**INTRODUCTION**

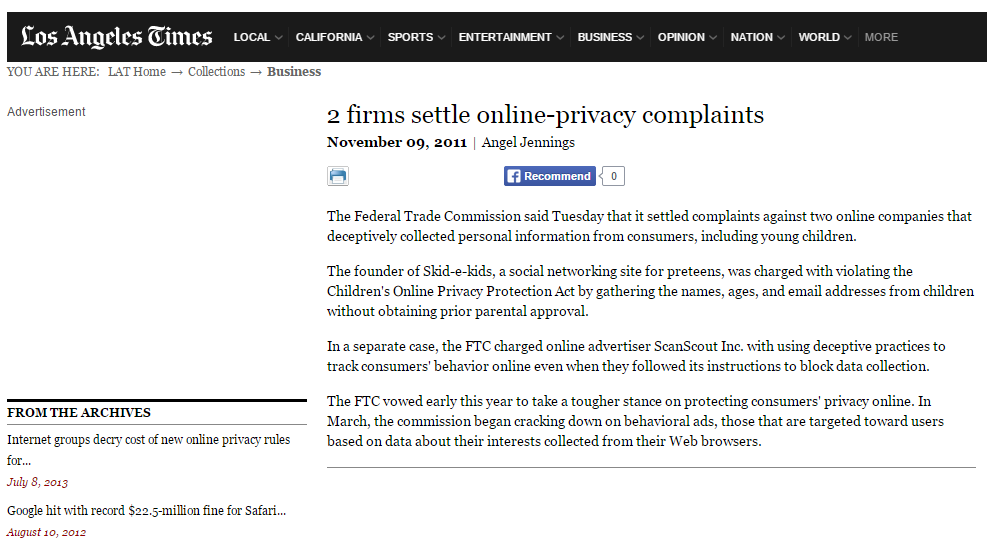
In this era of globalization, the use of internet is growing among all peoples over the world. Internet can simply describe as a global network connecting millions of computers. It uses the standard Internet Protocol suite (TCP/IP) to link several billion devices worldwide. The internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), the infrastructure to support email and peer-to-peer networks for file sharing and telephony.

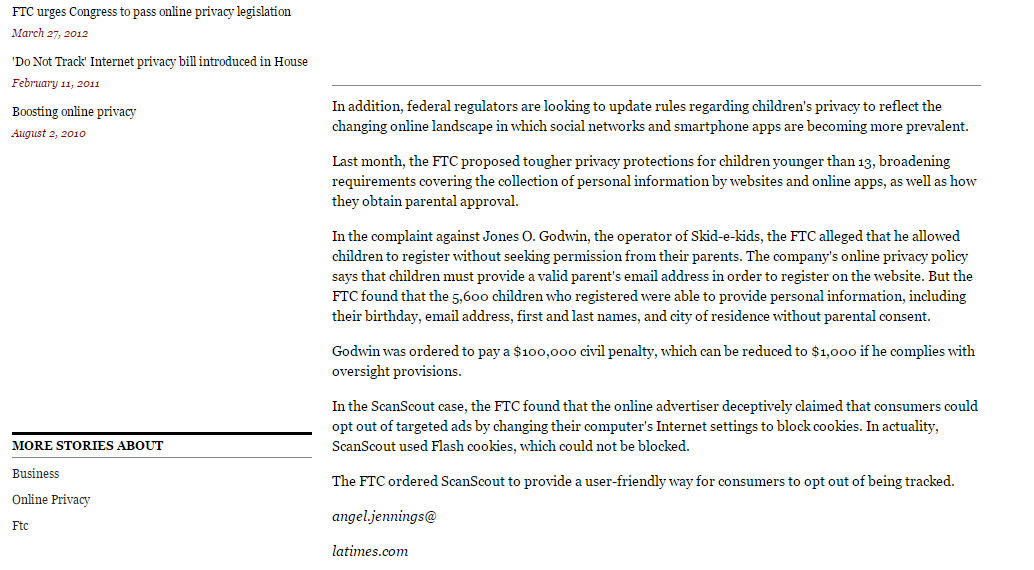
Thanks to internet basic features such as widespread and access, users have access to it anywhere and anytime. However, internet is very vulnerable to intentional attacks. This leads to uncountable computer crimes occurred such as hacking, virus creation, Denial of Service Attack (DoS), fraud and identity theft. Computer crimes such as fraud and identity theft are getting a lot of attention nowadays as it concerns the privacy of the users. For an example, there was an irresponsible user who hacked other user’s Twitter account and steals his/her information. By stealing the information, the perpetrator can gain the user’s username and password. With this advantage, the perpetrator can posted something that could be threats to other users.

These actions are against the cyber ethics where irresponsible users manipulate and also steal other users’ personal/private data or information. Those unethical actions should not occur as it could give impacts to the victims. For an example, the victim of identity theft can suffer adverse consequences if they are held responsible for the perpetrator’s action. Without knowing that his/her Twitter account had been hacked, the real owner of the account has wrongly accused for the crime that he/she did not commit. This kind of action should not happens to let internet users all around the world have access to internet without having fear about their private data security.

**CONTENTS**

1. **List the internet privacy issues**
2. Online shopping
3. Social networking site
4. iCloud
5. Online payment
6. Email
7. **Internet privacy issue article: Social networking site**

****

****

A social networking service is a platform to build social networks or social relations among people who share interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his or her social links, and a variety of additional services. Social network sites are web-based services that allow individuals to create a public profile, to create a list of users with whom to share connections, and view and cross the connections within the system.

The internet privacy issues that included in this article is about the complaints against two online companies that deceptively collected personal information from consumers, including young children. It is about privacy data and information have been steal from hacker or someone that you did not know. Data theft does not necessarily occur among adults but also can occur among children. For examples in this article, the founder of Skid-e-kids, a social networking site for preteens, was charged with violating the Children's Online Privacy Protection Act by gathering the names, ages, and email addresses from children without obtaining prior parental approval.

In this era of technology, many users misused the internet facilities to deceive people by making fake advertisement such as phishing, vishing or spamming in e-mail. For examples, phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. It can confused the others users whether they should trust the advertiser or not. For examples, the FTC charged online advertiser ScanScout Inc. with using deceptive practices to track consumers' behavior online even when they followed its instructions to block data collection. This behaviour is against the policy of ethical using internet.

**Internet Privacy Issues:**

**Advantages**

Internet users may protect their privacy through controlled disclosure of personal information. Some people desire much stronger privacy. In that case, they may try to achieve Internet anonymity to ensure privacy. Use the internet without giving any third parties the ability to link the internet activities to personally-identifiable information of the internet user. In order to keep their information private, people need to be careful with what they submit to and look at online. When filling out forms and buying merchandise, that becomes tracked and because the information was not private, companies are now sending Internet users spam and advertising on similar products.

Posting things on the Internet can be harmful or in danger of malicious attack. Some information posted on the Internet is permanent, depending on the terms of service, and privacy policies of particular services offered online. This can include comments written on blogs, pictures, and Internet sites, such as Facebook and Twitter. It is absorbed into cyberspace and once it is posted, anyone can potentially find it and access it. Some employers may research a potential employee by searching online for the details of their online behaviours, possibly affecting the outcome of the success of the candidate.

**Disadvantages**

There are many disadvantages that deal with internet privacy. In reality, people have little privacy when using the Internet. One of the disadvantages of internet privacies is theft of personal information, spamming, and virus threats. When you use the internet personal information can be stolen by many people. When you put things out online such as your name, credit card number, and where you live, these things are at risk of being used by other people.

Spamming is another invasion of privacy where you are sent e-mails that you do not want and take up space on your system. These e-mails are an invasion of privacy and can be very annoying. Virus threats can invade your privacy on the Internet and they can do much damage to a person’s computer as well.

**The Awareness of the Internet Privacy Issue**

As a social networking site service provider, the founder of the social networking site should aware that violating law can lead to legal action from the users. From the article, founder of Skid-e-kids was charged with violating the Children’s Online Privacy Protection Act. (S)he was charged because she was gathering the children names, ages, and email addresses without the children legal guardian knowing and even worst, without their permission. This action should not happen because according to law, the social networking site provider should keep users’ personal data confidential. This is because if someone’s personal data is exposed to public, peoples will manipulate the data and this action will give negative impacts to the users.

As for the online advertiser, ScanScout Inc. , their action is unethical because they were tracking online users’ behaviour without the users’ permission. Although they were doing this to promote their products, somehow this action will bother users with their continuous advertisement. Besides, they are targeting certain user by using their IP address. So, the users existence in the internet is not private anymore.

From the children parents’ perspective, the parents should give parental guide to their children when they are active on social networking site. Besides avoiding their children from communicating with strangers, parents also can monitor their children behaviour. For an example, when users made a new account, the social networking site will provide privacy policy before they can complete the sign up process. During this process, parents should read the policy together with their children so there will be no misunderstanding occurs between them and the social networking provider in the future.

Therefore, the child themselves plays a big role to secure their own personal data. They are advised not to reveal many of their personal data online because there are many hackers or even the social networking provider itself are waiting to misuse their personal data for their own benefits. The children should reveal only necessary data to fulfil the requirement to complete the sign up process.

Lastly, authorized organisation should take legal action against any social networking site that that violates the law and internet privacy policy. They also should frequently monitor the behaviour of the social networking site to avoid the social networking site misused their clients personal data.

**CONCLUSION**

In conclusion, we have Ten Commandments rules of computer ethics that we should follow to avoid problems that will occur beyond our expectations. For examples, forth commandments said that” thou shalt not use computer to steal”. Its means we should not steal other users’ works or information for our own greed. By this we have to secure our details and information from other users. Other than this, tenth commandments said that “thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.” We as an internet users should consider and also respect others privacy. If we are going to manipulate others personal information, think about the consequences first. ”What will happen if I revealed their personal information?”. Ask ourselves questions that related to the impacts of our actions.

In addition, all parties should take responsibility in order to secure internet users’ personal information. The social networking site and also the advertiser should not misuse their clients’ personal information and keep the information confidential. That information is very important to users in order to keep their privacy secure. They should not take action that benefits themselves but give negative impact to the users.

Besides the social networking site and advertiser, the users themselves should aware of this concern because they are the one who reveal their personal data to public. They are advised not to easily reveal their personal information in social networking site because once they revealed their personal information, the information will remain in the internet forever. Although the users have deleted the information, other users might have save the information without the legal user knowing.

And of course, authorities should concern about this issues because if this issues become a global problem, it will be hard to overcome this issues. So, besides tighten the law, they also enforce the law so that any social networking site and advertiser will not violates users right. They should handle any misuse issue immediately so that in the future, none of the issues arise.

REFERENCES

<http://cyber.law.harvard.edu/privacy/Module3_Intronew.html>

<http://articles.latimes.com/2011/nov/09/business/la-fi-online-privacy-20111109>

<http://en.wikipedia.org/wiki/Social_networking_service#cite_note-1>

<https://sites.google.com/a/cortland.edu/privacy-and-the-internet/home/disadvantages>