1. **Introduction**

Facebook has been criticised following revelations that a political consulting firm Cambridge Analytica secretly analysed data for political parties by collecting the personal data of 87 million Facebook users. The data was specifically used to assist American politicians to target potential voters during the major 2016 election. This has now prompted change in major privacy laws on what has to be explicitly disclosed to online users of services.

OneOne industries has tasked us, Doris Industries, to provide a case study which will discuss the existence of vulnerabilities in Facebook's systems which allowed Cambridge Analytica to obtain information and make recommendations for what Facebook and other social media platforms could do to protect client confidentiality.

1. **Analysis**

2.1 The What, Why, Who?

Cambridge Analytica harvested user information with a quiz app, "This is you Digital Life", which had a likeness to a Trojan horse. Users who downloaded and used the app, connected it to their personal Facebook accounts and the infamous data firm then had access to extremely personal information, such as Facebook messages, which users were not fully aware that they were giving due to the vagueness of the wording. Users were also not aware that they were giving free access to their information to harvest <https://refeds.org/a/1909>. This also included access to their friend’s information. Hence this exponentially increased the data leak as the average number of Facebook friends is 338 people (<https://www.brandwatch.com/blog/47-facebook-statistics/>).

This was all done to map certain personality traits to specific marketing schemes so political parties were able to target their ads to a popular demographic. Most notably, this analysis occurred for the 2016 American Presidential campaigns, but this has also been used for political parties worldwide.

<https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>

2.2 How did Facebook go wrong?

While Facebook technically had not done anything explicitly wrong on their part, and Cambridge Analytica had preyed upon the naivety of individuals to release the information; Facebook had been lax on monitoring what information third party apps had access to. Mark Zuckerberg even admitting, "We didn't take a broad enough view of our responsibility, and that was a big mistake." in the senate hearing on the 10th April 2018. (INSERT SENATE HEARING VIDEO). While Facebook was not "hacked" as at the time apps were allowed to have more access to information, the large mass of raw information obtained should not have been able to be acquired by third parties to then be monetised which breaches ethical guidelines as well as company guidelines (<https://www.facebook.com/about/basics/advertising>). Also while users were made aware that information was being given to this app associated with Facebook, the were never made aware that it was being collected by a third party - Cambridge Analytica nor were they aware that their friends data was also being collected. <https://dig.watch/trends/cambridge-analytica>

* 1. Future Preventative Measures.

While a lot of blame was shifted to Facebook, most of the preventative measures for something like this occurring are upon the users themselves. They have to monitor what has access to their information and how; this being done by checking what is connected to their accounts. This constant reviewing means that unused and unwanted apps will not be accessing and storing potential information. If this method is frequently in use, this would minimise the probability of information leaks. This method can also be used for other social media websites.

More resources need to be pooled into user education about the safety of their own data. 2018 shows a peak of data leaks compared to previous years (<https://securityscorecard.com/blog/cybersecurity-data-breaches-statistics-on-the-rise>). Most individuals are unaware of the high cost of their identity and would value from understanding this.

Facebook and other social media platforms may benefit from reviewing what private data is able to be accessed by third party apps. Facebook should have never allowed a loop hole where private messages were able to be easily accessed <https://www.wired.com/story/cambridge-analytica-private-facebook-messages/>. This lost the trust of users and negatively affected both parties. Also while users did grant permission to view the inbox, this permission was hidden in a list of other less confronting information like profile pictures. Therefore, social platforms would find advantage in being fully transparent with users so that confidence is once again built with the customer of the product.

1. **What has changed?**

Since Cambridge Analytica has been exposed, it has filed for bankruptcy and no longer is a running company. Facebook has also started reviewing the Application Programing Interface (API) it uses so that more restrictions on third party apps would be more visible in the future. Websites are also entitled to disclose what information is being stored on the website when users visit it under the new European Union (EU) guidelines <https://www.euronews.com/2018/04/11/could-eu-s-new-data-protection-law-have-stopped-cambridge-analytica-scandal>. This is to ensure that users are not having personal data shared without express consent.

1. **Conclusion**