The Facebook Cambridge-Analytica Data Scandal and Virtue Ethics

STS Research Paper
Presented to the Faculty of the
School of Engineering and Applied Science
University of Virginia

By

Alexander Hu

April 11, 2019

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _____

Approved: _____ Date _____
Benjamin J. Laugelli, Assistant Professor, Department of Engineering and Society

Introduction

The Facebook-Cambridge Analytica data scandal involved the leak of one of the largest amounts of consumer data of any data breach in history (Swinhoe, 2021). This data ranged from personal information such as users' names, emails, location, videos and photos to activity such as content they consume, their browsing history, purchase activity, and people they communicate with (Vigderman, 2020). Currently, discourse around this incident mainly focus on the consequences of the breach and how breaches like this one can be avoided in the future. However, it is much more difficult to find an ethical discussion on the responsibility of the engineers that were responsible for breach itself. It is just as important, if not more, to discuss the absence of virtue of the engineers that were in charge of the Facebook security protocols.

Without an understanding of the virtues necessary for any engineer to be morally responsible, incidents such as this data breach could easily happen again, leading to a repeat of the disastrous consequences that occurred in the Facebook-Cambridge Analytica data scandal. It is crucial to realize how the character of an engineer can impact the technology they work on in order to keep the public safe. Using primary newspaper reports on the scandal, a Facebook press release, and ads that users received as a consequence of the leak, I will examine the Facebook-Cambridge Analytica data scandal through the ethical framework of virtue ethics to explain that the engineers behind the development and mishandling of the Facebook Login feature that led to this leak were morally culpable due to their lack of the character traits crucial for morally responsible engineers: competence, openness to correction, and seeing the "big picture" as well as the details of smaller domains.

Background

The Facebook-Cambridge Analytica data scandal involved the harvesting of up to 87 million people around the world without their consent by the British political consulting firm Cambridge Analytica. The company developed an app called "thisisyourdigitallife" which analyzed the user's Facebook account of over 250,000 people. This app used a feature called Facebook Login which allowed users to sign in to the app using their Facebook account. However, due to the lax security programmed by Facebook engineers around user's private information, the app was able to acquire non-consented data from not only the user, but also every person in the user's friend network (Arora & Zinolabedini, 2019). Using this illegally obtained data, Cambridge Analytica provided analytical assistance to the 2016 presidential campaigns of Ted Cruz and Donald Trump by building individual psychographic profiles to specifically target users and was also accused of interfering with the Brexit referendum. Facebook eventually agreed to pay a hefty fine for exposing user's data to a "serious risk of harm" (Facebook agrees to pay, 2019).

Literature Review – Librarians confirmed that Rehman is academic peer-reviewed

A multitude of scholarly sources have investigated the Facebook Cambridge-Analytica data scandal. These sources mainly focus on analyzing the issues the scandal brought up and the responses to them and the results of the scandal. However, while the consequences of the scandal are an important topic, these sources avoid making moral claims using virtue ethics on the engineers that were responsible for Facebook's security system and practices.

In *Big data and the Facebook scandal: Issues and responses*, Michael Fuller describes how the data scandal illuminated wider concerns about 'big data' relating to the obtaining, storage, and use of personal data for commercial purposes (Fuller, 2018). Fuller begins by defining 'big data' and explaining the advent of how data has come to be seen now "primarily as

an economic asset, not as a research one" as it was in past practice. He then goes on to assert that users are not truly able to make a sufficiently informed choice when consenting to the use of their data when using online services. He mentions that because of the increasing use of more complex and opaque data-mining techniques, the interrelatedness of personal data, and the unpredictability of potential harms from its nearly ubiquitous collection, the notice and consent paradigm of acknowledging the 'terms and conditions' of a service are a "legal fantasy". Fuller concludes that individuals are insufficiently protected against the potential abuse in the future of their personal data given to online service providers and that the creation of a new industry centered around trading users' data means that there may be vested interests against the solving of this problem in legislation. While Fuller bring up the issues that the Facebook scandal brought up regarding data, it does not have any mention of the morality of the engineers that allowed the scandal happen in the first place.

Rehman focuses instead on the consequences of the data breach and how consumers should act in response to this incident (Rehman, 2019). Rehman begins by explaining how online data from individuals could be used to build a psychometric profile. He mentions for instance that fans of Lady Gaga were likely to be extroverts, while those that were interested in philosophy were likely to be introverts. Using the thousands of data points that make up one individual's online footprint allow the prediction of not only an individual's skin color, sexual orientation or political preference, but even things such as intelligence and cigarette and drug use. Rehman continues by explaining how the harvested data played a key role in Donald Trump's successful campaign in the 2016 presidential election by identifying specific voters to target with personalized ads with negative messages allowing the campaign to focus on just tens of thousands they knew were susceptible to be influenced instead of needing to advertise to the

millions of voters across the United States. Rehman concludes by calling for consumers to realize the value of their data and to read data privacy notices and take advantage of their rights to take back their data and have their personal data viewed, edited, and deleted. Again, no moral claim is made on the engineers at Facebook, instead focusing on the consequences of the scandal and its takeaways.

While it is definitely important to describe the consequences of the scandal including the new issues brought up because of it, as well as the specific actions that consumers should take in response to the incident, the current research does not make any sort of moral or ethical claims on the engineers that were responsible for the incident to happen in the first place. In this paper, I will deploy the framework of virtue ethics to asses the morality of these engineers and explain why these engineers do not hold the virtues that morally responsible engineers should possess.

Conceptual Framework

Virtue ethics is a normative ethical theory developed by Aristotle that emphasizes the virtues or the character of the moral actor. The theory focuses on certain qualities of excellence that people should cultivate to act morally and attain the goal of the good life, also known as eudaimonia, meaning true happiness and well-being. Subscribers to this theory believe that individuals should use reason and wisdom to obtain the mean between two extreme vices. For example, a willingness to compromise represents a virtue between not accepting anything but one's own opinion and letting others force one into their opinions. It is possible to cultivate virtues—they are not innate and can be learned through practice. In order to be moral, it is necessary for an to use moral skill to determine the most virtuous course of action (van de Poel & Royakkers, 2011).

Virtues can change depending on the situation and position of those involved. While virtues such as reliability, honesty, responsibility, and solidarity are general and should be possessed by morally responsible engineers, Michael Pritchard lists more specific virtues that are required for morally responsible engineers:

- Competence
- Ability to communicate clearly and informatively
- Cooperativeness (being a good "team player")
- Willingness to compromise
- Perseverance
- Habit of documenting work thoroughly and clearly
- Commitment to objectivity
- Openness to correction (admitting mistakes, acknowledging oversight)
- Commitment to quality
- Being imaginative
- Seeing the "big picture" as well as the details of smaller domains

In this case, I will be analyzing the actions of the Facebook engineers that were involved in the Facebook Cambridge-Analytica data scandal and thus, will focus on these specific virtues. Pritchard notes, while having these dispositions is not enough for responsible engineering practice, lacking any of them detracts from responsible engineering practice in general (Pritchard, 2001). In this paper, by analyzing their actions and decisions, I will assert the claim that the engineers responsible for Facebook's security did not embody three virtues necessary for morally responsible engineers: competence, openness to correction, and seeing the "big picture" as well as the details of smaller domains.

Analysis

Ethics is not commonly discussed in relation to engineering. Even when discussed, the discussion tends to focus on specific events with tragic consequences and focus on questions about the avoidance or prevention of wrongdoing. Equally as important, however, is the discussion about responsible engineering practice which is not discussed nearly as often. In the case of the Facebook Cambridge Analytica data scandal, current discourse is mainly centered around the consequences of the event and the issues it brings up and how these issues can be prevented in the future, while the absence of virtue of the engineers in charge of Facebook's privacy and security features has been left out. In order to be a morally responsible engineer, it is necessary to, at the very least, not lack any of the virtues noted by Pritchard (Pritchard). In the case of the data scandal, the engineers lacked three. It is important to realize how the actions of an engineer can impact the technology they work on so that incidents like the data scandal do not happen again. The character of an engineer is crucial to protecting the public, as there is little reason to expect competent engineering practice without any of them leading to disastrous outcomes. With the following analysis, I will illustrate the three virtues that the Facebook engineers failed to embody with their actions and decisions.

Competence

The first and arguably the most important virtue that the Facebook engineers responsible for the data scandal lacked was competence. Competence is defined as the ability to do something successfully or efficiently (Merriam-Webster, n.d.). For engineers, this virtue is vital to ensure that the technologies they create are not only usable and effective, but safe and free of

flaws. With technologies now having the ability to greatly impact the lives of billions of people across the world, this virtue is especially important.

Between its inception until 2013, Facebook had a long history in the mishandling of user data. This only had small consequences for the tech giant, in which the company had to give out small monetary settlements and received light admonishments from the government (Arora & Zinolabedini, 2019). In 2014, however, Facebook launched new technology tools for software developers, one of which was Facebook Login, which let people log in to a website or app using their Facebook account instead of creating a new username and password. This feature simplified the login process, allowing users to use a few taps to login and not need to remember more and more username and password combinations. In order to use Facebook Login, however, the user needed to grant the website or app's developer access to information such as their name, location, and email—things that Facebook thought would help app developers (Wagner, 2018). Back in 2014, however, the developer was able to access an abundance of information that the user may not have known would be shared. This included personal information such as religious or political views, relationship statuses, education and work history, news reading, and even things such as access to group content for closed groups without group admin permission, information about any events they host or attend, including private events, and the posts and comments from any of the user's pages (Schroepfer, 2018). While the user technically did need to consent to this, through a mixture of sharp design and obscure legal jargon, developers typically attempted to "minimize the ability of the person about whom data is being gathered to comprehend the scope of the data and its usage" (Fuller, 2018), causing "people to consent to the collection, use, and disclosure of their person data when it was not in their self-interest to do so" (Fuller, 2018). The oversight by the Facebook Login engineers to allow access to all of this

information was a clear failure, as users had no idea that they were opting into allowing developers unbounded access to all their private information. This was a dangerous amount of information, that could be used to completely identify and know everything about a user. This flaw should not have been possible in the first place and shows a lack of competence by the Facebook engineers in charge of the feature.

The most egregious flaw in the Facebook Login feature was not even this, however, but the ability of developers to collect the same information from the entire friend networks of the people who used Facebook Login. That meant that a single user agreeing to hand over their data—albeit almost certainly unknowingly—meant that developers could access the same data about all their friends without their consent or them using this feature at all (Wagner, 2018). This, in combination with the previous flaw, is what led to the Facebook Cambridge-Analytica data scandal. Through the app made by Cambridge-Analytica, 270,000 users opted in using Facebook Login. This allowed the company to gain access to the personal data of not only those users but of 87 million others in addition (Arora & Zinolabedini, 2019). This data contained enough information such as places of residence, that the company was able to match users to other records, allowing them to build psychographic profiles (Wagner, 2018). By allowing this kind of abuse of Facebook's networks and consumer data causing one of the largest data breaches in history, the Facebook engineers responsible for this lacked the virtue of competence. In a press release by the Chief Technology Officer of Facebook following the data scandal, Schroepfer notes "nine most important changes" to "better protect [one's] Facebook information" including the fix of both flaws mentioned above, with Facebook no longer allowing apps to ask for access to any of this personal information and access any data from user's friend networks (Schroepfer, 2018).

Openness to Correction

In addition to lacking the necessary competence that any morally responsible engineer should have, the Facebook engineers also lacked an openness to correction. While it is important to be firm in one's conviction when one believe that he or she is making the best decision or action, it is important to realize that everyone is fallible and that even the best engineer can make the wrong decision. Especially when a decision or action is important and could possibly lead to disastrous consequences, it is necessary to take a step back and get a second opinion from a trusted source. If others that are in the same practice and have similar qualifications or competence are saying that a decision is incorrect, it is important to objectively analyze that decision and be willing to change it if it is wrong. Oftentimes, stubbornness, arrogance, or pride can cloud one's judgement and cause great damage (Grensing-Pophal, 2019).

In the case of the Facebook scandal, the issue of the security weakness was actually already known. As mentioned in the section above, in 2014, the design the new Facebook Login service allowed developers to collect information on the friend networks of people that used Facebook Login to other services allowing for any third party that collected data from users that logged in to their service through Facebook to access the data of every user in their friend network without those user's consent. The design by the engineers responsible for this feature lacked competence in allowing this flaw to exist. However, in 2019, The Guardian revealed that Facebook was actually aware of this security disaster. The article included an internal Facebook correspondence from 2015 in which an anonymous Facebook employee raised concerns about the flaw that allowed external companies to scrape the large amount of raw consumer Facebook data. In the correspondence between the concerned employee and their supervisor, the employee

noted many times that there were “likely a few data policy violations” in regards to the Facebook Login feature (Wong, 2019). The employee mentioned that they believed many companies were exploiting this flaw by scraping the Facebook data of not only the intended user but also their entire friend network, and specifically named Cambridge Analytica in their concern. This employee was joined by a small group of other Facebook employees and brought their concerns to the senior Facebook engineer responsible for the feature. However, even with the evidence brought forth by the group, the engineer refused to investigate the alleged flaw, mentioning that Facebook should only explore this if they see red flags (Arora & Zinolabedini, 2019). Even with the clear red flags and group of employees bringing this fatal flaw to the engineer’s attention, the engineer was not open to correction and believed that there was no abuse of the flaw that warranted any change or investigation, proactively choosing to do nothing about it, showing a lack of the virtue of openness to correction.

Seeing the “big picture” as well as the details of smaller domains

Lastly, the Facebook engineers were not able to see the big picture. While it is important to focus on the details of a technology, such as how to make it work best for its users and making sure it works as efficiently as possible, it is equally important to consider the broader impacts of the technology such as how it could impact the safety and well-being of its users and society (Geldart, 2020).

The previous design of the Facebook Login feature that allowed for the unbounded access to user and friend data to app developers was actually intended by the developers (Wagner, 2018). The developers believed that access to this data would help the developers with their application or website. However, trusting all these third-party developers not to misuse the

private information of consumers and not foreseeing the potential abuse of this flaw was a failure to consider the big picture. While the developers of Facebook Login believed that this would be a boon to the developers, the large amount of private data available allowed for the complete identification of every user and the creation of psychometric profiles that allowed for the targeting of specific vulnerable and susceptible users. Based on the psychometric profiles of the users, different ads were shown based on which traits the users seemed to exhibit. For example, an ad that read "The Second Amendment isn't just a right. It's an insurance policy." was shown to users that were deemed to have scored high in the neuroticism and conscientious traits who tend to worry a lot and prefer order. A second ad that read "From father to son since the birth of our nation" was shown to those who scored high in the closed and agreeable traits who tend to put other people's needs before theirs, but don't enjoy new experiences (Rathi, 2019). By targeting these users, the data obtained by Cambridge-Analytica helped Trump gain an estimated 77,000 votes in three key states which led to his eventual victory in the 2016 presidential election, in addition to possibly influencing the Brexit referendum (Confessore, 2018). These engineers focused only on the details of the small domain and lacked the virtue of seeing the big picture leading to these incidents.

I have argued that the Facebook engineers that developed the Facebook Login feature lacked the virtue of seeing the big picture. Some may argue that it would have been impossible for these engineers to have foreseen the future abuse of the flaws in the feature. It should be noted, however, that these engineers were experts in their field. In fact, senior software engineers at Facebook were the highest paid software engineers of any company in 2020, making a salary of over a million dollars (MacNaughton, 2020). Additionally, with over 250,000 applicants a year for engineering positions and an acceptance rate of just 0.132%, Facebook has the ability

and resources to hire the best (Alexander, n.d.). As the top of their field, these engineers should have known the importance of privacy and security of personal information, even if they had not foreseen the specific use of that data in the 2016 presidential election.

Conclusion

Through the framework of virtue ethics, I have argued that the engineers responsible for the Facebook Login feature and the serious security flaw associated with it are morally irresponsible as their actions and decisions show that they lack three virtues that are vital for morally responsible engineers: competence, openness to correction, and seeing the "big picture" as well as the details of smaller domains. As lacking any one of the virtues is enough to completely detract from morally responsible engineering, I conclude that the Facebook engineers acted immorally and unethically.

Oftentimes, whenever any incident occurs involving technology, the focus is on the flaws of the technology itself and not on how the flaws of the engineers responsible for the technology could have an impact. While it is important that engineers learn through the consequences of technology failures to avoid making the same mistakes, it is just as important, if not more, to understand how an engineer can make just and moral decisions. As can be seen in the Facebook scandal case, the decisions and actions of engineers can have great effect on the safety of the users of the technology they create. The use of virtue ethics can help provide a baseline for engineers to ensure that they are acting virtuously and making the correct decisions. By embodying the virtues necessary for morally responsible engineers, it may be possible to avoid incidents such as the data scandal in the first place and make a better and safer society for all.

Word Count: 3640

References

Alexander, A. (n.d.). What Apple, Google and Facebook look for in employees. Retrieved from https://ansonalex.com/infographics/what-apple-google-and-facebook-look-for-in-employees-infographic/

Arora, N., & Zinolabedini, D. (2019, December). The ethical implications of the 2018 Facebook-Cambridge Analytica data scandal. *Texas ScholarWorks.* Retrieved from http://dx.doi.org/10.26153/tsw/7590

Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The scandal and the fallout so far. *The New York Times*. Retrieved from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Facebook agrees to pay Cambridge Analytica fine to UK. (2019, October 30). *BBC News*. Retrieved from https://www.bbc.com/news/technology-50234141

Fuller, M. (2018). Big data and the Facebook Scandal: Issues and responses. *Theology*, *122*(1), 14-21. doi:10.1177/0040571x18805908

Geldart, P. (2020, April 30). The importance of seeing the big picture. Retrieved from https://www.entrepreneur.com/article/349368

Grensing-Pophal, L. (2019, September 11). Manager training: The importance of being open to criticism. Retrieved from https://hrdailyadvisor.blr.com/2019/09/11/manager-training-the-importance-of-being-open-to-criticism/

MacNaughton, L. (2020, March 12). Top 10 highest-paying employers of software engineers in 2020. Retrieved from https://www.hackreactor.com/blog/top-10-highest-paying-employers-of-software-engineers-in-2020

Merriam-Webster. (n.d.). Competence. In *Merriam-Webster.com dictionary*. Retrieved April 20, 2021, from https://www.merriam-webster.com/dictionary/competence

Pritchard, M. (2001). Responsible engineering: The importance of character and imagination. *Science and Engineering Ethics, 7*(3), 391–402.

Rathi, R. (2019, January 13). Effect of Cambridge Analytica's Facebook ads on the 2016 US presidential election. Retrieved from https://towardsdatascience.com/effect-of-cambridge-analyticas-facebook-ads-on-the-2016-us-presidential-election-dacb5462155d

Rehman, I. U. (2019). Facebook-Cambridge Analytica data harvesting: What you need to know. *Library Philosophy and Practice*, (2497). Retrieved from https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5833&context=libphilprac

Schroepfer, M. (2018, April 4). An update on our plans to restrict data access on Facebook. Retrieved from https://about.fb.com/news/2018/04/restricting-data-access/

Swinhoe, D. (2021, January 8). The 15 biggest data breaches of the 21st century. Retrieved from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

van de Poel, I., & Royakkers, L. (2011). *Ethics, technology, and engineering: An introduction.* Hoboken, NJ:Blackwell Publishing Ltd.

Vigderman, A. (2020, October 27). The data big tech companies have on you. Retrieved from https://www.security.org/resources/data-tech-companies-have/

Wagner, K. (2018, March 17). Here's how Facebook allowed Cambridge Analytica to get data for 50 million users. *Vox*. Retrieved from https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data

Wong, J. (2019, August 23). Document reveals how Facebook downplayed early Cambridge Analytica concerns. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2019/aug/23/cambridge-analytica-facebook-response-internal-document