COMP 7530 Writing assessment Part 1

Seminar topic: ‘’Global Internet Governance: Of the Internet and On the Internet’’

Student Number: ____ 15451682_____

Student Name: _____CHEUNG Saiho_____

Program: _____MSc AIS_____

Nowadays, everyone can share their information on the internet, it is the core feature of web 2.0 technologies, such as social networking platform, peer to peer file sharing service. Therefore, the internet governance is a very hot topic how to balance in speech freedom and intellectual property rights or personal privacy protection for each internet user.

In this seminar, the speaker is Mr Edmon CHUNG who is CEO of DotAsia Organisation. The topic of speech is ''Global Internet Governance: Of the Internet and On the Internet''. The speaker elaborated some idea which focuses on the three categories of data protection issues, including privacy, security and anonymity. In addition, the speaker has talked about what is the Internet Corporation for Assigned Names and Numbers (ICANN) does. This organization headquarter is found in Los Angeles, California, USA which is central administered the several key technical and policy aspects of the core internet infrastructure and the principal namespaces of network service. It has assigned the unique identifiers on the internet globally, including domain name service (DNS), Internet protocol addresses (IP) for the assignment of different internet service providers (ISPs) in every country and define the port numbers of network applications in transport protocol. Definitely, it is belonged to technical aspects and define some network service protocol policies more easily, because there has not involved the freedom of human behaviour and less changing of network technical standard. (Carvalho 2014)

However, the web 2.0 technology concept has absolutely changed all users' behaviour for using the internet, it is not just downloaded and read information from the web server in a single way. There can be contributed their information on the website and interacted with other people on the internet. As the internet has an unlimited storage and public platform around the world, nobody can be monitored or restricted to other user's behaviour what kinds of information could be shared or not. Unfortunately, it has not a global policy to protect the privacy, data distribution or control who can have the right of access permission. In addition, some bad guys can be build up the website which is provided some bad contents or promoted the criminal behaviour, such as publish copyright material illegally, kidnap, gambling, pornography movie, drugs, violence, etc. it is very harmful for teenager psychological development and social peace, but the web hosting

company cannot remove them without any judgement of the local court before. (Mueller 2007)

In the issue of security, the speaker said that the hackers have produced some computer viruses, malware and spyware spread in different kinds of internet sources, there is including the e-mail attachment, pornography movie and download illegal software website. For example, The Pirate Bay, Torrentz etc. Most of hackers can exploit the zombie network, which is contained a hundred and thousands of these infected computers to attack the network servers, such as commercial companies, banks, government computer system. They have stolen a large set of customer data with a bank account or disruptive government daily service operation, it is a typical case in the cyber-attacks of DDoS and become a huge economic loss in the country, or even in the world. Actually, all kinds of cyber-attacks must need to destroy the other computer systems via internet. On the other hand, the internet connecting speed and hardware processing power is much more powerful than ten years before, so the hackers can get more easily to paralyze the network servers operation for a short time.

In addition, the speaker has claimed that any internet users should have responsibility to prevent using these illegal materials, such as commercial software, movies and songs, etc. The author is absolutely agreed this suggestion, but it is not enough and only focused on individual view. As these websites have involved the issue of digital copyright, there must need to use the massive web storage and high speed network connection which is provided by the web hosting company, so many people can download these illegal copyright materials simultaneously. In this case, the ISP can keep track of download speed and duration of the destination sources to customer IP address. If it finds some abnormal activity, the network administrator can stop it and report to the police. By the way, the ISPs and the IT sector of government should have control right to block some known harmful or containing illegal copyright material websites and web hosts. It seems like that the Chinese government has blocked the most of the western social networking platform for the whole national network, such as Facebook, Twitter. (Bygrave &Bing 2009) Certainly, this behaviour is suppressed freedom of speech. However, these harmful websites should be access denied by ISPs for enhancing the internet safety. It is absolutely not involved the freedom of speech issue.

By US government, they have established the internet storm centre which is in charge of the academic committee. This centre is especially monitored all kinds of cyber-attacks on the internet, it has posted the information of attacker's IP and the range of port numbers by victim hosts for updating frequency. Moreover, there have stayed alert that some latest harmful computer programs or coding is spreading or appearing in the web systems, such as Trojan horse programs, threatening web script, etc. this centre has reported the detail of information about the symptom of infected computers. Thus, most of enterprises and ISPs can get more easily to update the network connection policy, it should prevent the network attack and fix system vulnerability more efficiency.

In the issue of privacy, many people have used the social networking platforms to keep contact or invite to join social events with their friends and family, they always post their life photos and comments on these platforms. The main purpose is sharing their happiness with their friend groups immediately, it is the benefit of web 2.0 and easy to build up closed human relationship during the busy daily life. (Hargittai et al 2010) However, the speaker has warned that most of young people and students like to post everything to Facebook without any filtering before, it is very high risk and bad behaviour. According to the report of Facebook usage pattern, the report has found that most of age not over 30's young people have not hidden any critical information in their profile on Facebook page, such as real name, phone numbers, date of birth, etc. Besides, their profile is opened to the public, everyone can see it, or even copy it from this page. (Fogel &Nehmad 2008)

Actually, all the social networking platforms have a person privacy setting function page which information items should be hidden by the user's profile, it is very basic concept to protect their privacy information. For example, Facebook has provided some private information policy control for the users which group of people can see their posts and profile etc. (Madden 2012) if users do not found with them from the stranger, they can ignore all the request of friendship. The author believes that all people should have a responsibility to protect their privacy for their own, because this information is belonged to themselves.

For the part of leakage information, the speaker said that the octopus card company has leakage

customer information to the third-party company. The author disagrees with it, because every person has known that the octopus card company need to collect the personal information for activating card service before. They must need to sign the privacy agreement for the company which is accepted to use for the data analysis of customer behaviour and providing special offer from other companies. It is a very fair case, this customer information is an invaluable asset for the company, it is always kept high security for data protection and restricted permission for datacenter access. (Miyazaki &Fernandez 2000)

On the issue of anonymity, the internet is a public network, everyone can post any information on the website without display the real name. This information has not approved true or fake from their source destinations, so some bad guys have produced the fake news or violence speech on the internet, such as terrorist attack, shooting threat and murder, or easy to post libelous comments about someone. It is not only even involved the ethical and moral issue, this behaviour is a serious crime and should go to jail, because this fake news must be huge society unsafety on the countries, or even around the world.

Unfortunately, most of the social networking platforms have not some content filter mechanism to monitor what content of information have uploaded by users. Although the users must need to login in the platform when they want to post something on their page, it is not an anonymous. However, they can forward or capture the part of the content on the other web page without any verification before. The speaker is very worried that this bad content is distributed other people very fast via Facebook, because the internet time shifting is very short when people can see their Facebook at any time and everywhere. It is very difficult to block this content immediately, but the Facebook should do some information auditing work and blacklist some words and web links. The author absolutely agrees with it, because Facebook can allow to post anything on the page, or even the pornography material and violence speech without any warning notices. Certainly, there is including the fake news, for example, the Hong Kong weather would be dropped down to -5 degrees during Chinese New Year holiday, it is impossible which is confirmed by the Hong Kong Observatory. Thus, the author has suggested that the social networking platforms should have kept track of user activity and implemented the content filtering function to restrict some bad information which is posted by users. (Lee et

al. 2003)

Besides, all ISPs can monitor all network activities for each user when their IT device has connected to the internet, it is not completely anonymous. Therefore, the speaker has claimed that the Google is very difficult to identify the real person when they have turned off the GPS location of their smart phone or tablet. The author does not agree with it, because the digital footprint has kept track of ISPs by users, this is an IP address. Although the IP address is dynamic to assign in the user, the ISP has recorded which IP address is used by user account in the specify of time. In addition, most of social networking platforms have kept the user‘s IP address during the login process, such as Google, Facebook, etc. it is very easy to find out the criminal when they have involved the cyber-attacks or illegal activities on these websites.

As a result, the author believes that the global internet governance policy should be started in the national government and ISP companies, because they have the important role to organize the internet infrastructure, it is not only even related to the technical aspects. The government and ISP companies have a responsibility to prevent the cyber crimes which is always happening on internet repeated again and again, it does not involve the freedom of speech problem, because the fake news, infringing goods, cyber-attacks and pornography material must be illegal and should not exist on the internet, there must be needed to monitor by the global internet governance policy.

Bibliography:

Bygrave, L. a. &Bing, J., 2009. Internet Governance. , (September). Available at: http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199561131.001.0001/acprof-9780199561131.

Carvalho, F., 2014. *Olfactory objects*,

Fogel, J. &Nehmad, E., 2008. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25, pp.153–160.

Hargittai, Eszter. "Facebook privacy settings: Who cares?." First Monday 15.8 (2010). Available at: http://journals.uic.edu/ojs/index.php/fm/article/view/3086/2589 [Accessed February4, 2017].

Lee, P.Y., Hui, S.C. &Fong, A.C.M., 2003. A structural and content-based analysis for Web filtering. *Internet Research-Electronic Networking Applications and Policy*, 13(1), pp.27–37. Available at: http://dx.doi.org/10.1108/10662240310458350 [Accessed February4, 2017].

Madden, M., 2012. Privacy management on social media sites. *Young*, p.20. Available at: http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx.

Miyazaki, A.D. &Fernandez, A., 2000. Internet Privacy and Security: An Examination of Online Retailer Disclosures. *Source Journal of Public Policy & Marketing*, 19(1), pp.54–61. Available at: http://www.jstor.org/stable/30000487%5Cnhttp://about.jstor.org/terms.

Mueller, M., 2007. Net Neutrality as Global Norm for Internet Governance. *2nd Annual Giganet Symposium*.