How Much Privacy We Still Have?

Ayn Nur Azhana Binti Azhar Amanullah[1], Nur Faizah Binti Ab Aziz[2], Maya Novia Sari[3], Jamaludin Bin Ibrahim[4]

Department of Information Systems, Kulliyyah of Information and Communication Technology,
International Islamic University Malaysia

Abstract: ***Privacy is very crucial to users nowadays especially to the OSNs or SNSs, cloud storage, and e-commerce sites. In the era of millions of users throughout the world, it becomes increasingly difficult to protect their private information from being exploited by attackers. Revealing too much of information on those sites will give negative impacts to users as their personal information might be stolen from third parties. In this paper, we analyze the private information whether to reveal or not regarding the privacy concerns, information leakage, and how to improve privacy. Location is considered as private data that the users do not want to reveal as it might contain private and confidential information. A new technology called Geo-location enables our device to detect and record the information. Therefore, the security awareness among the users is important in mitigating the security issues. Thus, this paper discuss on the privacy level that we still have in OSNs, cloud storage, geo-location, as well as in reality.***

Keywords: Private information, information security, privacy, geo-location, security, security awareness, OSNs, SNSs, cloud storage, e-commerce

1. Introduction

Private information or personally identifiable information (PII) defined as information that can be used on its own or associate with other information to identify, contact, or locate a single person [18]. In other words, PII is used to identify an individual in context. According to NIST [3], PII is defined as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." This section will analyze on the privacy concern in online social networks (OSNs) and cloud storage, the information leakage in OSNs and cloud storage, and how to improve privacy. The rise of smartphones and social media show that geo-location has become more popular. Geo-location technology is globally use as the app which is attached to mobile devices in our pocket and capable of displaying map information and identify the real-world geographic location of a person or object. For privacy reasons, user will be asked for permission to report location information but how secure is the technology to protect the privacy. This module will express more on the individual privacy when using geo-location service and the security involves protecting individual privacy.

Nowadays, nearly all internet users are members of some social network sites (SNSs) or e-commerce sites. This context results in enormous shift on the patterns of information exchange over the Web. Instead of being consumers, users are also become information providers to those sites. They must have some expectations on how their information is used. However, there are possibility on mismatched users expectations and reality on their privacy settings and security. This can also result in a significant privacy violations that need to be avoid.

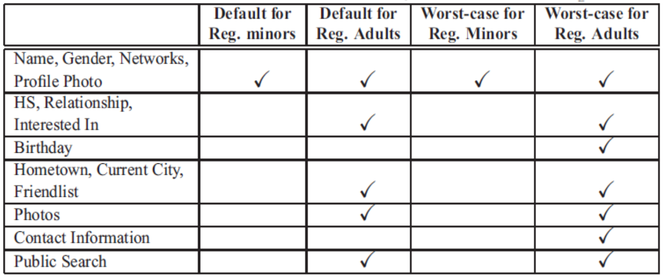
This research was conducted using literature review methodologies. The literature review was started with a list of online academic journals and conferences from diverse online databases. To ensure the most relevant and better quality articles, researchers went backwards to review other works cited in the reviewed articles. Researchers focus on reviewing journal and conferences in the field of information and privacy security.

2. Private Information – To Reveal Or Not To Reveal

A. Privacy Concern in OSNs and Cloud Storage

The US government has established Children's Online Privacy Protection Act (COPPA) to protect the privacy of children under 13 years old [15]. The act describes on what a website operator must include in a privacy policy, how to seek parents' consent, and what responsibilities an online service provider has to provide children's safety and privacy. Online Social Networks (OSNs) take additional measures to protect the privacy of minors (people under 18 years old in the US) [15]. For example, Facebook bans children under 13 to sign up, does not list minors when searching users' high school or city. A third-party can explore and develop profiles for minors, ages 14 to 17 in that particular city by profiling all the high schools in a city. Hence, use the profiles to sell the profiles, to spear phishing attacks on minors, and physical attacks such as kidnapping and set meeting for sexual abuse. In Facebook, registered minors and registered adults have different view in terms of privacy.

Table 1 [15]: Facebook Default And Worst-Case Information Available To Strangers



	Default for Reg. minors	Default for Reg. Adults	Worst-case for Reg. Minors	Worst-case for Reg. Adults
Name, Gender, Networks, Profile Photo	✓	✓	✓	✓
HS, Relationship, Interested In		✓		✓
Birthday				✓
Hometown, Current City, Friendlist		✓		✓
Photos		✓		✓
Contact Information				✓
Public Search		✓		✓

Licensed Under Creative Commons Attribution CC BY

Table 1 shows the default information of a user available to a stranger and when the user configures the setting for maximum sharing (worst-case). The check in the box indicates that the information is available to the stranger. For example, when a stranger visits a registered minor's profile, only limited information is available such as user's name, gender, networks joined, and profile photo. Besides, the contact information is also not visible to strangers such as "Message" button on the profile.

Security and privacy threats usually focused on enterprise cloud adoption and it gives impact to end-users' privacy and expose users private documents to hackers [4]. The examples of data storage are Dropbox and Google Drive by simply moving the users' data into dedicated online storage systems. Privacy activists argued that users' expectation of privacy indicated that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third-parties [4]." According to the studies on Internet privacy attitudes and social networks in California [4], most of the participants denoted high and medium privacy concerns on cloud storage and only 20-25% of people "unconcerned". The studies also found that users do not read the privacy policies beforehand. Moreover, they assumed that if a website has privacy policy then, the data will be kept private from selling the user data to third-parties. Furthermore, the participants felt that the availability of the data is better online in case of the computer crashed but for sensitive documents, they strongly preferred to keep them offline [4]. In the online survey conducted by Iulia et al. [4], the respondents had to choose between Company A and Company B where Company A offered the service for free, but they may sell personal information documents while Company B costs 20 USD, but they will not sell any personal information documents.

Table 2 shows that Company B had resulted on higher percentage of 79.1% compared to Company A which is only 20.9%. This survey concludes that the users are willing to pay as long as their data is kept privately from third-parties. The respondents that opt for Company B might not have private or sensitive information to be stored.

Table 2 [4]: Willing To Pay For Privacy: "Which Company Would You Choose To Store Your Data, And Why?"

CompanyA: free, may sell user data	
– It is free.	3.0%
– I don't have sensitive data anyway.	11.4%
– I never know what they do with my data.	6.5%
	Total: 20.9%
CompanyB: costs $20, won't sell data	
– I value my privacy.	37.3%
– If the price was lower.	9.7%
– If they are trustworthy.	32.1%
	Total: 79.1%

B. Information Leakage in OSNs and Cloud Storage

Online Social Networks (OSNs) have rapidly growth from time to time from Friendster, Myspace, Twitter, to Facebook and more third-party take the opportunity from OSNs to discover data. The information is available to strangers based on different criteria searched by the strangers. There are a lot of OSNs users who do not aware of personal data revelation since their information is to be known by public [19].

Fig. 1 demonstrates the overall network of participants' identity disclosure such as name, photo, friends, age, gender, and location (city, states, and country). People have to reveal personal information such as name, date of birth, and contacts on their profiles to be matured and effective [19] without realizing that the communication on the Internet are more exposed compared to face-to-face communication. Therefore, user needs to disclose partly of their personal information instead of disclosing all of their personal information as a security measure.

In a study on privacy concerns for consumer cloud storage, the participants were asked on who might be able to see their cloud storage data except for themselves and several of them said "anybody" could see it [4]. The aspects of hackers, storage providers, and goverments are also been examined during the interview and can be concluded as follows [4]:

1) Hackers: All participants except for one person believed that it would be very easy for a hacker to exploit their data from the cloud.

2) Storage Provider: All participants except for one person were aware that their storage provider can access their data.

3) Governments: The two participants said that the police or government cannot access their account and believed that they are just a normal person as in they are not a criminal or wanted person of the country.

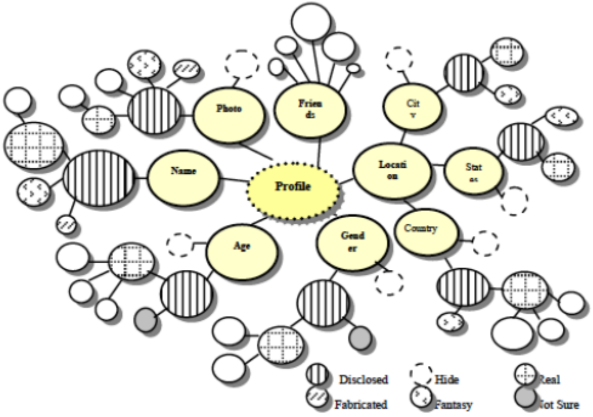


Figure 1: An overview of personal information disclosure [19]

C. How to Improve Privacy?

Carnegie Mellon University provides world-class opportunities for security and privacy research and hosts one of the largest academic security and privacy research centres in the world (CyLab) [6]. Carnegie Mellon proposed the technologies to improve privacy such as user authentication, security of long passwords, and online single-sign on. The proposed technologies described as follows [6]:

1) User Authentication: User authentication is needed especially to make online transactions where the user must first authenticate in order to provide some privacy in the process. The solution for authentication problem is to use biometric authentication where the users provide unique characteristics such as fingerprints and iris scan to allow a different party to confirm their identity and check whether they are authorized person for the particular transaction.

2) Security of Long Passwords: Longer passwords contain more characters and it is hard to crack by brute-force attack. Long password modelled as “noun-verb-article-adjective-noun” is a common construction such as “Mary had a little lamb” that the attackers would guess for the common construction. As an alternative, try to construct “verb-verb-article-article” as it is probably rare and the attackers would not try for such combinations in guessing a password.

3) Online Single Sign-On: Single sign-on eases users from remembering many passwords and also eases service online providers from developing and maintaining their authentication mechanisms. Google and Facebook have started using this single sign-on. However, it will potentially cause to privacy where the identity provider may send a service provider data that the service provider would not have known.

There are some measures to be taken by the governments as well in order to ensure the privacy issues are reduced and controlled in future [17]:

i. The government should take issues regarding to high-tech related crimes such as private data exploitation into considerations whenever to conduct negotiations of mutual agreements.
ii. The government should make workable solutions to ensure the freedom and private lives of people are well protected.
iii. One country should collaborate with another country to develop new technologies that are tailor made to combat the privacy information from being stolen.

In short, the privacy in OSNs and cloud storage can be considered as less privacy. This is due to the reason that the information uploaded on those OSNs and cloud storage can be easily stolen by the third parties no matter how protected the sites are. For example, in Facebook, they gather users’ information by keeping track of pages users have “Liked” and also via the interactions among users. Advertising is one of the strategies of the marketers to gain revenue. Therefore, the users’ information might be stolen by the marketers through OSNs to be shared as a target group for their advertisement.

On the other hand, lack of privacy and over-sharing on OSNs and cloud storage will endanger the users indirectly. Users are tend to share their personal information such as real name and date of birth which is fine to show the maturity of the users and also ease their friends to find them in OSNs; however, the private information such as phone number and address number should not be exposed to public as the person with bad intentions might steal the information and do something bad after that. Also, the users should not share whatever personal status on their OSN as it will open up the chance for the bad people. For example, the Facebook on Twitter status could get you robbed by updating status like “I’m going out tonight,” this will simply provide information to the burglars to enter the house when the person is not home. Therefore, it is good to think twice before updating status on the OSNs and ensure that the profile is set to private and do not accept friend request from unknown person. To avoid information from being stolen in cloud storage, do not simply upload the important and private documents such as working documents or personal bio data that contains private information. It is good to keep those documents in users’ personal drive instead of put it online as the privacy nowadays are very less no matter how secure the sites are.

3. Privacy And Geo-Location

A. What is Geo-Location?

Location is considered as private data that we as a user does not want to reveal as it might contain private and confidential information. Location privacy is based on the idea that the users should be able to control the location information to be disclosed [10]. Geo-location is a term used to describe the capability to track and record our location and other people are located. Geo-location information can be obtained in a number of ways including information about a user's IP address, MAC address, Wi-Fi connection location, or GPS coordinates [16].

Geo-location is not a gadget; it is an application to be used for tracking our device. Nowadays, geo-location applications disclose our location to several parties including our personal information. We can see the growth in geo-location technology and digital mapping with the rise of Google Earth, Google Maps, and other services. Apps like Foursquare and Facebook Check In have been around for years. Google Location is a geo-location service by Google Maps for mobile device that enables us to share our location with others as well as see their locations. Typically, geo-location application work in two ways: First, we report our location to other users, and second the application will relate real-world locations to our location [12]. Geo-location application used on mobile devices provide a wide experience compare to fixed device like desktop because the relevant data you send and receive changes as your location changes.

In some country, geo-location technology can locate emergency call when emergency happen. Location tracking system helps the response team to track the exact victims’ location. Geo-location technology offers accuracy, availability, and coverage as the technology is attached to our devices [9]. Moreover, application like Google Maps if used properly can be very useful in business. This application can make us more efficient and increase our visibility online. It provides business opportunity as company will use geo-location based application to track business’s mobile assets to improve supply chain management and create more meaningful engagement with consumers or potential customers. It is important to make sure items or products arrive to the receiver as expected. Furthermore, geo-location applications are designed to encourage communication and companionship. Social network site with location tracking system allow people to post and share personal information with a geographical content. Parents can now track and know their children’s location.

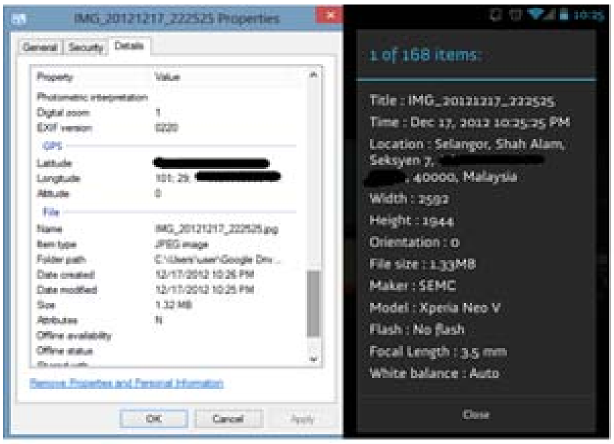
Licensed Under Creative Commons Attribution CC BY

B. Geo-Location and Privacy

Many navigation software help in navigating our destination but do we realize our movement is recorded somewhere. Geo-location technology makes our device detected and our information recorded. There are many applications that we use or installed in our device transmit device information, contact information and location to the developer or third party such as data aggregator. We not aware of the activities which expose us to danger by uploading our sensitive data without us realize it. Algorithm can be applied to that data set to make assumption about us in ways that could benefit or disadvantage us [1]. Privacy-aware geo-location assumes that private positions can be associated with environmental fingerprints and that those fingerprints can be recognized in real time [7].

The protection of the position information (location privacy) is a major issue in Geo-location [5]. This concern is due to the fact that geo-location providers may not have the ability or interest to protect the position information conveyed by the requesters of the service, while position is kind of personal information that, as such, requires special care [7].

In most countries, data about location cannot be collected without providing users with privacy guarantees. However, during online, users have only limited control over the disclosure of their location information, as they can either accept or deny consent as shown in Fig. 3. The worst situation is when user did not notice their information is recorded or tracked by the third party. Collected location data are exposed to a variety of risk such as fraudulent access. Fraudulent access can be understand as getting access into information without authorization or exceed the authorized limit.



IMG_20121217_222525 Properties

Property	Value
Photometric interpretation	
Digital zoom	1
EXIF version	0220
GPS	
Latitude	[redacted]
Longitude	101; 29; [redacted]
Altitude	0
File	
Name	IMG_20121217_222525.jpg
Item type	JPEG image
Folder path	C:\Users\user\Google Driv...
Date created	12/17/2012 10:26 PM
Date modified	12/17/2012 10:25 PM
Size	1.32 MB
Attributes	N
Offline availability	
Offline status	

1 of 168 items:

Title : IMG_20121217_222525
Time : Dec 17, 2012 10:25:25 PM
Location : Selangor, Shah Alam, Seksyen 7, [redacted] [redacted], 40000, Malaysia
Width : 2592
Height : 1944
Orientation : 0
File size : 1.33MB
Maker : SEMC
Model : Xperia Neo V
Flash : No flash
Focal Length : 3.5 mm
White balance : Auto

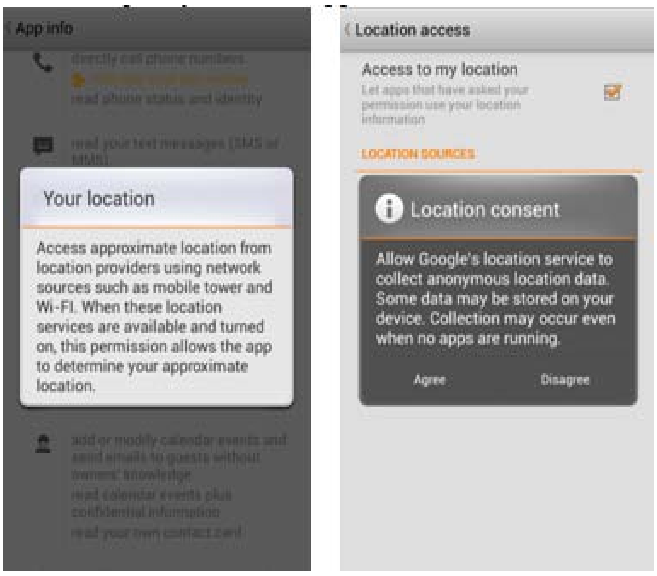
Figure 2: Location information in picture

As the devices that people use to connect to the Internet become more mobile, information about our location has become a critical piece of context that applications can use to customize services to the needs of users [2]. This means that many people feel threatened by the idea that they are being "followed" or that their location would be revealed to strangers or even friends that could compromise this information. Even when we capture our moment, our picture will include accurate location information by displaying both latitude and longitude in the picture properties as shown in Fig. 2.

Google Chrome is a freeware web browser developed by Google Inc. Google Chrome as in its site states that it never shares our location without our permission. By default, whenever we want to use our location information, Google Chrome will alert us by showing a prompt message at the top of the page. Our location is sent to the site only if we click **Allow** in the prompt. If we allow Google Chrome to share our location, the browser will send local network information to Google Location Services to get an estimate of our location. The browser can then share our location with the requesting site [11].

The ◉ location icon appears in the address bar to remind that we have permitted the site such as a map to access our location. To see more details or to clear location permissions for the site, just click the icon [11]. In this situation we should examine a website's privacy policy before sharing our location.

Smartphones today have a GPS system attached, and the system uses satellite data to analyse our exact position usually when we are outside and the signal is available, which services such as Google Maps can then locate our location accurately. Nevertheless, the collection of data may happen even we did not request the service and it is vulnerable to us as "someone" is tracking our steps and activities. The risk is bigger for those who are not aware of this as they assume their privacy and safety are protected. This is the situation where privacy breaches using geo-location.



directly call phone numbers
read phone status and identity
read your text messages (SMS or MMS)

Your location

Access approximate location from location providers using network sources such as mobile tower and Wi-FI. When these location services are available and turned on, this permission allows the app to determine your approximate location.

add or modify calendar events and send emails to guests without owners' knowledge
read calendar events plus confidential information
read your own contact card

Access to my location ☑
Let apps that have asked your permission use your location information

LOCATION SOURCES

Location consent

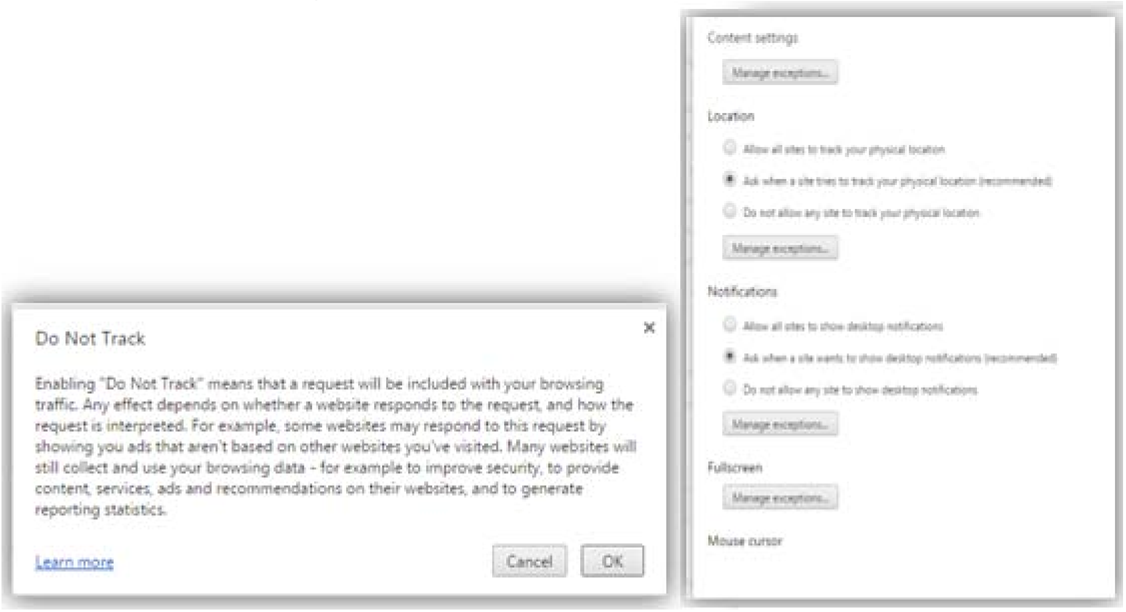
Allow Google's location service to collect anonymous location data. Some data may be stored on your device. Collection may occur even when no apps are running.

Figure 3: Smartphone location consent

Privacy geo-location is not possible to be fully protected but we as user can minimize and control the exposure as shown in Fig. 4. Consumers should be able to decide when we are comfortable sharing our information and avoids sending unexpected notifications. Make sure we are always aware and know about the safety of our smartphones as security systems can be hacked by a human carelessness. Avoid installing any application manually; otherwise download through Google Play or App Store. Read and understand the meaning of "permission" displayed each time we want to install application. Turn off the tracking capability through the settings menus. Turning off tracking means those

Licensed Under Creative Commons Attribution CC BY

applications have no access to our locations. The important is minimizing the use of public hotspots and only allows people we trust following our social network site activities. The developer shall consider offering a Do Not Track (DNT) mechanism for smartphone users [1]. It supposes to allow user to choose to prevent any tracking when they navigate among applications on their gadget.



Do Not Track ×

Enabling "Do Not Track" means that a request will be included with your browsing traffic. Any effect depends on whether a website responds to the request, and how the request is interpreted. For example, some websites may respond to this request by showing you ads that aren't based on other websites you've visited. Many websites will still collect and use your browsing data - for example to improve security, to provide content, services, ads and recommendations on their websites, and to generate reporting statistics.

Learn more

Cancel OK

Content settings

Manage exceptions...

Location

○ Allow all sites to track your physical location

● Ask when a site tries to track your physical location (recommended)

○ Do not allow any site to track your physical location

Manage exceptions...

Notifications

○ Allow all sites to show desktop notifications

● Ask when a site wants to show desktop notifications (recommended)

○ Do not allow any site to show desktop notifications

Manage exceptions...

Fullscreen

Manage exceptions...

Mouse cursor

Figure 4: Privacy setting

New technologies can now record our every movement, revealing private information about our life. Without the right protections in place, data aggregator or third party can gain access to this information. Location privacy is dependent on our minds and will remain in the headlines. Therefore, how much location privacy we still have? We can say that we still have location privacy as long as we endeavor to keep our information by taking preventive action from data theft.

4. Privacy – Expectation vs. Reality

Sharing personal information has become a common thing nowadays, especially with the existing online social network and e-commerce. An individual is often willing to provide their personal information in exchange for perceived benefits or for services without understanding the importance of security on their personal information. Researchers defined the meaning of personal information differently. In European Network and Information Security Agency article, personal data can be defined as broadly as any information that can be linked, either by itself or in combination with other available information, to uniquely identify a natural person [14].

Technology nowadays allows the storing of any information on the internet. Sometimes, people may not include their identifiable information such as phone numbers, email, and home addresses in their social network sites. This occurred because they often tried to keep their information discreet from potential thieves. However, e-commerce sites usually possess this kind of personal information of their users. Moreover, some social network sites even allow users to include information regarding their activities and their locations. This kind of information may lead to privacy implications. Many researchers have shown that people will disclose more personal information online than the will face-to-face. Not only do people readily self-disclose in online experimental settings, but they often also disclose personal identifiable information when this is requested by a website [8]. Such broadcast ability is very concerning regarding the possibility of their information being misused.

In terms of social network sites, some of the existing social networking sites such as Facebook and Twitter allow users to manage their privacy settings of uploaded content (photos, videos, statuses, links and notes) according to their own preferences. Others sites such as Path even set their users' contents to be displayed only to their friends for more privacy protection. By this privacy settings provided by SNSs, users expect their information to be protected and only available to their chosen groups of people [13]. However, most of users even are not aware of the existence of privacy settings. Unless they modify them, their information is basically open to the public.

On the contrary, it is an issue that the anonymity of the internet often spurs people to be more open than they would in face-to-face conversation. Data aggregation may be occurred using social network sites. By using a range of different SNSs, people may be able to build up a picture of an individual. The danger resulted by such activity could be vary from the possibility of identity thefts or malicious attacks.

Privacy concerns in e-commerce exchanges are evolving issues in customers' perspectives, reflecting both marketing and public policy perspectives. Technologies nowadays allow companies to efficiently store and exchange consumer data that are useful for their marketing strategies such as consumer profiling [13]. Private information is one of the sources of profit for companies which may lead to privacy concerns. Most customers are aware that their personal information is being collected for commercial purposes.

However, they might not acknowledge on how, why, or what it is used for. Customers' information could be extracted without their consent and could be passed or sold to third parties. This is in contradicting to what consumers expect their personal information to be used by the companies they trusted.

By looking at the above problems, we can say that people who are active in social networking sites have only little privacy left. Social Networking sites are the central of private information. It is designed for communication and social purposes that involves spreading information about a person. People use SNS deliberately to disclose their own basic information and activities for the reason of communicating with their friends and maintaining their social life. This reason contributes a lot in making their private information available on the internet. Thus, their SNS activities and updates will limit and lower their own privacy.

E-commerce sites also have the potential of exposing their users' privacy. It possesses more critical data such as credit card no., postal address, and email address. However, due to strong IT policies and regulations, many still believe that their private information will be protected. Nowadays, many SSL certifications available to ensure the sites are trustworthy and safe. Therefore, in reality, if the users' are cautious in using only the trusted sites, they will still have their privacy protected from unauthorized personnel.

5. Conclusion

In the nutshells, the users of OSNs and cloud storage especially in Facebook, Google Drive, and Dropbox need to realize that their private information can be exploited easily by the attackers with any means. Children's Online Privacy Protection Act (COPPA) has been established by the US government to protect the privacy of children under 13 years old. The privacy concerns among users are high when most of the users of cloud storage are willing to pay for the storage as long as their data can be kept privately from other parties. The users are also aware on the information leakage on OSN as they have already know that beside them, there are other "person" that is able to see their private information but they do not bother since they are not "wanted" people of the country. So, they assumed that nobody might exploit their data. Moreover, there are proposed technologies in improving privacy such as user authentication, long passwords, and user single sign-on. However, further studies need to be done in order to ensure that the technologies are equipped with high security measure.

With over 1 billion users connected through OSNs, the users' privacy are becoming more important and the individual information is not secure anymore as it is put online. The information can be easily stolen by third parties as the technology is growing up, the knowledge of such people (hackers or burglars) are also increase from time to time that made them knowledgeable enough to exploit one's data.

Furthermore, geo-location provides the location of a device and generally used in a variety of applications to help locate users. Regardless, what is most important, we must always be aware of everything we do. In this world, we are not aware that we have to expose ourselves to danger. The general right to individual privacy guarantees the integrity of an individual's. The purpose of the general right to individual privacy is to provide more flexible and comprehensive protection than that guaranteed by the traditional fundamental freedoms. Clear policy and standard about application developer and other third parties should amend to protect community fraudulent access.

In order to mitigate any potential information security risks, it is important to raise awareness to people. Users' expectations of their privacy security may not match the reality. They often lack of information on what, why, and how their information is actually being collected and used. People are unpredictable. It is meaningless to have the latest state of the art of security technology if the people factor is not mitigated. There must be a strong security policy that includes the convergence of physical and logical security at any level. The created policy should be supported and distributed to the users because most of them failed to read user agreement and privacy policy properly. It should also be maintained because security issues and requirements grow along with the growth of technology.

People may not have much privacy left in terms of social networking because they disclose their own private information. Once they update and safe it on SNS, It will be available on the internet to be seen by other people. Everything that users post to websites can be tracked, and the Internet is always watching. People are currently live in a surveillance state that is growing more efficient and eerily omniscient by the day [20]. Thus, their privacy becomes harder to be protected.

However, the existence of IT Policy, Laws and Regulations may lessen the possibility of misused information. This is especially important in E-commerce sites, because it is sites that stored a very critical and significant data. Therefore, in terms of E-commerce, people may still have their privacy protected; provided they use it with cautions. Again, does privacy still exist? As a user, we can choose and determine our level of privacy and take action to ensure that our information is safe.

References

[1] A. Lori, "Where's Waldo?:Geo-location, Mobile Apps, and Privacy," *The SciTech Lawyer*, vol. 9, 2013.

[2] B. Richard, W. James, and D. Martin, "Services, Location Geo-location and Location-Based," *IETF Standards Update*, pp. 102-108, Apr. 2011.

[3] E. McCallister., T. Grrance, and K. Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. National Institute of Standards and Technology (NIST) U.S. Department of Commerce, Apr. 2010.

[4] I. Ion, N. Sachdeva, P. Kumaraguru, and S. Capkun, "Home is Safer than the Cloud! Privacy Concerns for

Licensed Under Creative Commons Attribution CC BY

Consumer Cloud Storage," *Symposium on Usable Privacy and Security (SOUPS)*, Jul. 14, 2011.

[5] J. I and W. R.T, "Location-Based services," *Commun. ACM*, no. 51, pp. 65-69, March 2008.

[6] L. Bauer, A. Acquisti, N. Christin, L. Cranor, and A. Datta, "Efforts to promote online privacy via research and education at Carnegie Mellon," Carnegie Mellon University, May 21, 2014.

[7] L. D. Maria, "Third party geo-location services in LBS-privacy requirements and research issues," *Transactions on data privacy*, no. 4, pp. 55-72, 2011.

[8] L. Humphreys, P. Gill, and B. Krishnamurthy, "How much is too much? Privacy issues on Twitter," *Conference of International Communication Association, Singapore*, 2010.

[9] M. D. Goran and E. R. Robert, "Geo-location and Assisted GPS," pp. 123, 2001.

[10] M. Sergio, F. Dario, B. Claudio, W. X. Sean, and J. Sushil, "Privacy in geo-social networks:proximity notification with untrusted service providers and curios buddies," *The VLDB Journal*, 2011.

[11] N.A. "Google Terms of Services : Privacy and Terms," Google Inc, Apr. 14, 2014. [Online]. Available: http://www.google.com/intl/en/policies/terms/.

[12] N.A., "The pros and cons of geo-location apps for your business," Wasp Barcode Technologies, Sept. 15, 2011. [Online]. Available: http://www.waspbarcode.com/buzz/pros-cons-geo-location-apps-business/.

[13] N. Olivero and P. Lunt, "Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control," *Journal of Economic Psychology*, vol. 2, pp. 243-262, 2004.

[14] P. Druschel, M. Backes, and R. Tirtea, "The right to be forgotten - between expectations and practice," European Network and Information Security Agency, 2011.

[15] R. Dey, Y. Ding, and K. W. Ross, "Profiling High-School Students with Facebook: How Online Privacy Laws Can Actually Increase Minors' Risk," *ACM*, Oct. 23, 2013.

[16] S. Forrest, B. Vangie and S. Paul, "webopedia," [Online]. Available: http://www.webopedia.com/TERM/G/geo-location.html.

[17] S. S. Basamh, H. A. Qudaih., and J. Ibrahim, "An Overview of Cyber Security Awareness in Muslim Countries," *International Journal of Information and Communication Technology Research*, vol. 4, pp. 21-24, Jan. 2014.

[18] Wikipedia. (Oct. 27, 2014). Personally identifiable information. [Online]. Available: http://en.wikipedia.org/wiki/Personally_identifiable_information

[19] W. Binden, M. Jormae, Z. Zain, & J, Ibrahim, "Employing Information Security Awareness to Minimize Over-Exposure of Average Internet User on Social Networks," *International Journal of Scientific and Research Publications*, vol. 4, pp. 1-6, Jan. 2014.

[20] L. Pickett., " In the age of social networking, there's no such thing as privacy,", 2013. [Online]. Available: http://www.wbez.org/blogs/leah-pickett/2013-05/age-social-networking-theres-no-such-thing-privacy-107021

Author Profile

Ayn Nur Azhana Binti Azhar Amanullah, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia and azhana90@yahoo.com

Nur Faizah Binti Ab. Aziz, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia

Maya Novia Sari, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia

Jamaludin Bin Ibrahim, Senior Academic Fellow, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia

Licensed Under Creative Commons Attribution CC BY