The article *What Facebook Did to American Democracy* by Madrigal, outlines a number of facts about how Facebook has influenced American elections. In 2012, Facebook was seemingly used by American Democrats as a tool to mobilize for their eventual victory in that election. In response, Republicans decided to invest heavily in using Facebook to achieve their goals in the 2016 election. They did this with great success. Facebook's news feed and advertising features have changed significantly and increased in usage and importance since 2012. Its features were set up so that it became a very powerful tool capable of influencing large swathes of people. This culminated in a large amount of “fake news” and Russian propaganda being disseminated among Americans. This disinformation campaign was even more successful, as Facebook's algorithm was particularly constructed to deploy personalized information where it was deemed most effective. After the results of the election were decided by a small margin, much was made of this disinformation campaign. Many called for investigations or charges to be brought against Facebook for its role in the results. In this case analysis, I will argue that the ethics of care show us that Facebook did engage in information warfare because it allowed disinformation to disseminate on its platform, and further that they were partly responsible for the election outcome because of this and its features that amplified the effects for the sake of profits.

Jarred Prier’s Commanding the Trend: Social Media as Information Warfare is a work that seeks to shed light on how social media platforms can, and have been, used as tools of information warfare. One concept Prier discusses here is the obsession social media websites have with trends, and how that obsession is weaponized for usage in information warfare. Prier explains that social media websites use algorithms to identify trending topics. These trending topics are then displayed to users, also in ways designed by algorithms. These topics often garner large interest from a large audience, even if it is only for a short time. The side effect of this mechanism is that it is incredibly good at being used to set an agenda. Bot accounts, in tandem with a dedicated team of agents, could easily change the trends and set a narrative. Prier outlines that there are three primary methods to disseminate propaganda using trending features. Trend distribution is simply applying a message to a trending topic. Trend hijacking is taking a pre-existing trend and changing it toward a different narrative. Trend creation involves the wholesale fabrication of a trend from the ground up using bots. Prier also details the nature of propaganda and what makes social media so compatible with it. It’s explained that propaganda can work on those predisposed to the message as well as those who are not. Even groups that are opposed to the propaganda message can, over time, begin to accept it. This is usually done through a messaging tactic that could be described as a "fire hose of information". Essentially, if a message is repeated and there is a huge volume of reports including the message, it can become normalized and accepted. Trending algorithms and social media can make this process easier. Part of the reason why is that social media is so present in the lives of the average American. Prier reports that 72% of Americans at the time of publication received their news from a mobile device. While this may not be all from social media, it could be assumed that a lot of it is. Nowadays, instead of a local newspaper or expert, people could get their news entirely from a friend or some other self-selected close group. This compounds the fact that, according to a 2016 poll, trust in mass media among Americans is at an all-time low. Prier then showcases two cases where we have real-world examples of agents conducting disinformation campaigns using social media. The case of Russian agents is particularly

relevant to the topic of discussion. Prier outlines how Russian agents have used the aforementioned tactics to great effect even before the 2016 election coverage. During the 2016 election race, Russian agents used large networks of bot accounts and a number of "cyber warriors", along with American "true believers", to wage a large-scale campaign in the election itself. Among the results of this campaign were entirely fabricated fake news trends like "Pizza-gate", and the amplification of other trends like WikiLeaks release of the Podesta emails. Prier notes that while Clinton almost won the popular vote by around 3 million votes, the actual outcome of the election was decided by a mere 80,000 or so votes in key states. He points out that claims that the Russian disinformation war had a significant effect on, or even decided, the election is not completely unfounded. When you combine the fact that Russia waged an intelligent and highly motivated information war with the fact that a relatively small number of votes decided the election, the possibility is there. Prier points out that the attacks were not only to raise the status of Russia and Putin in the eyes of the American people. From the efforts before the election to during and after, the goals include causing chaos, eroding trust in America and its institutions, sowing discord, and promoting other Russian interests. Prier concludes that while it could very well be that Russia used social media companies like Facebook and Twitter to help decide the 2016 election, there is more to the story. There are underlying conditions that made it possible for them to do so. The increasing reliance on social media for news and the increasing distrust of traditional news, combined with social media platforms existing issues and business models, provided a welcoming environment for such operations to take place. It's clear the American people were vulnerable, and those with a responsibility to protect them did not seem to do so and, in fact, may have completely ignored such a responsibility. The ethics of care would deem this is an ethical failing. To show care, is to educate, defend from threats, nurture skills, and provide guidance when you can and have the responsibility to. Even if there was not an organized disinformation campaign, Facebook had the responsibility to show care in the creation of its platform, and care for its users. This platform did not educate its users on dangers and threats, it did not have means to defend against potential threats, and did not nurture any skills that could allow its users to help themselves and allow them to care for others as well. Once you add the context of this organized disinformation campaign in, it becomes clear how easily the lack of care put in could be utilized to create a climate of chaos and harm.

Keith Scott's proceedings of the 17th European Conference on Cyber Warfare and Security in 2018 entitled *A Second Amendment for Cyber? Possession, Prohibition and Personal Liberty for the Information Age*, provides even more insight into how we can diagnose Facebook's actions. Scott starts off by reminding us that due to the nature of cyberspace and the modern world, many of the harms that could be done due to that world, like cyberstalking and cyberbullying, will only grow in regularity and intensity as our reliance on those technologies also grows. One important reason for this, is that technology doesn't just amplify human interaction, it will also fundamentally change it. Scott believes this is in part because of four key problems. Firstly, internet access is seen as a right and not a privilege. Second, the vast majority of those that use the internet are ignorant of its shortcomings, and how easily they can be compromised. Third, the vast majority of users are also ignorant of how the very information they absorb online could also be compromised. Finally, every user with access, likely has a vast array of tools at their disposal capable of causing immense harm. Scott highlights how dangerous these problems are, comparing internet access to an Ak-47, due to the potential

wide scale harm that could be done with each respective tool. All these facts come together to paint a picture that highlights how vulnerable the average user is. Using the ethics of care, we could see how Facebook has a responsibility to care for these vulnerable users, but also see how it failed to do so. Facebook seems to ecstatic to walk in the shoes of a "big brother" role, when it comes to profits. It collects hordes of information, it chooses what you see through algorithms, and can tailor the information to best garner the largest profits it can. When it comes time for big brother to care for its users the way a brother should, it seems to not only fail to do so, but even acknowledge the responsibility it has to do it in the first place. As showcased, now more than ever, users rely on and use the internet and cyberspace. This is true not only for news but all aspects of life. Facebook's users are vulnerable, and Facebook has the ability to care for them, and it is already dependent on them, as without them, there would be no social media to make a website for. The two parties are already intensely interdependent, but it seems as if Facebook was only concerned about itself flourishing, and not a mutual flourishing. As was established, the Russian operations during and before the 2016 elections were motivated to sew discord, erode trust, and ultimately, harm the American people. By crafting a platform that allowed such attacks to be performed (and potentially suceed) it highlights the failure to provide care within the very platform of Facebook itself. Facebook's crafting of its tools and algorithms did not meet the standard of care that was required of them. Instead, the crafting of its platform was seemingly devoted to only one thing, profit margins.

In conclusion, Facebook's platform caused it to become a conduit and agent of its own for information warfare during the 2016 election. Russian agents set out to harm American institutions and people with their disinformation campaign and information war. Facebook did not properly craft its platform out of care for its users, and the platform itself was perfectly compatible with information warfare. The users of Facebook rely on it more than ever for news and are more vulnerable than ever to cyber threats. This leaves Facebook with a responsibility to care for its vulnerable user base. Facebook did not meet this responsibility, did not show care towards those it should have, and thus acted unethically. While Facebook may have flourished due to its design focused solely on profit margins, a mutual flourishing between the users and Facebookbwas not achieved. The importance of these circumstances extends to other social media platforms and will only grow more important as news habits change and internet access and usage further proliferate.