Cyber Security Issues Brought on by Facebook

Student's Name

College Affiliation

Cyber Security Issues Brought on by Facebook

A recent scandal around Facebook and Cambridge Analytica has revealed a huge data leak, which resulted in influencing American voters via targeted advertisements during the US presidential election in 2016 (Cadwalladr and Graham-Harrison, 2018). This has pointed out at how vulnerable private data may be and that any information stored online can one day be disclosed to a third party, with the websites it was submitted to not having control over it. As a result, this incident made millions of Internet users think twice before sharing personal details with online platforms and applications, because it can lead to the unauthorized use of private information.

For a better understanding of why the situation caused hot debates, we need to clarify what happened at the very beginning of the circumstances. Dr. Aleksandr Kogan from the Department of Psychology at the University of Cambridge had created a Facebook application “thisisyourdigitallife” with a quiz that helped to discover more about one’s personality. Nearly 270,000 users took the test and shared their personal data from Facebook. Besides this, the application gained access to the public data of people from each user’s friends list. Altogether, Kogan collected data from almost 50 million Facebook profiles. After that, he sold the harvested information to Cambridge Analytica, a political consulting company (BBC, 2018).

Andrew Bosworth, VP of VR/AR at Facebook, states that in 2015, Facebook had revealed that fact and requested that Cambridge Analytica should remove all the data they received from Kogan. The company claims to have deleted it, yet it appears they failed to do so and still used this information for voter segmentation and to deliver personalized advertisements during the US election in 2016 (Landau, 2018). In its turn, Cambridge Analytica denies the accusations and says that Kogan’s data has proven to be less effective than traditional demographic segmentation. As a result, they say that have not used it and have conducted their own research instead, which was applied to the Donald Trump presidential campaign (Cambridge Analytica, 2018).

At the same time, Aleksandr Kogan said in his interview with the BBC that the data he provided to Cambridge Analytica was not accurate enough. Also, he thinks that Facebook and Cambridge Analytica made him a "scapegoat," as he did not suspect he did anything wrong. Besides, he added that the consulting firm had assured him that their deal was legitimate and did not violate any privacy policy or terms of use (BBC, 2018).

Meanwhile, Facebook VP and Deputy General Counsel, Paul Grewal, noted that though Dr. Kogan received the information in a legal way, by no means was he allowed to pass the results of his research to any third party—especially if it was intended to be used for commercial purposes, as it was in case with Cambridge Analytica. Paul underlines that as soon as Facebook discovered this violation, they took action and removed Kogan's application and insisted that the researcher should delete all the obtained information as well. Grewal (2018) also tried to justify the social network and explained that unlike traditional cyber attacks, when personal data is stolen, in this case the users provided their information to Cambridge Analytica voluntarily:

> The claim that this is a data breach is completely false. Aleksandr Kogan requested and gained access to information from users who chose to sign up to his app, and everyone involved gave their consent. People knowingly provided their information, no systems were infiltrated, and no passwords or sensitive pieces of information were stolen or hacked.

From a technical point of view, Grewal's statement is correct. In fact, all those Facebook profiles were not hacked. On the contrary, the information from them was taken by the permission of each user, who allowed Kogan's application to access their personal details. Thus, despite the fact that Facebook was not able to control this data leak, part of the responsibility is on the users, because they gave their consent to provide information to the researcher.

Even though Facebook has tightened up its policies regarding what user information the applications can collect, as well as introduced a possibility for every user to check what permissions he or she grants to a certain application, one should remember that even the most secure systems and platforms cannot guarantee full confidentiality. As Pariser (2011) cites Chris Palmer of the Electronic Frontier Foundation "You are getting a free service, and the cost is information about you" (p. 8). That is why each of us should be more careful when sharing our personal information with any online or mobile resources, because one day it may be accidentally used against us.

References

Cadwalladr, C., and Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian.* Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Dr Aleksandr Kogan interviewed by 60 Minutes. (2018). *Cambridge Analytica.* Retrieved from https://ca-commercial.com/news/dr-aleksandr-kogan-interviewed-60-minutes.

Facebook data row: Cambridge Analytica academic a 'scapegoat'. (2018). *BBC News UK*. Retrieved from http://www.bbc.com/news/uk-43480978.

Grewal, P. (2018). Suspending Cambridge Analytica and SCL group from Facebook. *Facebook newsroom.* Retrieved from https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/.

Landau, S. (2018). No, Facebook, It's Not About Security; It's About Privacy. *Lawfare Blog.* Retrieved from https://www.lawfareblog.com/no-facebook-its-not-about-security-its-about-privacy.

Pariser, E. (2011). *The filter bubble: what the Internet is hiding from you.* London: Viking.