Ethical Analysis: Facebook “Research App” Violates Apple’s Privacy Policy

Lacey A. Weeks

University of North Alabama

Table of Contents

Abstract

In 2016, Facebook created a research VPN app, called Project Atlas, to collect a variety of data from the users that participated in the study. For the next two or three years the app collected personal information regarding its users and paying the users for the data they provided before Apple responded. The app not only violate Facebook's and Apple's agreement in order to have the app on Apple's Enterprise system, but it also went against Apple's privacy policy by collecting personal data from the users who downloaded the app. Apple revoked the Enterprise Certificate they gave Facebook and forced Facebook to remove their research VPN app. This was not the first time Facebook attempted to create an app that obtain personal data from its users. The ethical problem here is should Facebook have access to all a user's personal data even if they are paying the user for this data and the user consented? This paper is designed to analyze the privacy issue that Apple and Facebook had encountered and to use the Laudon and Traver approach to solve this ethical dilemma.

Keywords: Facebook, Apple, privacy, research, app

Ethical Analysis: Facebook “Research App” Violates Apple’s Privacy Policy

For this paper, I will follow the five guidelines introduced by Laudon and Traver in their *E-Commerce* book (Laudon & Traver, 2014). These key guidelines are useful to analyze the ethical dilemma where Facebook violated both their agreement with Apple and Apple’s privacy policy. In 2016, Facebook created a research app designed to be used on both Android and Apple devices. This app recruited users to download and use this app while also paying these users a monthly fee. Unknowingly to the users, Facebook were obtaining personal data from these users’ phones for personal gain (Constine, Apple bans Facebook's Research app that paid users for data, 2019). After two or three years since the app’s release, Apple discovered the true nature of Facebook’s research app. Due to Facebook violating both the privacy policy and their agreement with Apple, Apple revoked Facebook’s Enterprise Certificate which prevents some of Facebook’s apps from working on Apple devices. I will be analyzing the privacy and agreement violations of Facebook’s research app on Apple devices using the guidelines provided.

Analyzing the Ethical Dilemma

The five-step process to analyze the ethical dilemma first begins with identifying the current facts. Next is to define the conflict. Third, the stakeholders needs to be identified for the purpose of this analysis. Afterwards, identify any suggestions that could potentially resolve this conflict. Finally, identify any consequence that could be the result of the solutions. These steps will be used to analyze the Facebook and Apple privacy conflict.

The facts

In 2016, Facebook created a research app designed to be used on both Android and Apple devices. It recruited people from the ages of 13 to 35 years old with roughly 5 percent of those people being teenagers to download and use this app (Constine, Apple bans Facebook's Research app that paid users for data, 2019). Facebook paid the willing users a monthly fee alongside referral bonuses. This app required the user "to 'Trust' the company with root network access to their phone" (Constine, Apple bans Facebook's Research app that paid users for data, 2019) which violates the user's privacy. In order for Facebook to be allowed to have this app on Apple devices they needed to take part in the Apple Developer Enterprise Program and obtain an Enterprise Certificate offered by Apple. The Apple Developer Enterprise Program was only intended to be used for distributing "apps within an organization" (Constine, Facebook pays teens to install VPN that spies on them, 2019).

The conflict

Facebook violated their agreement with Apple and Apple's privacy policy with their research app. The agreement between the two companies was for Facebook to only use the Enterprise Certificate to distribute the app among its employees, not to consumers. However, Facebook was able to distribute this app to consumers, most likely using the Enterprise Certificate that Apple gave them. Not only that, but the company invaded the privacy of many of its users by using the app to obtain "a user's web browsing activity, what apps are on their phone and how they use them..." (Constine, Apple bans Facebook's Research app that paid users for data, 2019). Apple did not approve of Facebook invading the privacy of Apple's users through this app nor did they approve of the agreement violation, so they revoked the Enterprise Certificate they have given the company.

The stakeholders

The main stakeholders involved in this conflict are Facebook, Apple, and users. On one hand, Facebook claims that they did not violate any of Apple's rules because they distributed the app using the Enterprise Certificate program, despite that the this program was not intended for what Facebook did (Lee, 2019). However, on the other hand, Apple revoked Facebook's Enterprise Certificate in order to protect their users from having personal data collected and used to benefit Facebook. From Apple's point of view, Facebook tried to manipulate the system and take advantage of their trust in order to obtain information of these users that could benefit the company.

Reasonable solutions

The most reasonable solution would be for Facebook to take responsibility for their actions rather than to continue trying to bypass Apple's security and privacy policy. If they want to continue to work with Apple and have Apple accept any future apps, Facebook needs to follow Apple's rules. Because of Facebook's behavior, it would be a good idea for Apple to monitor their Enterprise program better than before. Consider adding further restrictions in what any company can do using this program while also considering a background check of each company that wants to use the program when possible.

The Consequences

Apple's response to Facebook's violations was a reasonable response. If Apple were to come down on who can use their Enterprise program, it could potentially affect the program negatively if nobody wants to use the program if the rules are too strict. Depending on how many companies wanted to use the program at any given time, the background checks could be too time consuming and potentially still not get the results Apple might want. Also, if companies like

Facebook did not try to pull stunts like these, then Apple might not be aware of backdoors that could be used to take advantage of their program.

Conclusion

Facebook tried to manipulate Apple and misuse their Enterprise program for personal gain. Fortunately, Apple discovered their manipulation and acted in order to prevent any further damage to their users' privacy. I do agree with Apple's approach to solving this conflict. However, I do not believe this is the end of Facebook's attempts to obtain personal information of users. Unfortunately, Facebook is not the only one invading privacy and dealing with data scandals. Incidents like this make me like Facebook less, but due to habit of using the social media platform it would be somewhat challenging to break away. If anything else, this should serve as a reminder to all users to be cautious of what they share online and which apps they use.

Works Cited

Constine, J. (2019, January 30). *Apple bans Facebook's Research app that paid users for data*. Retrieved from Tech Crunch: https://techcrunch.com/2019/01/30/apple-bans-facebook-vpn/

Constine, J. (2019, January 29). *Facebook pays teens to install VPN that spies on them*. Retrieved from Tech Crunch: https://techcrunch.com/2019/01/29/facebook-project-atlas

Laudon, K. C., & Traver, C. G. (2014). *E-Commerce.* New York: Pearson.

Lee, N. (2019, January 29). *Facebook secretly pays users for complete access to their data*. Retrieved from engadget: https://engadget.com/2019-01-29-facebook-project-atlas.html