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.

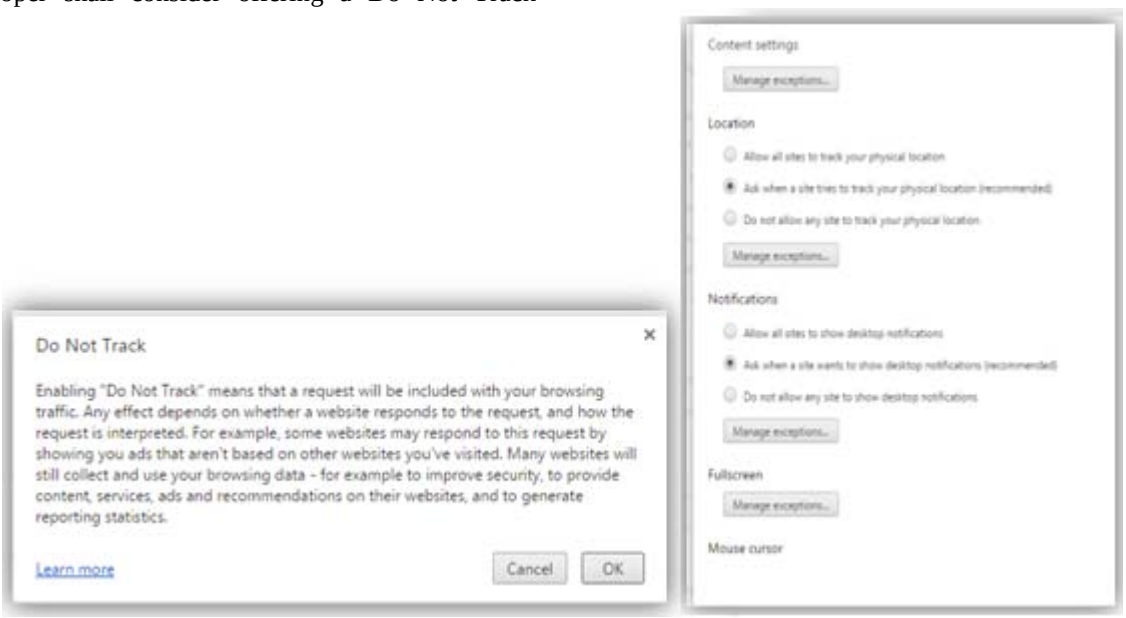

Figure 4: Privacy setting

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

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