7.4 CASE ANALYSIS

Information warfare, otherwise known as cyberwarfare or cyber conflict, is a relatively new form of warfare that incorporates the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes. Informational warfare usually uses data or information in a specific way to target people. The spread of misinformation, as well as disinformation, is a form of information warfare because it uses information in a particular form to target certain people in order to influence their thinking and behavior. The 2016 democratic election showcases one of the worst cases of informational warfare. The data on Facebook users by Cambridge Analytica, with the knowledge of Facebook, tremendously assisted the Trump administration in creating targeted ads that they could use to influence the minds of voters, without their knowledge or consent. In this case, I will argue that the ethics of care shows us that Facebook did engage in informational warfare because they allowed Cambridge Analytica to collect data on millions of users without their knowledge and then used that information to influence those same users to think a certain way, and further that they were partly responsible for the election outcome because they could've done more to protect user data and how user data is used.

Information and data exchange is a continuous process in the cyber realm, and as users, we are constantly taking in the information we come across, especially on sites like Facebook and Twitter. As users, when we use these social media sites, we exercise some level of trust in these sites, that they will not actively deceive us or mislead us. A case can be made that since we use these sites for free, these social media sites should be able to use our data however they deem fit because after all, that is our payment in exchange for them providing these sites for free. I

definitely can see how an argument like this can be made, but we must also understand that with the data these sites and cyber organizations have on us, they can use that information for extremely nefarious purposes. When considering the Facebook and Cambridge Analytica scandal surrounding the 2016 election, we can truly see how appalling these companies can use users' data against them. Facebook has access to all this information internally within their systems and not doing their due diligence to ensure that users' data wasn't being used in a vile way, as well as not ensuring that other companies with access to this information were using it in a proper way, definitely shows Facebook at fault for not truly caring about its users' data. In Keith Scott's *A Second Amendment for Cyber? Possession, Prohibition, and Personal Liberty for the Information Age,* he states " Technologies alter our ability to preserve and circulate ideas and stories, the ways in which we connect and converse, the people with whom we interact, the things that we can see, and the structures of power that oversee that means of contact" (Scott 3). Applying this statement to the scandal surrounding Facebook and Cambridge Analytica, we can start to see how important our interactions in cyberspace are, and upon realizing this we can also understand that having structures of power, such as Facebook and Cambridge Analytica is use this information however they desire, can have lasting implications on how users connect with one another. Not only can they disrupt the flow of information, but they can alter information to meet their agendas, and even develop persuasion tools to influence our decision and thinking. When considering that these companies technically have the upper hand due to the fact that they have so much of our information, it is imperative that there is some care or accountability in place, to hold these companies accountable. In his work, he also suggests that with how evolved technology has become and with the ways that we use it, it is only practical that we have a second amendment for cyberspace. Personally, I believe that a system like this, where the cyber

world is regulated similarly to that of the physical world just makes sense. The cyber domain is truly a realm of its own and having policies and laws in place can allow users to hold the structures of power that oversee sites like Facebook accountable for their actions. Having a specific amendment in place for the cyber world can also foster an environment of care, because the interdependent relationship between users and social sites will be realized, due to the fact that users on the site will know exactly how their data and information are being used and collected, and the transparency about data usage from social sites will assist in making that relationship healthy.

Fostering an environment of deep care and accountability is truly what the ethics of care is all about. The ethics of care requires that we show partiality to those we care about due to the intimate interdependent relationships we have built with them. When applying such a relationship to a company like Facebook and its users, it can be acknowledged that there really isn't much of that care shown toward users. I say this because of the usually risky and outright dangerous practices that Facebook can engage in with users' information. I believe that in a relationship between a company and a user, the same factors cannot be applied in the way that it would be a personal relationship between 2 people. This is why I believe that having a third factor such as stricter laws for how user data is handled by companies, as well as third-party companies who also have access to user data is necessary for fostering an environment of deep care. Holding companies accountable for their actions cultivates an environment that ensures that users' rights aren't being abused and their data misused. In Jarred Prier's *Commanding the Trend: Social Media As Information Warfare,* Prier offers insight when he states that " Social Media creates a point of injection for propaganda and has become the nexus of information

operations and cyber warfare" (Prier 52). With this statement, we can see how culpable Facebook is for engaging informational warfare especially since it allowed itself to be that point of injection for propaganda for the events surrounding the Cambridge Analytica scandal and the 2016 election. Facebook knew well enough about what Cambridge Analytica was doing when they gained access to user data. Cambridge Analytica's quizzes that provided them with data on the quiz takers, as well as people associated with them, were extremely deceiving because the people who took the quizzes didn't even know their data was being collected and used. Facebook commented that they never authorized permission for Cambridge Analytica to use the information how they used it, but Facebook clearly had the upper hand in that scenario because they owned the data primarily. They should definitely inquire a lot more about Cambridge Analytica's actions to target people with certain information using their data. For a company as big as Facebook, with its enormous financial resources, it definitely could've done more to protect users from being manipulated or being taken advantage of. Essentially without Facebook providing access to Cambridge Analytica, the user data would've never been Cambridge Analytica's to exploit, and further would've never been given to the Trump Administration to use as well. It truly all comes down to how much Facebook cared about its users and how much it wanted to protect them, and in the end, it seems that Facebook just didn't seem to care about its users enough. Facebook is definitely responsible for the outcome of the 2016 election because, without the user data taken from them, none of the subsequent actions like the Trump Administration getting their hand on the data would've ever happened.

Informational warfare is on the rise, especially with the ease of being connected to the internet. People are finding more and more ways to influence the way people think, and the way

society thinks. It is no wonder that there is so much misinformation and disinformation floating around on the internet. Facebook has had a huge impact on how information is distributed to people on online platforms. With millions of people on Facebook, the site has become one of the most influential ways to reach people, and reach into their ideologies and beliefs. The argument can be made that Facebook is in fact not responsible for the outcome of the election or even that Facebook did not actively participate in information warfare, but we must also realize that since Facebook is the nexus for where all these events started and escalated from, and their lack of stricter policies to ensure that such heinous things did not happens, makes Facebook responsible for their part in the whole ordeal.