collected from a SNS by a third party. In the context of SNSs, misuse of personal 2 information usually occurs when users disclose inappropriate information due to a negligence during the configuration of their privacy settings or ignorance about how privacy is managed on the SNS. The rest of privacy threats affect different levels of privacy on SNSs and fall out of the scope of this study. Identity theft and unauthorized access are related to access control enforcement (Kirkpatrick 2010).

For example, unauthorized access can occur if the authentication mechanisms of the SNS are not good enough or if the communication between the user and the SNS is not properly encrypted. Profiling is a threat when the party which owns the information on the SNS is not trustworthy. A typical case of profiling occurs when the party that manages the SNS sells the information available on the SNS to third parties that use it for marketing purposes. It has been acknowledged that in order to properly minimize misuse of personal information, a new privacy mechanism is needed. In the next section, we detail the requirements for such a new privacy mechanism

Any privacy mechanism has at its base an access control. Access controls dictate how permissions are given, what elements can be private, how access rules are defined, and so on. Access control models of current SNSs tend to be very simplistic. Nonetheless, recent improvements in facebook like SNSs have enhanced the access control models. For example, now it is possible to define policies to deny access to groups of users, instead of individuals. Some SNSs allow the possibility to express a social distance of contacts that have access to the resource, for example, friends of friends (two hops), friends of friends of friends (three hops), and so on. Another addition that only a few SNSs have added is the possibility to choose the amount of information from a friend that we want to receive (Johnson & Egelman 2012) .

However, these models still lack key elements. One of the most important is the lack of diversity in the type of relationships. Most SNSs only employ ”friend” as the only type of possible relationship. This lack of classification of contacts leads to privacy leaks to other members inside the social network. This is referred to by Johnson as the insider threat. Gates identifies the following requirements that an access control model for a SNS must fulfill:

• Relationship-based: People base their decision of sharing information on their relationship with others. Moreover, the properties of the relationship also affect the way people disclose their personal information. In social psychology, it is generally accepted that one discloses more of his/her personal information to someone in a strong relationship . Hence, a control access model that tries to reflect the way people disclose and share in real life should be based on relationships.

• Fine-grained: The access control has to allow users to define access policies for single items. If the access control is available in a fine-grained format the privacy policies can be more flexible and they can express the user’s preferences exactly. For example, a user should be able to define privacy policies for specific photos, individual blog entries, or even some words or phrases of a comment. In other words, users should be able to decide exactly to what extent others can access their information.

• Interoperability: Many SNSs have a specific objective; while Facebook aims to facilitate users contacting their friends, LinkedIn helps users to maintain their professional networks. Facebook and Linkedin have clearly different purposes. Because of this variety of purposes, users may have several multiple accounts in different SNSs, each one for a different social 3 objective. In this scenario, it is highly desirable for access controls to be interoperable and follow the users, so it is not necessary to define an entire new access control for each SNS.

• Sticky policies: Besides being interoperable, privacy policies should also follow the data to which they apply. For example, many SNS allow third party applications to access users’ data. The privacy preferences assigned to that data should be respected by these third parties and in whatever context it might travel to. This idea was introduced by Karjoth et al. .

In the related literature, we have also identified additional requirements that play a crucial role in developing successful access control models for SNSs:

• Content Type Management: SNS enable users to share a variety of different pieces of information: photos, videos, comments, events, hobbies, and so on. Besides the miscellany in the format of the information, its content also matters when deciding who has access and who has not . Flickr employs tags so users can classify their pictures according to their type. A similar approach could be used so users could define permissions based on the type of the content.

• Co-privacy: SNS users like to upload items to their profiles, such as photographs and videos, where other users are depicted. Specially, SNSs that focus on helping users to maintain their friend relationships encourage users to upload publications of this kind. Items of this type can raise several privacy concerns. While the owner of the item is in charge of assigning a privacy policy to it, the other users related to the item can be affected if the privacy policy is not appropriate for their interests. It is possible to infer a great amount of information about an individual from information leaks that occur due to shared items and privacy preference conflicts. Current access models do not consider these situations; thus, users are forced to use strategies like untagging, asking the owner to remove the photo or, in the most extreme situations, removing friendship links. Access controls should consider co-privacy management and offer mechanisms that allow every user involved in a single item to express their privacy preference so that the resulting privacy policy applied to that item maximizes the utility for everyone. An access control acts as the base for a privacy mechanism, however, they require other elements to be functional. It is not realistic to assume that SNS users can understand access control models and use them intuitively. Powerful privacy models are useless if they lack usability and are not understood by the people that will use them. Users need tools that guide them through the process of setting their privacy preferences. Users also require mechanisms that help them to understand their current privacy preferences and how their information is disseminated among other SNS users. According to related literature, a privacy mechanism for SNSs should fulfill these requirements:

• Automatic relationship inferring: If the access control has to be based on social relationships, these have to be accurately defined. SNS users tend to have a high number of friends. For example, according to the Facebook statistics, the average number of friends in that social network is 130. Hence, classifying every contact in a social network can represent a burden on the user. Privacy mechanisms should have the capacity to automatically infer the type of a relationship and make the whole process of friend classification easy and fast.

• Privacy setting recommendation: While privacy is paramount on SNSs, users are focused on enjoying the functionality that these offer. For many users privacy settings represent a burden, for others privacy settings are difficult to manage and understand. Recommender tools can help users to set properly their privacy settings. While recommenders can help reduce the user's burden, they are rarely perfectly accurate. Thus, it is important for the user to be able to view, understand, and modify the recommended policy before it is applied

• Privacy understandability: Access controls can be complex and daunting for SNS users. Average SNS users do not have expertise on security, thus, it is difficult for them to accurately evaluate how their information is disclosed through the SNS.

4.2.Privacy issues of SNS

Privacy implications associated with online social networking depend on the level of identifiability of the information provided, its possible recipients, and its possible uses. Even social networking websites that do not openly expose their users' identities may provide enough information to identify the profile's owner(Liu & Maes 2005).

This may happen, for example, through face re-identification Liu and Maes estimate in a 15% overlap in 2 of the major social networking sites they studied. Since users often re-use the same or similar photos across different sites, an identified face can be used to identify a pseudonym profile with the same or similar face on another site. Similar re-identifications are possible through demographic data, but also through category-based representations of interests that reveal unique or rare overlaps of hobbies or tastes(Liu & Maes 2005).

It is noted that information revelation can work in two ways: by allowing another party to identify a pseudonymous profile through previous knowledge of a subject's characteristics or traits; or by allowing another party to infer previously unknown characteristics or traits about a subject identified on a certain site.

4.3.Current Privacy Preferences on the most popular SNS

Facebook

Most users of Facebook find user privacy settings confusing. While a lot of users think they have their Facebook Profile locked down, 50% of Facebook users have yet to use the “view as” feature to check privacy settings.

What this means is that even though a user may have setup Facebook privacy settings , he could be leaving important information exposed.

For those of who don’t think that Facebook user privacy is a concern, here are a few surprising stats.

- 25% of users don’t know if Facebook tracks their location.
- 29% of Facebook users don’t use strong passwords.
- 39% of users don’t review posts or photos they are tagged in before they are published.

The statistic below shows the results of a survey among social network members regarding their preferred privacy settings for social networks in Germany in 2013. During the survey period it was found that 82 percent of respondents said that they wanted a setting to block other users.

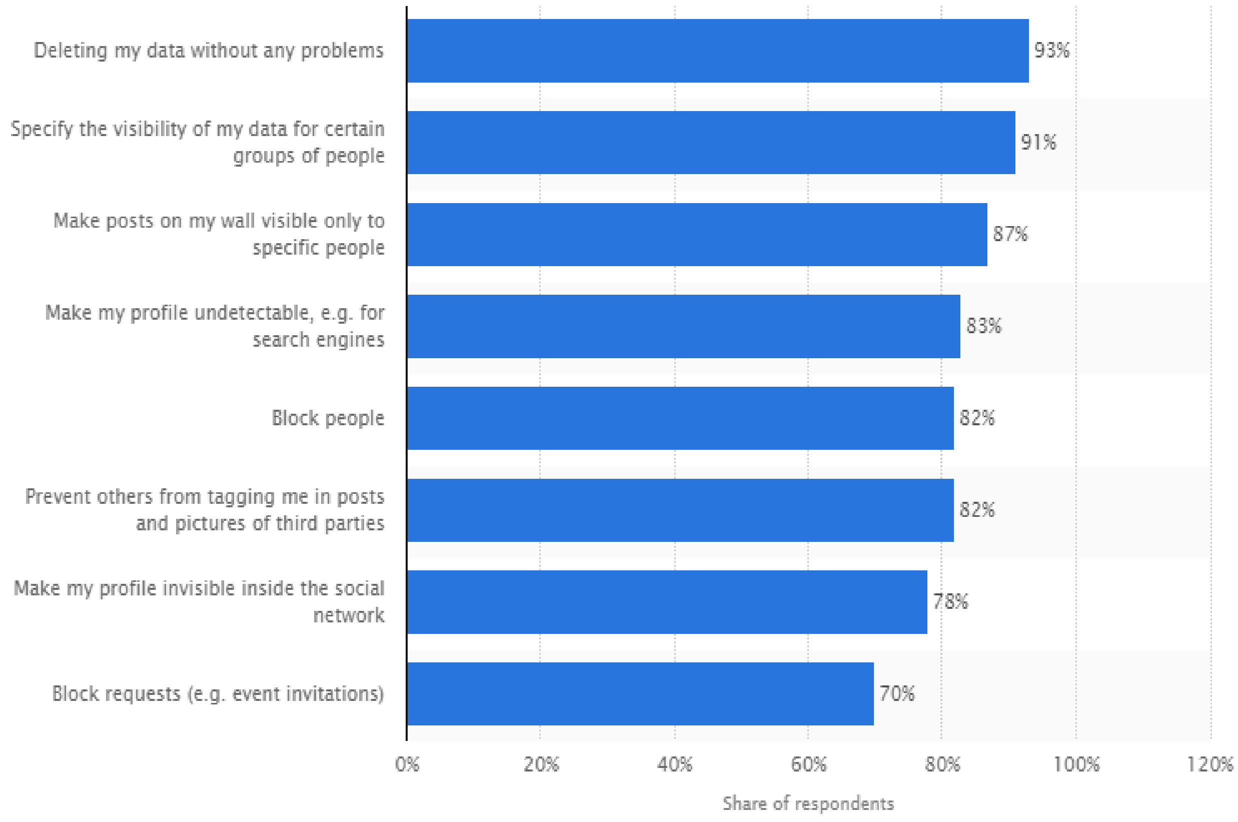


Table 10 – preferred privacy settings for social networks

1. Privacy management on social media sites

The results of the following survey is based on the findings of a survey on Americans' use of the Internet. The results in this report are based on data from telephone interviews conducted by Princeton Survey Research Associates International from April 26 to May 22, 2011, among a sample of 2,277 adults, age 18 and older.

This report addresses several questions about the privacy settings people choose for their social networking profiles, and provides new data about the specific steps users take to control the flow of information to different people within their networks.

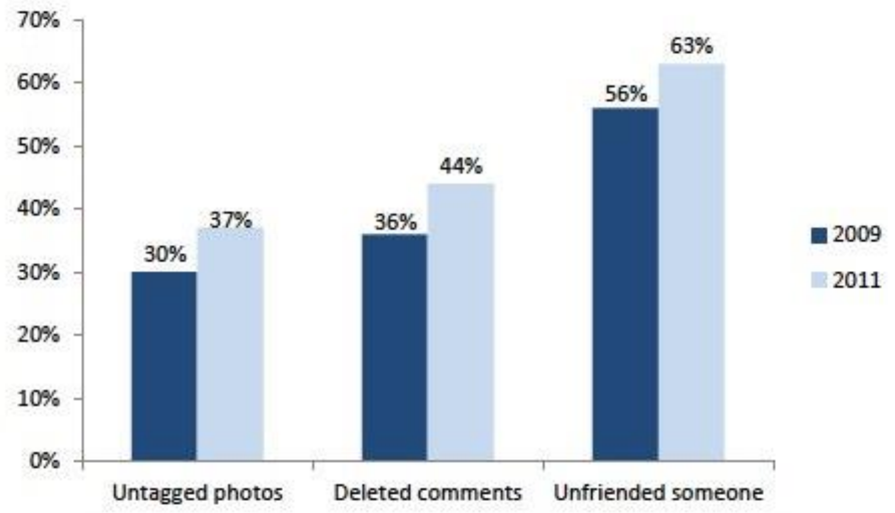
The most important findings of the survey are shown below:

2. Social network users are becoming more active in pruning and managing their accounts. Women and younger users tend to unfriend more than others.

About two-thirds of internet users use social networking sites (SNS) and all the major metrics for profile management are up, compared to 2009: 63% of them have deleted people from their “friends” lists, up from 56% in 2009; 44% have deleted comments made by others on their profile; and 37% have removed their names from photos that were tagged to identify them.

More privacy and reputation management on social networking sites

% of social networking site users who have taken these steps on their profile



Source: The Pew Research Center's Internet & American Life Project, April 26 – May 22, 2011 Spring Tracking Survey; n=2,277 adults ages 18 and older, including 755 cell phone interviews. Interviews were conducted in English and Spanish. Margin of error is +/-3 percentage points for SNS users (n=1,015)

Table 11

Some 67% of women who maintain a profile say they have deleted people from their network, compared with 58% of men. Likewise, young adults are more active “unfrienders” when compared with older users.

3. A majority of social network site users – 58% – restrict access to their profiles and women are significantly more likely to choose private settings.

More than half of social networking site users (58%) say their main profile is set to private so that only friends can see it; 19% set their profile to partially private so that friends of friends can view it; and 20% say their main profile is set to be completely public. Women who use SNS are more likely than men to set the highest restrictions (67% vs. 48%).

4. Half of SNS users say they have some difficulty in managing privacy controls, but just 2% say it is "very difficult" to use the controls. Those with the most education report the most trouble.

In all, 48% of social media users report some level of difficulty in managing the privacy controls on their profile, while 49% say that it is "not difficult at all." Very few users (2%) describe their experiences as "very difficult," while 16% say they are "somewhat difficult" and another 30% say the controls are "not too difficult" to manage.

Social media users who are college graduates are significantly more likely than those with lower levels of education to say that they experience some difficulty in managing the privacy controls on their profiles.

5. 11% of SNS users have posted content they regret.

Male profile owners are almost twice as likely as female profile owners to profess regret for posting content (15% vs. 8%). Young adults are also more prone to say they regret some of their social media postings; 15% of profile owners ages 18-29 say they have posted content they later regret, compared with just 5% of profile owners ages 50 and older.

6. Two-thirds of online adults have a profile on a social networking site, and most restrict access to friends only.

Two in three online adults (63%) say they currently maintain a profile on a social networking site, up from just 20% who said they had ever created a profile in 2006. When asked to think about the profile they use most often, 58% say their main profile is set to be private so that only friends can see it. Another 19% say they have their profile set to be partially private so that friends of friends or networks can view it and 20% say their main profile is set to be completely public.

A notable portion of those who already restrict access to their SNS profile take further steps to limit what certain friends can see. Some 26% of those whose profile is at least partially private say they use additional privacy settings to limit what certain friends can and cannot see. This finding is consistent across all core demographic groups.

7.Women who maintain social media profiles are significantly more likely than men to keep their profiles private.

However, there is a significant gender gap when it comes to the way male and female social media users choose to manage their profiles. Women are much more conservative in the basic settings they choose; 67% of female profile owners restrict access to friends only compared with 48% of male profile owners. Likewise, men are more apt than women to choose partially private (23% vs. 16%) or fully public (26% vs. 14%) settings.

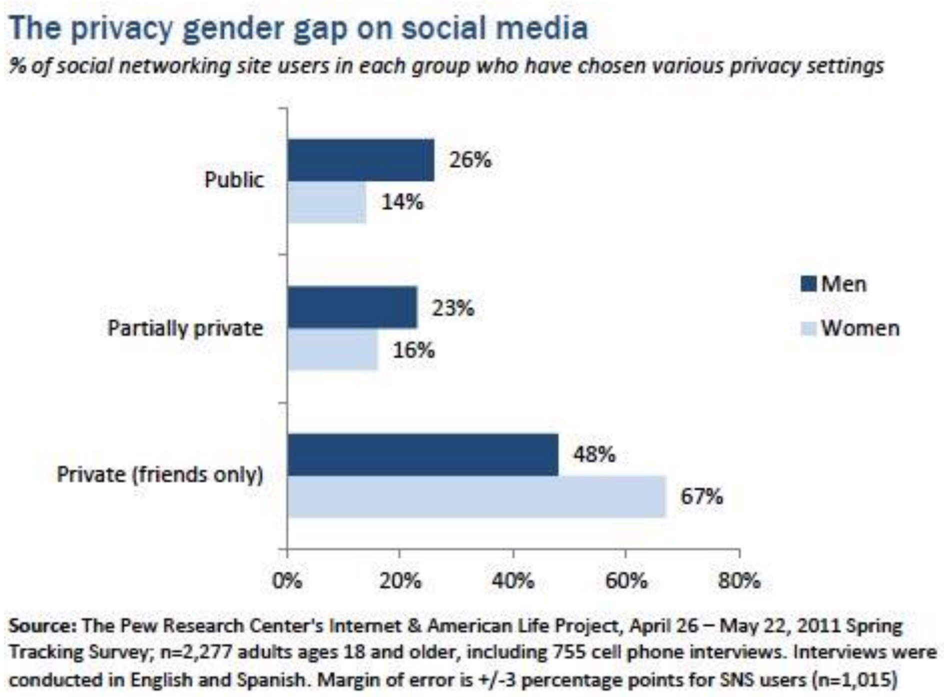


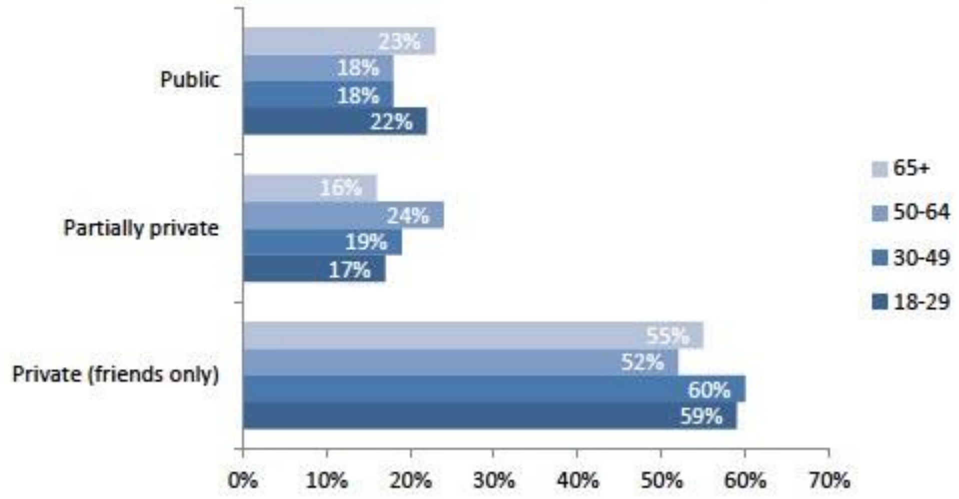
Table 12 – preffered settings among genders

8. Young and old alike choose private settings for their profiles.

When looking at social media usage patterns, age tends to be one of the strongest variables. For instance, younger users have long been the most active users of the sites and the most active managers of their online reputations.However, when it comes to basic privacy settings, users of all ages are equally likely to choose a private, semi-private or public setting for their profile. There are no significant variations across age groups.

Private settings are the norm, regardless of age

% of social networking site users in each age group who have chosen various privacy settings



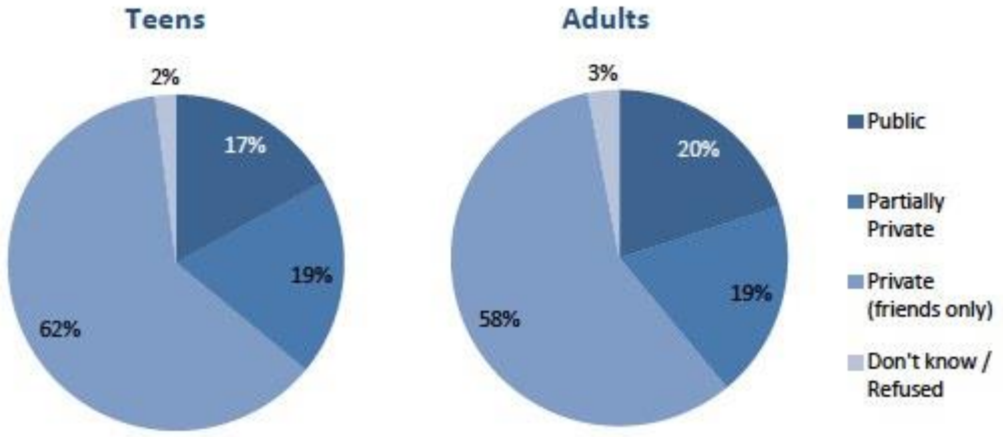
Source: The Pew Research Center's Internet & American Life Project, April 26 – May 22, 2011 Spring Tracking Survey; n=2,277 adults ages 18 and older, including 755 cell phone interviews. Interviews were conducted in English and Spanish. Margin of error is +/-3 percentage points for SNS users (n=1,015)

Table 13 – preffered settings

The choices that adults make regarding their privacy settings are also virtually identical to those of teenage social media users. Close to two-thirds (62%) of teens who have a social media profile say the profile they use most often is set to be private so that only their friends can see the content they post. One in five (19%) say their profile is partially private so that friends of friends or their networks can see some version of their profile. Just 17% say their profile is set to public so that everyone can see it. This distribution is consistent regardless of how often a teen uses social network sites.

Teens' and adults' privacy settings on social media sites

Based on teen SNS or Twitter users (n=623) and adult SNS or Twitter users who have an SNS profile (n=975)



Source: The Pew Research Center's Internet & American Life Project, April 26 – May 22, 2011 Spring Tracking Survey; n=2,277 adults ages 18 and older, including 755 cell phone interviews. Interviews were conducted in English and Spanish. Margin of error is +/-3 percentage points for SNS users (n=1,015) Teen data from Pew Internet's Teen-Parent survey, April 19-July 14, 2011. n=799 for teens and parents, including oversample of minority families. Interviews were conducted in English and Spanish.

Table 14 – preferred settings of Social networks sites, comparing teens and adults

9. Half of social media users report some difficulty in managing the privacy controls on their profile, but few describe their experience as "very difficult."

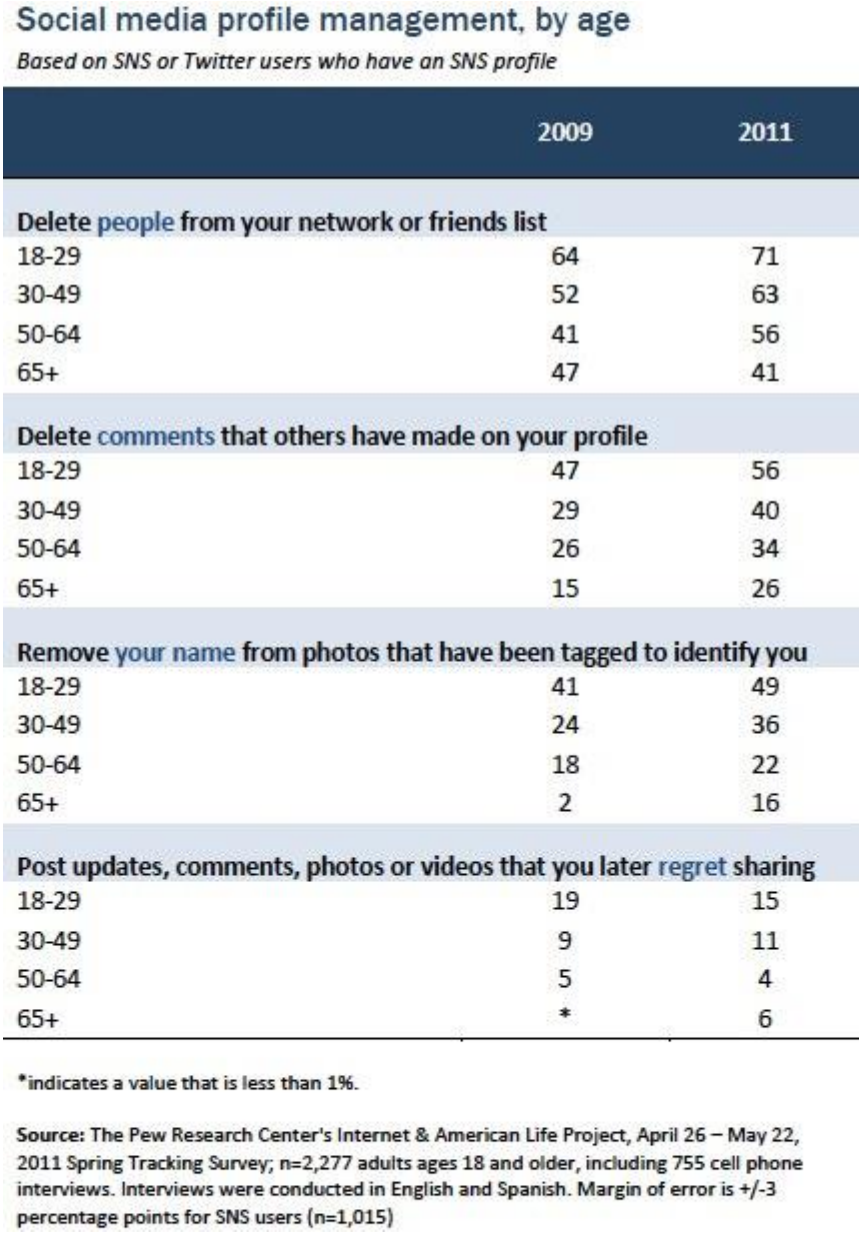
The complexity of privacy settings varies greatly across different social media sites, and in the case of Facebook, the default settings have changed significantly over time.9 In all, 48% of social media users report some level of difficulty in managing the privacy controls on their profile, while 49% say that it is "not difficult at all." Few users (2%) describe their experiences as "very difficult," while 16% say they are "somewhat difficult" and another 30% say the controls are "not too difficult" to manage. Young adults are considerably more likely than any other age group to feel fully confident in their privacy controls; 57% of social media users ages 18-29 say it is "not difficult at all" to manage them, compared with 48% of those ages 30-49, 41% of those ages 50-64 and 31% of those ages 65 and older.

10. Social media users with the highest levels of education report the most difficulty in managing the privacy controls on their profiles.

Social media users who are college graduates are significantly more likely than those with lower levels of education to say that they experience some difficulty in managing the privacy controls on their profiles. For those in the highest education bracket, the majority (62%) report some level of difficulty, compared with just 42% of those with some college education. However, again, few college graduates who are social media users (2%) describe their experiences as “very difficult.” Instead, they are more likely to report that managing the privacy settings on their profile is “somewhat difficult” (21%) or “not too difficult” (39%). Those with only some college education report less trouble; 12% describe their experiences as somewhat difficult and 29% say that managing their controls is “not too difficult.”

11. Profile “pruning” is on the rise. Deleting unwanted friends, comments and photo tags grows in popularity.

Over time, as social networking sites have become a mainstream communications channel in everyday life, profile owners have become more active managers of their profiles and the content that is posted by others in their networks. Two-thirds of profile owners (63%) have deleted people from their networks or friend lists, up from 56% in 2009. Another 44% say they have deleted comments that others have made on their profile, up from just 36% two years prior. And as photo tagging has become more automated on sites like Facebook, users have become more likely to remove their names from photos that were tagged to identify them; 37% of profile owners have done this, up from 30% in 2009.



Social media profile management, by age

Based on SNS or Twitter users who have an SNS profile

	2009	2011
Delete people from your network or friends list		
18-29	64	71
30-49	52	63
50-64	41	56
65+	47	41
Delete comments that others have made on your profile		
18-29	47	56
30-49	29	40
50-64	26	34
65+	15	26
Remove your name from photos that have been tagged to identify you		
18-29	41	49
30-49	24	36
50-64	18	22
65+	2	16
Post updates, comments, photos or videos that you later regret sharing		
18-29	19	15
30-49	9	11
50-64	5	4
65+	*	6

*indicates a value that is less than 1%.

Source: The Pew Research Center's Internet & American Life Project, April 26 – May 22, 2011 Spring Tracking Survey; n=2,277 adults ages 18 and older, including 755 cell phone interviews. Interviews were conducted in English and Spanish. Margin of error is +/-3 percentage points for SNS users (n=1,015)

Table 15

12. Women and young adults are the "unfriend-liest".

Female social media users are more apt than male users to cull their list of friends and delete any unwanted contacts: 67% of women who maintain a profile say they have deleted people from their network, compared with just 58% of men. Likewise, young adults are more active unfrienders when compared with older users. Seven in ten (71%) young adult social media users say they have deleted contacts from their friends list, compared with 63% of users ages 30-49, 56% of those ages 50-64 and only 41% of those ages 65 and older.

13. Deleting social media comments is part of the reputation management work of being a young adult.

All users have become more likely to delete comments on their profiles over time, but this is especially true of young adults. It is now the case that 56% of social media users ages 18-29 say they have deleted comments that others have made on their profile, compared with 40% of those ages 30-49, 34% of those ages 50-64 and 26% of social media users ages 65 and older. In contrast to the gender differences with unfriending, male and female social media users are equally as likely to say that they have deleted comments that others have made on their profile (44% of men and women report this).

The task of removing photo tags is also much more common among young adults.

Whether because there are simply more photos being shared or there is more sensitivity to their content, young adult social media users are the most likely age group to report removal of photo tags. Fully half of young adult social media users (49%) say they have deleted their name from photos that were tagged to identify them. That compares to 36% of social media users ages 30-49, 22% of those ages 50-64 and only 16% of those ages 65 and older. As with comments, there are no significant gender differences; male and female users are equally likely to delete photo tags (36% vs. 38%).

14. While users manage the content that others post, one in ten profile owners voices regrets about their own posts.

Even as social media users become more active curators of their profile, a small group of what might be described as trigger-happy users say they post updates, comments, photos or videos that they later regret sharing. One in ten profile owners (11%) say they have posted regrettable content to a social networking site, virtually the same number as reported this activity in 2009 (12%). Male profile owners are almost twice as likely as female profile owners to profess regret for posting content (15% vs. 8%). Young adults are also considerably more prone to regret; 15% of profile owners ages 18-29 say they have posted content they later regret, compared with just 5% of profile owners ages 50 and older.

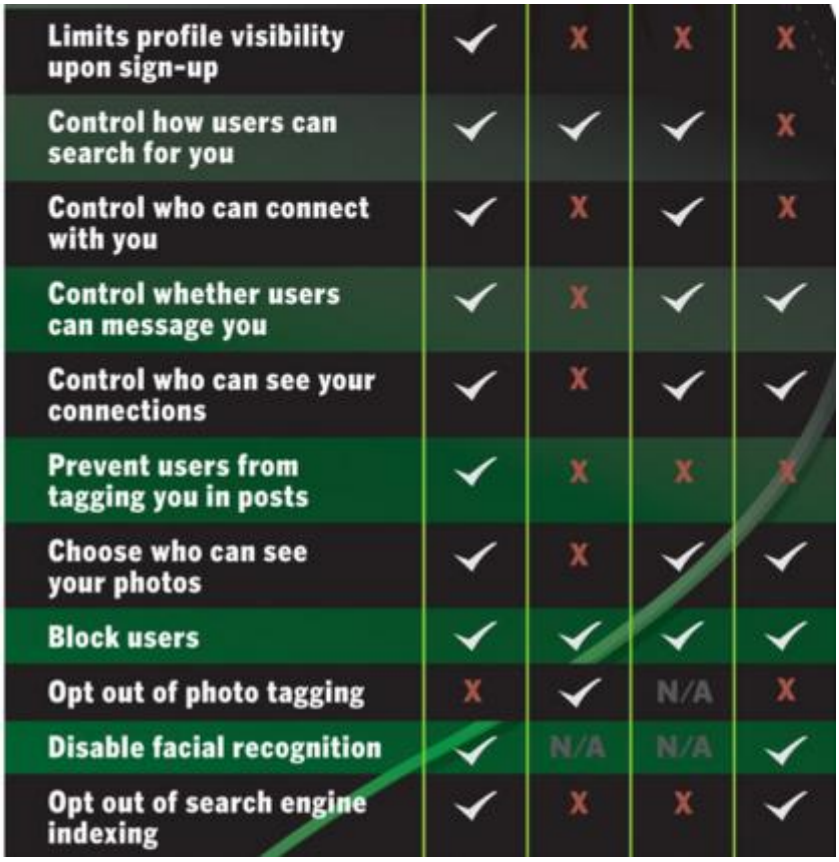
15. Most social networking users are on Facebook and manage their social media presence through one account.

More than nine in ten (93%) profile owners say that they have a profile on Facebook, up from 73% in 2009. Over the same period, the popularity of MySpace has continued to wane; 48% maintained a presence there in 2009, while just 23% of profile owners said they used MySpace in the latest survey. At the same time, use of Twitter has grown almost twofold, such that 11% of profile owners say they have a presence there, up from just 6% in 2009.

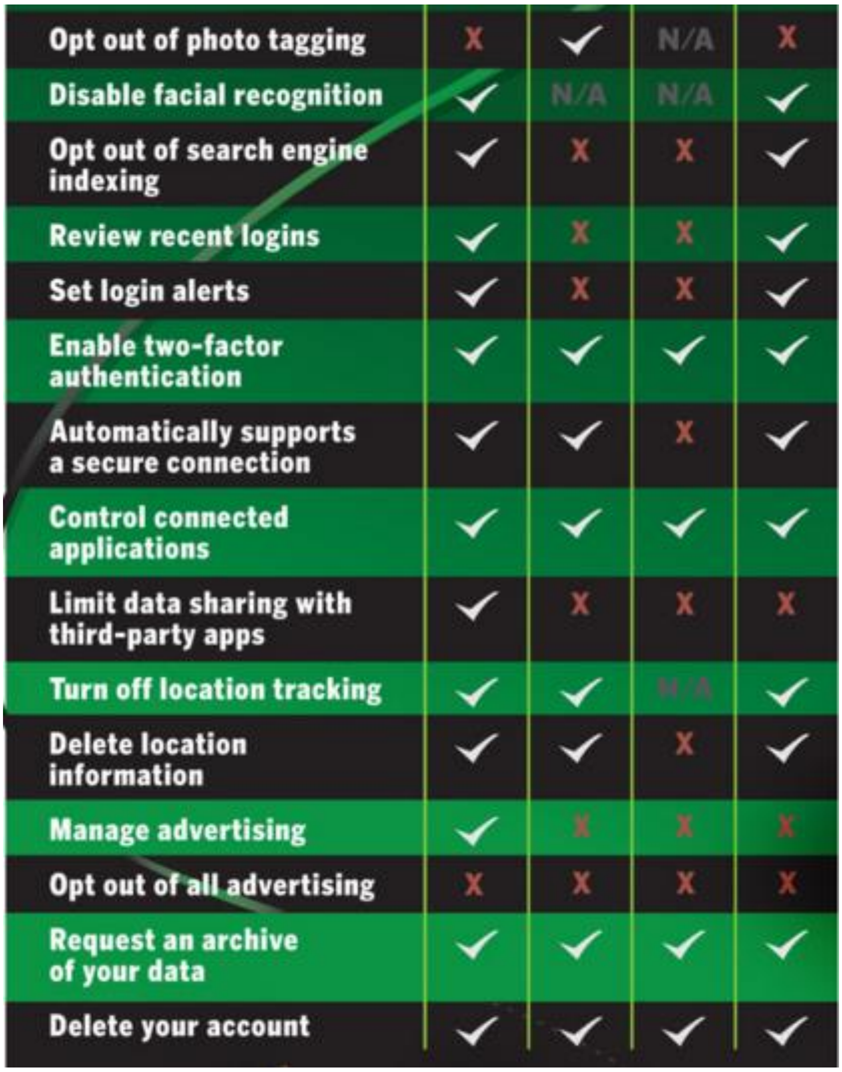
Whether due to the influx of new social media users in recent years or to those who are simplifying their online identity management, users have become more likely to maintain a profile on just one site. More than half (55%) of social networking and Twitter users say this, up from 45% in 2009.

4.4.Comparison of the Privacy Preferences

Observing the above table, we can see the settings that are available of most popular social networks, Facebook, Twitter, LinkedIn, Google:



Limits profile visibility upon sign-up	✓	X	X	X
Control how users can search for you	✓	✓	✓	X
Control who can connect with you	✓	X	✓	X
Control whether users can message you	✓	X	✓	✓
Control who can see your connections	✓	X	✓	✓
Prevent users from tagging you in posts	✓	X	X	X
Choose who can see your photos	✓	X	✓	✓
Block users	✓	✓	✓	✓
Opt out of photo tagging	X	✓	N/A	X
Disable facial recognition	✓	N/A	N/A	✓
Opt out of search engine indexing	✓	X	X	✓



Opt out of photo tagging	X	✓	N/A	X
Disable facial recognition	✓	N/A	N/A	✓
Opt out of search engine indexing	✓	X	X	✓
Review recent logins	✓	X	X	✓
Set login alerts	✓	X	X	✓
Enable two-factor authentication	✓	✓	✓	✓
Automatically supports a secure connection	✓	✓	X	✓
Control connected applications	✓	✓	✓	✓
Limit data sharing with third-party apps	✓	X	X	X
Turn off location tracking	✓	✓	N/A	✓
Delete location information	✓	✓	X	✓
Manage advertising	✓	X	X	X
Opt out of all advertising	X	X	X	X
Request an archive of your data	✓	✓	✓	✓
Delete your account	✓	✓	✓	✓

Table 16-available security options among popular Social Networks

From table 16 we can conclude that not all Social networks privacy settings options are the same. Concerning "Facebook", a user has almost full control of limitation of who can show his posts or photos uploaded in his profile.

There is difference upon sign-up in social networks. Only Facebook gives the option to a user to choose and set visibility of profile.

It is worth mentioned that in Twitter options for privacy settings, there are some options that are not available for a user. For example, While option “choose who can see your photo” is available in Facebook, it is not available in Twitter. Also the option “prevent people to make posts to photos” is available in Facebook but not in Twitter and also not available in LinkedIn or Google.

4.5. Privacy on Mobile SNS

We know that our web browsers transmit our habits to a ton of trackers and advertisers unless we use a privacy plugin for our protection).

Professor Jason Hong who is the leader of the Carnegie Mellon University research team says

“There is a lot more sensitive data on your smartphone, such as your call log, contact lists, and location,”, a site that grades Android apps on their privacy behaviors. “Smartphone advertising is currently not as bad as online advertising because it's limited, but in the near future, it wouldn't be hard for it to get far more intrusive.”

For example, advertisers may be able to learn something as personal as the hours you sleep by monitoring the level of sound through any app that requests access to the mic. Privacy Grade is funded by the National Science Foundation, NQ Mobile, Google and the Army Research Office and analyzes apps for what data users expect to be taken versus what data the app actually lifts. The privacy grade isn't so much a reflection of how tight a grip the app keeps on user data, but rather how aware the user is of its data skimming.

Hong says that when people know why an app is using something as sensitive as their location – for example, for targeted advertising – it makes them more comfortable than when simply told an app is using their location.

“It's about being aware of how an application uses data so people can make better decisions,” Hong says.

Yet many apps may violate their own privacy policies, resulting in private posts that aren’t actually private or users being tracked against their will. From indefinite storage of supposedly deleted content, to the unknowing transmission of personal data directly to the NSA, the worst apps for privacy are...

4.5.1.Privacy Issues on Mobile SNS

There are many applications that violate our privacy :

Uber: An application that knows every place where a user go

Most of us expect that our locations are recorded and fed back to certain apps for a better service. Naturally, a car-hailing app whose success is dependent on its ability to locate the nearest vehicle and send it to you is expected to have access to this data. What isn't expected is for the data to be used to track its customers (Stokes 2014).

In November, Uber started an investigation of its New York director for looking up the profile of a Buzzfeed News journalist and tracking her Uber trips. This followed allegations that Uber allowed any employee to use an internal company tool called "God View" so as to track any Uber passenger's movements -- of particular concern when each profile is attached to some personal information, unlike passengers in regular taxis.

Parker Higgin, an activist at the Electronics Frontier Foundation claims:

"There's a lot you can tell about a person from their location,"

"When they arrive at and leave work, if they're spending the night at home or frequently somewhere else, how religious someone is based on their location on Sundays. Location is a sensitive thing that wraps a lot of other sensitive things."

Applications: Whisper, Secret, Yik-Yak

Whisper, Secret and Yik-Yak are social networking apps with two major selling points in common: all three claim that users can make anonymous posts, and all three subsequently failed to deliver on that claim.

Whisper called itself "the safest place on the internet". However, an investigation by the Guardian published in October revealed that this application violated its own terms of service by tracking users who had opted out and storing posts that users thought they had deleted in a searchable database that goes back to Whisper's 2012 launch. According to the report, users deemed to be newsworthy -- such as individuals who claimed to work at Disney, Capitol Hill or in the military -- were monitored through their history of posts and locations.

"The kind of secrets that people are confessing to on these sites could be used as leverage to bully or even extort the confessor should their identity be revealed," says Lookout senior security product manager Jeremy Linden. "This is exacerbated by the fact that these services are attractive to teens."

Another application called "Secret" which is similar to "Whisper" had 42 security holes revealed by white-hat hackers. To be more specific, security researchers Benjamin Caudill and Bryan Seely were able to exploit Secret's news feed feature that shows posts from (anonymous) friends once a user amasses seven or more. By using bots for fake accounts, the researchers connected seven bots with one real user and because the bots didn't post, they were able to read all the posts from one user and identify them based on the details in the posts.

"There are vulnerabilities with these apps in terms of encryption," Linden says. "Many of them do not encrypt their data and even more only encrypt the parts of the session that the developers feel needs to be protected, such as financial transactions or logins."

Another application called "Yik-Yak", the anonymous social network especially popular with high-school and college students, which doesn't use passwords -- and doesn't encrypt all traffic from the application.

Cloud security company SilverSky Labs found that hackers could de-anonymize users and take control of the account by intruding on the non-encrypted traffic between Yik-Yak and an analytics company (Stokes 2014).

Popular game "Angry Birds"

Advertisers aren't the only ones interested in your fruit-slicing, bird-slinging efforts. The New York Times reported that the NSA and its British equivalent, GCHQ, were targeting leaky smartphone apps including Angry Birds -- which has been downloaded over 2 billion times -- for user data such as age, gender and location. One classified 2012 British report included a code for mining profiles created when Android users play Angry Birds. Another documented that an ad company called Millennial Media worked with Angry Birds developer Rovio to create more intrusive profiles for Android and iOS versions, including additional categories such as ethnicity, marital status and sexual orientation (Stokes 2014).

Since then, President Obama has announced major reforms to the surveillance program, so our exploits with the furious fowl may be less leaky.

Over at Privacy Grade, the Angry Birds Android app still receives a middling grade of C for using the phone's unique identity and cell number for market and customer analysis. That network access is leveraged both for app functionality and that old faithful: targeted advertising. According to Rovio's privacy policy, its iOS app does much the same(Stokes 2014).

The self-destructing photo app that doesn't: Snapchat

Last year (2015) , self-deleting photo messaging app Snapchat was hacked and lost a database of 4.6 million usernames connected to phone numbers. After being charged by the Federal Trade Commission (FTC), the company made partial amends by adding a feature for users to opt out of entering their phone numbers. But the app is far from its self-claimed "ephemeral media" ideal.

Photos that are sent over Snapchat can't be screenshotted and are meant to be viewable for only 1-10 seconds, depending on the sender, but there are several third-party apps for Android and iOS that work with Snapchat to allow recipients to screenshot images for as long as they're on screen. Most notorious of all is Snapsaved, which earlier this year lost hundreds of thousands of photos that Snapchat users had (unethically) saved to its cloud servers(Stokes 2014).

This doesn't take into account the simplest hack of all: using another phone to take a photo of a Snapchat “temporary” photo.

Though most of the photos sent over Snapchat are not “sensitive content,” according to a University of Washington study, the same study found that many users would change their behavior after knowing about Snapchat's (lack of) security features (Stokes 2014).

Messenger apps: Mxit, QQ

“QQ” application is a China-based IM offering used by 820 million people that's available in six languages, and application “Mxit”, a smaller one, South African based-social network, were the two least-private services, sending and storing messages in plain text so hackers and staff alike can access them. Nor did they verify contacts so users know they're talking to who they think they're talking to (to be fair, neither does Google Chat, Viber, Yahoo or any other popular service). Their security designs were also not open to review, nor had they had code audited for vulnerabilities.

Facebook Messenger and WhatsApp were just barely superior, encrypting messages in transit. Apple's iMessage was deemed the best of the mainstream messengers: messages are encrypted end-to-end and can't be decrypted by Apple (Stokes 2014).

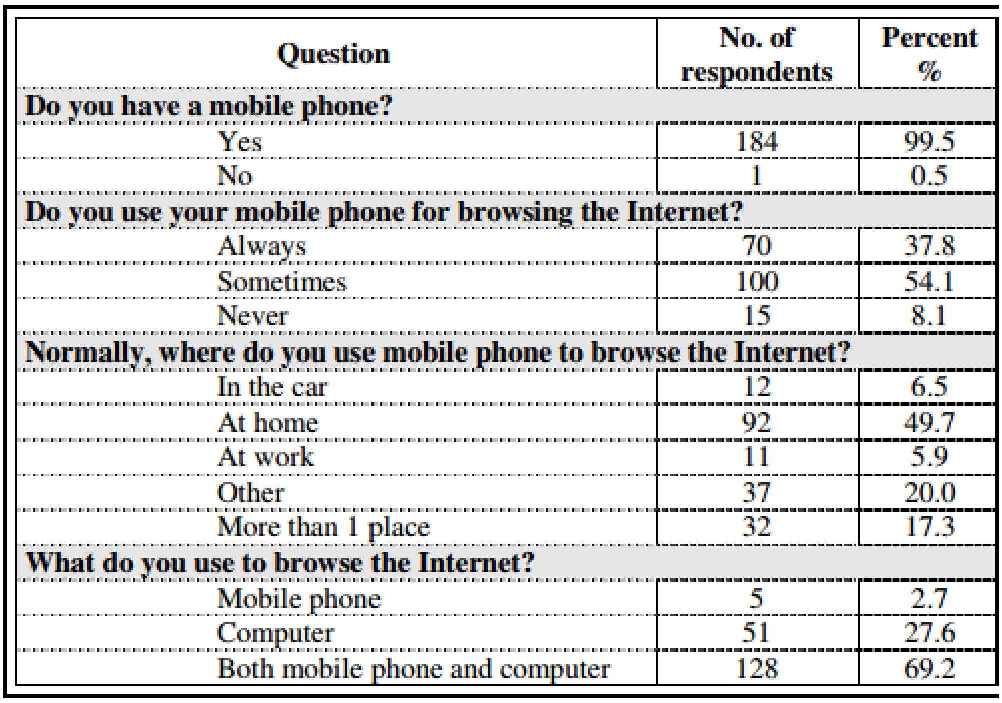
4.5.2. Current Privacy preferences on Mobile SNS

To understand current privacy preferences of users on mobile using social networks we will show a survey from University of Dammam.

The study sample was selected from the University of Dammam in Saudi Arabia and the New England University in Australia. The criteria for selecting respondents were that respondents should have at least one social networks account and mobile phone. In addition, the study population was both students and staff of University of New England and University of Dammam and aged 18 and more than 45 years. Data were collected from some departments and colleges through hard copy forms included with the participation invitations. Most of the participants from the University of Dammam were males because there is no mix between genders on colleges(Aldhafferi & Watson 2013).

The survey questionnaire was available in two languages: English and Arabic. A total of 185 respondents completed the survey (95 used the Arabic questionnaire and 90 used the English questionnaire) and all questions were multi-choices questions.

. Summary of descriptive statistics A total of 185 participants (157 males and 28 females) participated in the survey. Majority (75%) of the respondents belonged to the 18-25 age group. Table 17 shows that nearly all of the respondents had their own mobile phones, and most of them (92%) used their mobile phones to browse the Internet. Half (50%) of them used their mobile phones to browse the Internet at home. About 70 percent used both their mobile phones and computers to browse the Internet(Aldhafferi & Watson 2013).

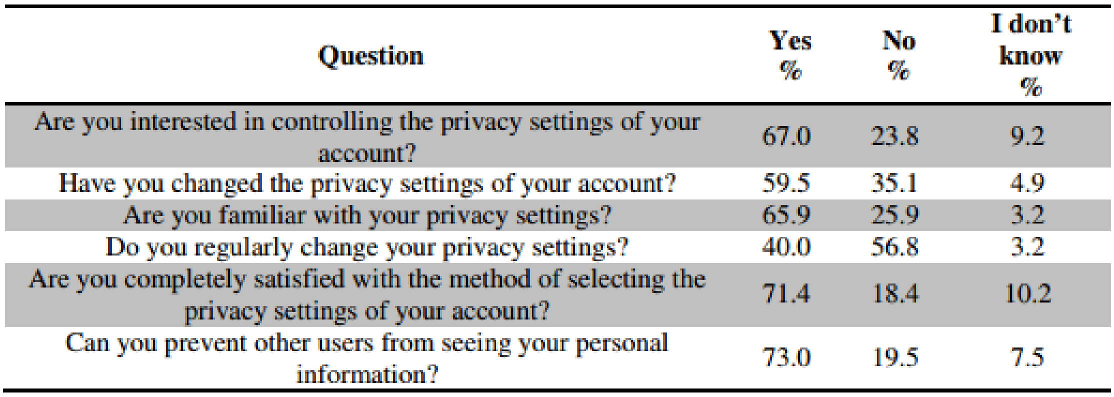


Question	No. of respondents	Percent %
Do you have a mobile phone?		
Yes	184	99.5
No	1	0.5
Do you use your mobile phone for browsing the Internet?		
Always	70	37.8
Sometimes	100	54.1
Never	15	8.1
Normally, where do you use mobile phone to browse the Internet?		
In the car	12	6.5
At home	92	49.7
At work	11	5.9
Other	37	20.0
More than 1 place	32	17.3
What do you use to browse the Internet?		
Mobile phone	5	2.7
Computer	51	27.6
Both mobile phone and computer	128	69.2

Table 17 – Ownership of mobile phones and devices used to browse the Internet

Results of a survey show that although most of the users are aware of the privacy settings, most of them do not change their privacy settings from default settings (Table 2). Majority (67%) of the respondents were interested in controlling their privacy settings, but only 60 percent changed them. Only 40 percent changed their privacy settings regularly. Twothirds (66%) of the users said they were familiar with privacy settings, and about three-fourths (73%) said they could prevent others from seeing their personal information. Majority (71%) of the respondents claimed they were completely satisfied with the method of selecting their account's privacy settings (Aldhafferi & Watson 2013).

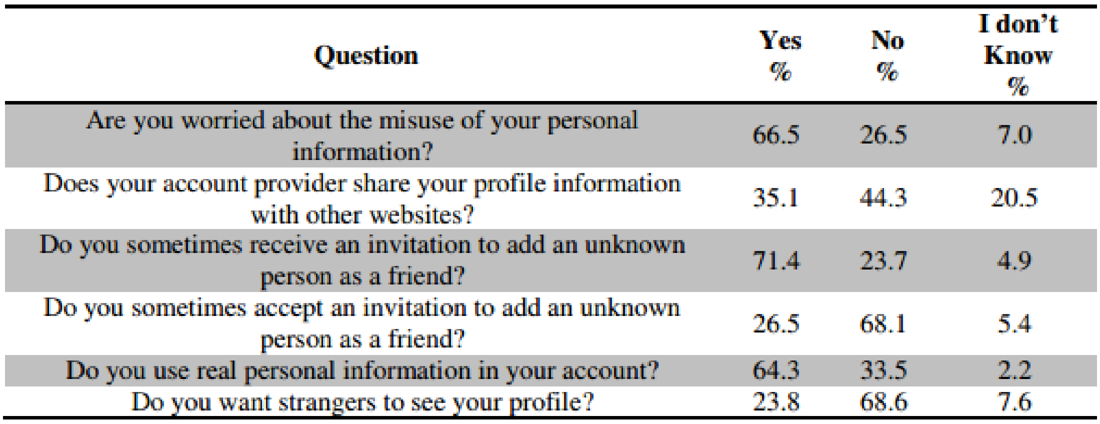
Table 12 – preferred settings among genders



Question	Yes %	No %	I don't know %
Are you interested in controlling the privacy settings of your account?	67.0	23.8	9.2
Have you changed the privacy settings of your account?	59.5	35.1	4.9
Are you familiar with your privacy settings?	65.9	25.9	3.2
Do you regularly change your privacy settings?	40.0	56.8	3.2
Are you completely satisfied with the method of selecting the privacy settings of your account?	71.4	18.4	10.2
Can you prevent other users from seeing your personal information?	73.0	19.5	7.5

Table 18 – Awareness and use of privacy settings

The survey questionnaire also measured the respondents' awareness of the risks that could occur from the leakage of personal information. Respondents were asked if they posted real personal information on their accounts. Table 3 shows that two-thirds (66%) of the respondents were worried about the misuse of their personal information on their accounts. In addition, 69% of the respondents did not want strangers to see their personal information. The respondents were also asked if their account providers shared their profile information with other websites. Slightly more than one-third (35%) said yes. This highlights the need to develop a framework that gives users the authority to allow or disallow websites to use their personal information. Results show that users were cautious about accepting friend requests from strangers. Although 71 percent of the respondents received invitations to add an unknown person as a friend, 68 percent rejected these requests(Aldhafferi & Watson 2013).



Question	Yes %	No %	I don't Know %
Are you worried about the misuse of your personal information?	66.5	26.5	7.0
Does your account provider share your profile information with other websites?	35.1	44.3	20.5
Do you sometimes receive an invitation to add an unknown person as a friend?	71.4	23.7	4.9
Do you sometimes accept an invitation to add an unknown person as a friend?	26.5	68.1	5.4
Do you use real personal information in your account?	64.3	33.5	2.2
Do you want strangers to see your profile?	23.8	68.6	7.6

Table 19 – Awareness of the risk of personal information misuse

Conclusion

Social networking services (SNSs) such as Facebook or Twitter have experienced an explosive growth during the few past years. Millions of users have created their profiles on these services because they experience great benefits in terms of friendship. The success of social media networks growth is due to supported activities of society and the current researches shows that it there is no doubt of continuation and existence of social networks.

The rates of use are impressive. There are many companies that have made researches for example "Nielsen". According to this research , in February 2010 each user spent roughly 5.5-hour per month in the web pages of social networking. Facebook is for sure, one from these web pages. Compared 2010 to year 2009, there is an increase of 2 hours in surfing on social networks sites.. This company has made this research in 10 countries worldwide. SNSs can help people to maintain their friendships, organize their social lives, start new friendships, or meet others that share their hobbies and interests.

However, all these benefits can be eclipsed by the privacy hazards that affect people in SNSs. People expose intimate information of their lives on SNSs, and this information affects the way others think about them. It is crucial that users be able to control how their information is distributed through the SNSs and decide who can access it.

The increasing sophistication of information technology with its capacity to collect, analyze and disseminate information is posing significant threats to social networks users privacy. It is argued that the changes and the impacts of information technology are big and accelerating so quickly. Privacy issues are totally concern users about potential invasions all over the Internet world. Also, new security threats are emerging in social networks because of location tracking.

To conclude, many surveys in the past proved that first of all many users of social networks sites are totally unaware and uninformed about private policies of the social networking sites. Usually they get bored to read them or they just trust social networking sites.

However, after many incidents of privacy violation recent surveys shows that users have matured their thinks about privacy and now care more about setting privacy level on social networking web sites.

References

Aldhafferi N., Charles Watson and A.S.M Sajeev (2013) *PERSONAL INFORMATION PRIVACY SETTINGS OF ONLINE SOCIAL NETWORKS AND THEIR SUITABILITY FOR MOBILE INTERNET DEVICES*, school of Science and Technology, University of New England,International Journal of Security, Privacy and Trust Management (IJSPTM) vol 2, No 2, April 2013

Boyd, Danah M.; Nicole B. Ellison; "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication*, vol. 13, p. 210-230, 2008

Boyd D. , Ellison N. (2007),
Social Network Sites: Definition, History, and Scholarship, Michigan State University, 2007

Chen, Guanling; F. Rahman; "Analyzing Privacy Designs of Mobile Social Networking Applications," Procceedings of International Symposium on Trust, Security and Privacy for Pervasive Applications, Shanghai, China, 2008

Ghiglieri M. , SImo H., 2, and Waidner M (2012), *Technical Aspects of Online Privacy* Technische Universität Darmstadt, FB Informatik/FG SIT 2 Fraunhofer Institute for Secure Information Technology (SIT), Darmst

Gross. Re-identifying facial images. Technical report, Carnegie Mellon University, Institute for Software Research International, 2005. In preparation

Houghton & Joinson (2010) Journal of Technology in Human Services *Privacy, Social Network Sites, and Social Relations*

Johnson M. Serge Egelman, Steven M. Bellovin (2012) *Facebook and Privacy: It's Complicated*, Symposium on Usable Privacy and Security (SOUPS) 2012, July 11–13, 2012, Washington, DC USA

Kirkpatrick, David; *The Facebook Effect*, Simon and Schuster, USA, 2010

Lipsman, A. (2010). 2009: Another strong year for Facebook. Retrieved from http:// blog.comscore.com/2010/01/strong_year_for_facebook.html

Moreham (2008) *Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy* , Victoria University of Wellington

Media Badger (2011) , www.mediabadger.com/2011/10/senior-citizens-and-social-media/

Westin A. *PRIVACY AND FREEDOM* by Vol. 22, No. 1 (OCTOBER, 1969), pp. 101-106

Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixie Hawtin, (2012) Global Survey oj Internet Privacy and Freedom Of expression, Unesco Series On Internet Freedom

Solove D. (2002), Conceptualizing Privacy Daniel, California Law Review Volume 90 , Issue 4 Article 2 July 2002

Stokes Natasha Stokes (2014), The Worst Apps for Privacy Retrieved http://www.techlicious.com/tip/the-worst-apps-for-privacy/

Liu H. and P. Maes. Interestmap: Harvesting social network profiles for recommendations. In Beyond Personalization - IUI 2005, January 9, San Diego, California, USA, 2005

Yao M. , R. Rice, and K. Wallis.(2007) Predicting user concerns about online privacy. Journal of the American Society for Information Science and Technology, 58(5):710–722, 2007.

Web- Sites

http://www.huffingtonpost.com/jeffrey-evans/top-5-privacy-violations-_b_802615.html

http://socialnetworking.lovetoknow.com/What_Types_of_Social_Networks_Exist)

http://www.socialmediatoday.com/social-networks/2015-04-13/worlds-21-most-important-social-media-sites-and-apps-2015

http://www.statista.com/statistics/

http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/

http://www.techlicious.com/tip/the-worst-apps-for-privacy/ by Natasha Stokes on December 18, 2014

http://www.informationweek.com/software/social/linkedin-faces-lawsuit-over-privacy-violation/d/d-id/1278588