SUNWAY

INT'L BUSINESS SCHOOL

Programme Name: _____**BCS HONS**_____

Course Code: __**CSC 1015**_____

Course Name: _____**Ethics and Professional Conducts**_____

Individual project

Date of Submission: _____**5/02/2021**_____

Submitted By: **Submitted To:**

Student Name: **CSC_1015_Dipesh Tha Shrestha**   Faculty Name: **Khushal Regmi**
IUKL ID: **041902900028**   Department**: LMS**

Semester**: Third Semester**

Intake**: September 2019**

1. **Now a day's social media e.g. Facebook, twitter, Instagram, sagoon is being popular in Nepal. You can put your private data, photo and other location tracking information at social media platform. It my sometimes violate one's privacy.**

As we know, Social media refers to the means of interactions among people in which they create, share, and/or exchange information and ideas in virtual communities and networks. Social media is a computer-based technology that facilitates the sharing of ideas, thoughts, and information through the building of virtual networks and communities. By design, social media is Internet-based and gives users quick electronic communication of content. Content includes personal information, documents, videos, and photos. Users engage with social media via a computer, tablet, or smartphone via web-based software or applications.

A. **How can those all social media application may violate one's privacy.**
Answer: Social media have become extremely popular in recent years, and their widespread adoption has led to the presence of huge volumes of users' personal information on the Internet. The ever-increasing number of social networks' users on one hand and the massive amount of information being shared daily on the other hand have encouraged attackers to develop and use different techniques to collect and analyze such information for a number of malicious purposes, including *spear-phishing* attacks and *identity theft*. Users are not even aware of the disclosure of their personal information through their profiles. Leakage of a user's private information can happen in different ways. There are countless cases of data being harvested without an individual's knowledge, profiles being created based upon social media activity, accounts being hijacked and so forth. Some social media application can involve on tracking people's activities online and harvesting personal data and conversations from social media, job websites and online forums. In general, social media platforms, which collect and store huge amounts of personal information with limited governmental oversight, serve as attractive targets for bad actors seeking to use that data to perpetrate fraud and theft.
Example of how social media application may violate one's privacy is:
Facebook apps leaking personal data.

It has been reported several times that certain Facebook apps are leaking identifying information about those who are using them, to advertising and Internet tracking companies. And without the users having a clue!

B. **There are privacy risks at Social media. Explain your own answer about the privacy risks**.

Answer:

As we know, Privacy risk is the potential loss of control over personal information. There has been an uptick in social media users' concerns about their privacy. Many people have expressed concern about data leaks, prompting them to rethink their social network activities and the security of their personal information. With today's social media privacy issues and problems, experienced cybersecurity experts will play a critical role in safeguarding the data and personal information of social media users.

Some of the privacy risk at social media are:

Information leaks

This is relatively well known as a data privacy breach. Offenders include technology giants such as Facebook and WhatsApp. In 2018, an attack on Facebook's computer network left the data of 50 million users exposed. This was the biggest security breach in the history of the company, leaving users questioning the values of the platform regarding privacy and security.

Phishing

Phishing is one of the most popular ways for criminals to access sensitive personal information. A phishing attack sends an email, text message, or phone call disguised as a message from a legitimate entity. There are Messages persuade recipients to share personal data including passwords, banking records, or credit card numbers. Phishing attacks are most often carried out via social media sites. Typical examples of Facebook phishing messages are "look what they're saying about you…" and "is this video yours?" alongside a link. This is a typical way that

criminals gain access to a variety of personal information. This can include passwords or financial information.

Social tracking

Social media platforms tend to track various things about the way that you use these networking sites. For example, the people that you follow or add as a friend, the posts you like, the statuses or photos you post and also the profiles that you visit the most. They can analyze this activity to find out more about the type of person you are and what content can be fed to you.

Data collection and analysis

Data analysts can create profiles for you through the information that you post on your social media profile. By analyzing the type of websites you visit, adverts you click on and your personal information, analysts determine the type content that is likely to interest you. This information can then be sold to various businesses for their financial benefit.

C. **Suppose you are hired to develop the Nepali Social media site like facebook, being developer what technical aspects you can implement to the person's privacy and how you can minimize the privacy risks.**

Answer:

If I was hired to develop the Nepali Social media site like Facebook, being developer I will implement following technical change or adjustment to the person's privacy and minimize the privacy risks.

I. **I will have a strong privacy policy.** Customers/user need to know that we are protecting their information. We will make sure we have a policy they can refer to explaining how we are keeping personal information safe. We will be straightforward with customers about the consumer data we collect and what we do with it. Being honest with them will help you build consumer trust and show that we value their data and are working to protect it. So, I will make strong privacy Policy.

II. **I will collect Minimum Data and Information.** The more valuable information we have, the bigger a target we might be. Avoid using social

security numbers or other personal information for customer identification. Opt instead for log in identification and passwords. More layers of identification help keep attackers from being able to simulate users. Consider deleting personal information that we don't really need. So, I will collect minimum data from the user of my social media site.

III. **I will Enable firewalls and antivirus protection.** Firewalls and antivirus protection are basic security measures to safeguard our data. While firewalls help to prevent unauthorized access, antivirus software helps prevent, detect, and remove harmful programs from our computer. Without these in place, we could have vulnerabilities in our system that we aren't even aware of.

IV. **I will Use multiple layers of security.** I will work with an IT professional to ensure your databases, network, and website are as secure as possible. Include multiple layers of security on your website, as this is typically the first area of attack from cyber criminals. Spam filters will weed out malware and phishing scams. Employ a firewall to keep criminals out and sensitive data in.

V. **I will make require our customers to utilize strong passwords** whenever they create online accounts.so is will protect the user form hacker.

VI. **I will scan all new devices. I will** make sure to scan all USB and other devices before they are attached to our network because USB and other devices may have virus which may steal data from our database.

VII. **I will Pay attention to software and hardware updates**. I will Make sure all of our devices including computers tablets and smartphones are protected with *comprehensive* security software. I will Always update our apps and operating systems when new security updates are released.

VIII. **I will educate my employees**. As we know, Employees are often the handlers of customer data. They therefore need to be kept up-to-date on how to protect that information to make sure it does not accidentally land in the wrong hands. They should be educated about the newest fraud

schemes and urged to employ best practices such as not responding to or opening attachments or clicking suspicious links in unsolicited email messages.so I will teach this how to use the software and other.

D. **As Instagram regularly introduces new services, new ways to share with friends and stay up-to-date on their activities. Several times, Instagram seriously misjudged how members would react and made poor choices. Do you think that new developing social media site should introduce such features turned "on" for everyone? Justify your own answers!**

Answer:

As we know, Instagram is a photo sharing app which allows users to assign filters to photos and share them with followers. Instagram rolled out a desktop site this year for browsing (not uploading), but the app continues to be preferred environment for users to interact. Instagramers can sync their photo sharing to other social networks, so Instagram photos can be posted directly to Facebook, Tumblr, Twitter, Flickr, and Foursquare.

I think that new developing social media site should introduce new features for everyone because Technology advances regularly and app development industry has been enjoying its fair share of advancement too. So, it is necessary to follow the trend by adding new and unique feature on your site and application. Software updates offer plenty of benefits. It's all about revisions. These might include repairing security holes that have been discovered and fixing or removing computer bugs. Updates can add new features to your devices and remove outdated ones. If they don't bring new features on their app or website, the user will surely change their website which have more feature than of others. As we know, the more the features, more the user. User get attracted due to the features, so the social media site should keep updating and adding new features on their site and application. If social media can provide unique features which is

only available on this app, for sure tons of people will use the application for that feature. If you don't add new features, you cannot improve user experience. But some features may harm user privacy too. For example, while uploading or posting a photo on Instagram, it may share your location to other.

 The reality is that apps or social media site must be updated on a regular basis to keep them fresh and functioning. So, *I think that new developing social media site should introduce new features for everyone*.

Thank You.