1. **Introduction**

Facebook is a social media and networking website based in California, USA. It 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 used to assist American politicians to target potential voters during the 2016 election. This has now prompted a change in significant privacy laws on dictating that websites have to explicitly disclose what information is being stored while users use online services.

OneOne industries have 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. We will then make recommendations for what Facebook and other social media platforms could do to protect client confidentiality.

2. **Analysis**

2.1 The What, Why, Who?

Cambridge Analytica harvested user information with the quiz app, "This is your Digital Life". This app was developed by the data scientist Aleksandr Kogan and has been likened to a Trojan horse. Users who downloaded and used the app connected it to their personal Facebook accounts and thus to Cambridge Analytica. This then gave the data firm access to extremely personal information such as Facebook messages, which users were not fully aware that they were given due to the vague wording of the permissions page.

Users were also not aware that they were giving free access to their information for harvesting [1]. Data harvesting is the method used to collect and store data for future use by the parties. On average, one person has 338 friends on Facebook [2]. Therefore, if a user were to connect to the "This is your Digital Life" app, it would have access to 339 users' information. However, this was an extremely unethical, back-road way for "This is your Digital Life" to obtain data as they were not permitted by the users' friends to access their information also. This method of data collection meant that the effect of the leak became increasingly worse as more users connected to the app.

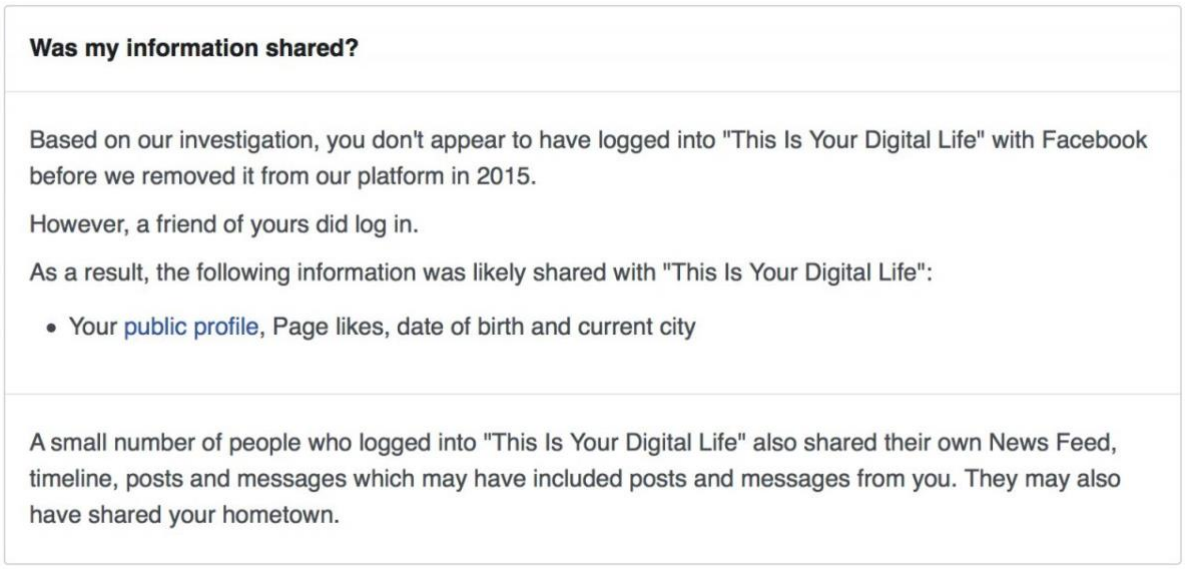

Fig.1

As shown in the image above (Fig.1 [3], a range of information was used for the marketing of political parties. This was done to map certain personality traits alongside specific marketing schemes, so political parties were able to target their ads to popular demographics. While this data harvesting and analysis was used famously in the 2016 American Presidential campaigns, political parties worldwide [4]. Information such as; likes, posts and messages can be matched with each other to show hidden details of a person such as sexual orientation [5] [6]. This demonstrates why the "This is Your Digital Life" was a powerful and sought-after tool to use, and why Facebook was negligent not to monitor the information that apps had access to, but also in failing to investigate how they were using the data.

2.2 How did Facebook go wrong?

Though Facebook had not technically done anything explicitly wrong, and that is was Cambridge Analytica that preyed upon the naivety of individuals to obtain information, Facebook had been overly relaxed on monitoring what information third-party apps had access to. During his Senate hearing on 10 April 2018, Mark Zuckerberg admitted that Facebook “didn't take a broad enough view of our responsibility, and that was a big mistake." [7] Facebook was not "hacked", I actively allowed apps on the platform to have easy access to information. The large mass of raw information should not have been able to be acquired and monetised by third parties like Cambridge Analytica. This directly breaches engineering ethical guidelines as well as company guidelines [8]. Also, while users were informed that information was being given to this app associated with Facebook, they were never made

aware that it was being collected by a third neither party nor were they aware that their friends' data were also being collected [9].

3. Future Preventative Measures.

While Facebook faced the brunt of the blame, some responsibility for maintaining preventative measures for breaches occurring is upon the users themselves. They have to monitor what has access to their information and how. Users would benefit by checking what apps are connected to accounts. This means that unused and unwanted apps will not be accessing and storing potential information as users are constantly monitoring the apps. If this method is frequently in use, this would minimise the probability of information leaks and can be implemented on other social media platforms. Facebook can support this by giving users reminders every 6 months to check their permitted apps.

However, users are usually unaware of the measures they can take themselves to minimise the risk of their data being leaked. Therefore, more resources need to be pooled into user education about the safety of their data. Doris industries recommend Facebook implements this especially as 2018 shows a peak of data leaks compared to previous years [10]. Personal information is highly valuable for advertisement, research and fraud related uses [11]. Most individuals are unaware of the high cost of their identity and would value from understanding this.

While users did grant permission to view the inbox, this permission was hidden in a list of asking other less confronting information like profile pictures. Therefore, Facebook and other social platforms would find an advantage in being fully transparent with users. Doris industries recommend this so that confidence is once again built with the users of Facebook. This would include disclosing to users what other parties may have access to the app, what information is being given, how data is being collected, and what the data is being used for [12]. Not only would this benefit user trust, but Facebook would also then be able to monitor how information is being used and by who so can see if any apps are going against the community guidelines.

4. Conclusion

Since Cambridge Analytica has been exposed, it has filed for bankruptcy and is no longer a running company. Facebook has also started reviewing the Application Programming

Interface (API) it uses so that more restrictions on third-party apps would be implemented in the future. Under the new European Union (EU) guidelines, websites are also entitled to disclose what information is being stored on the site when users visit it. https://www.euronews.com/2018/04/11/could-eu-s-new-data-protection-law-have-stopped-cambridge-analytica-scandal. This acts to ensure that users do not have their data shared without their express consent.

Facebook should be aware that while Cambridge Analytica monetised information for unethical gain, the social media platform made it easier for the company to do so by not monitoring the apps on the platform. This oversight breached the international engineering code of ethics and should not occur again. Doris industries suggest Facebook follow these preventative measures in the future to rebuild the trust of users, as well as improving their oversight of what third-party information apps have access to through their website.

Bibliography

[1] N. Harris, "Is This Your Digital Life?," 13 April 2018. [Online]. Available: https://refeds.org/a/1909. [Accessed 24 September 2018].

[2] K. Smith, "47 Incredible Facebook Statistics and Facts," 5 March 2018. [Online]. Available: https://www.brandwatch.com/blog/47-facebook-statistics/. [Accessed 24 September 2018].

[3] C. Davies, "Your personal Facebook messages may also have been shared," 10 April 2018. [Online]. Available: https://www.brandwatch.com/blog/47-facebook-statistics/. [Accessed 2018 September 24].

[4] K. Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, The New York Times, 2018.

[5] "Cambridge Analytica controversy must spur researchers to update data ethics," *Nature*, no. 7698, pp. 559-560, 2018.

[6] Y. &. K. M. Wang, "Deep neural networks are more accurate than humans at detecting

sexual orientation from facial images," *Journal of Personality and Social Psychology,* vol. 114, no. 2, pp. 246-257, 2018.

[7] T. c. o. B. Government, *Transcript of Mark Zuckerberg's Senate hearing,* Washington Post, 2018.

[8] Facebook, *Advertising,* Facebook.

I found peer review process very helpful – most of my comments were that I had to add more details which I attempted to do.